Machine Learning and Artificial Intelligence
A.J. Tallón-Ballesteros and C. Chen (Eds.)

doi:10.3233/FAIA200803

Ad-Hoc Network Access Control System and Method for Edge NFC Terminal

Yiqin BAO[a] and Zhengtang SUN[b]
[a]College of Information Engineering of Nanjing XiaoZhuang University, China
[b]School of computer science and technology of Heilongjiang University, China

Abstract. With the rapid development of wireless communication technology, Near field communication (NFC) and Ad-Hoc network (ZigBee) have attracted wide attention for their security, speed and low power consumption. NFC has been used in access control research. In the past, the system only considered the switch control of the door lock, but could not achieve safety management in large building scenarios, resulting in security loopholes and poor maintenance of access control. In order to solve the above problems, Automatic networking access control system based on NFC and ZigBee technology is implemented. The access control and Internet of Things system (IoT) are fused through NFC. NFC identity information is transmitted through ZigBee to the management for identity authentication. The wireless transmission adopts the improved reduced AES advanced encryption algorithm R-AES, which ensures reliable data transmission. On this basis, the security of access control is realized. Practical results show that the Ad-Hoc network access control system and method for edge NFC terminal can improve the management efficiency and security of building access control.

Keywords. Iot, edge computing, NFC, ZigBee, AES-128

1. Introduction

With the rapid development of national economy, people's living environment has changed dramatically. High rise buildings bring more and more serious safety and security problems. The increasing number of high-tech crimes directly threatens the personal safety. At the same time, people's demand for intelligent management is also increasing, so the term "intelligent access control system" merged. At present, the design of the convenience and security of access control system is a very popular topic [1]. Based on the rapid development of Internet of things (IoT) solutions, the system presents new challenges to information collection, processing [2]

In recent years, with the continuous progress of biometric technology and induction technology, access control system has grown unprecedentedly and entered a relatively mature stage. For domestic, contactless IC card, password and biological characteristics constitute the three solutions of the current intelligent access control system, but there are some disadvantages. First of all, for contactless IC card and password, the corresponding reader can only identify through the information or password in IC card, but can't confirm whether it's personal operation [3]; second, for biometrics, such as camera, fingerprint, etc., its hardware cost is relatively high, the identification time is long, and it needs to be identified repeatedly. For NFC access control, smart phones have the advantages of low cost, convenience and strong reliability. Related literature

[4] has used NFC for access control system and ECS connection management; related literature [5] realizes authentication management through 3G connection; literature [6] realizes access control identity identification management by combining NFC and fingerprint.

At present, NFC intelligent application has become a development hotspot. It has been applied in the process of vehicle charging[7], in food monitoring[8], in geological and mineral data collection[9], and in electronic payment[10].

This paper presents an intelligent access control system for mobile NFC terminals, which is connected to the Internet of things through NFC. It has the advantages of low cost, high reliability and scalability.The self-organizing intelligent access control system for mobile NFC terminal is close to the NFC access control terminal through NFC smart phone. After the access control terminal reads the identity information, it is uploaded to the server side through ZigBee network and compared with the database to give the corresponding access rights. At the same time, Managers can view the user's access records in the system and change the opening and closing status of corresponding doors according to the actual situation. The wireless information transmission adopts the customized simplified encryption algorithm R-AES to ensure the security of information transmission.This paper analyzes the technical framework of the access control system, analyzes the system design, unifies the wireless communication network communication and encryption, and realizes an intelligent access control system for mobile NFC terminal. With the functions of authentication, unified management and wireless data encryption, it greatly facilitates access control management, enhances the security of access control data transmission, and greatly facilitates management and life [11].

2. System Architecture

The structure of smart access control system for mobile NFC terminal is shown in Figure 1. The system is mainly composed of four parts, including Android application terminal, access control terminal, network forwarding terminal and server terminal. Android application terminal mainly refers to Android smart phone with NFC function, which transmits identity authentication information through contact with access control terminal; access control terminal includes NFC module, gate magnet module and ZigBee module; access control terminal integrates data collection and control, which can not only collect NFC data, but also control corresponding gate magnet module; network forwarding terminal is composed of ZigBee router, Responsible for the data interaction between the access control identification control terminal and the server; the server is mainly composed of ZigBee coordinator, WiFi router, PC and background database, responsible for the upload of the authentication information of the whole system and the release of access control commands. The system supports two-way data transmission from left to right. From left to right, first collect NFC authentication information through the access control terminal, then upload it to the server through ZigBee wireless sensor network and ZigBee network forwarding terminal to realize the docking of system access platform. From the right to the left, the server sends the access control data to the corresponding access terminal via ZigBee wireless sensor network through the network forwarding terminal to realize the access control. The whole system can not only realize NFC identity authentication and access control functions, but also has the advantages of convenient networking, strong

anti-interference performance and low cost [12], which can greatly improve the security management efficiency of the whole access control system.

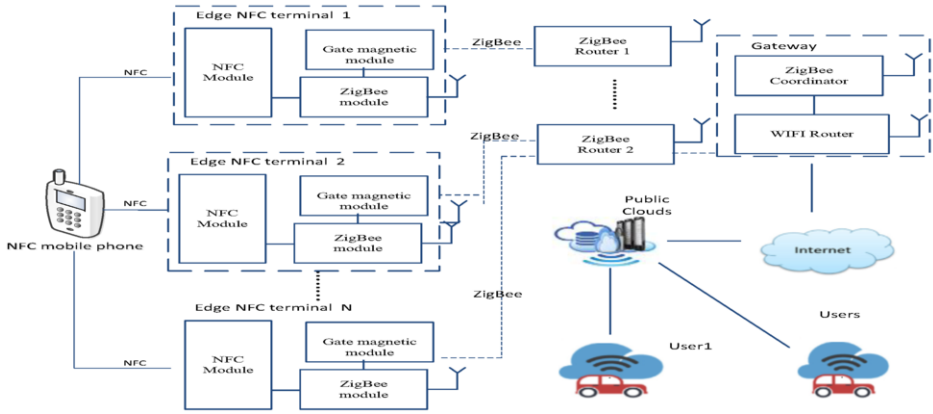

Figure 1. System architecture chart

3. System Design

3.1 NFC Module

NFC (Near Field Communication) is a short-range wireless communication technology. Mobile phones communicate with access control through NFC, and its foundation is RFID technology [13]. PN532 of NXP company is adopted as NFC access control reading module.As a short-range and high-frequency radio technology, NFC operates at a distance of 20cm in the frequency of 13.56MHz. Its transmission speed includes 106kbit / s, 212kbit / s and 424kbit / s. NFC has three modes of operation:

(1) Card emulation mode. This mode simulates the NFC device as an IC card. This has a great advantage: the card is powered through the RF domain of the contactless card reader, and can work even if the NFC device is powered down.

(2) Point to point mode. For data exchange. In this mode, the transmission distance is short, but the transmission speed is fast and the power consumption is low.

(3) Reader mode. Use the NFC device as a contactless card reader only, and read the corresponding information from the electronic label .

3.2 Zigbee Module

The ZigBee module used in the system is CC2530 chip, which is a real SOC solution based on 2.4GHz IEEE802.15.4, ZigBee and RF4CE application produced by Texas Instruments (TI). It can build powerful network nodes with little total material cost, program the chip, and perform logic operation, sequence control, timing, counting and calculation Technical operation, etc., through digital or analog input and output for environmental monitoring and equipment control signal output. As a new technology of wireless sensor network (WSN), it has a wide application prospect [14]. CC2530f256 is selected to realize the maximum function. The minimum system circuit is shown in Figure 2 [15].

NFC data needs to be uploaded to the server through ZigBee network for identity authentication. As a low-power, wireless ad hoc network protocol, ZigBee adopts

802.15.4 standard as the basis of its peer-to-peer communication. The standard was developed and managed by the ZigBee alliance. ZigBee is most commonly used in asynchronous communication, with CSMA / Ca channel intervention capability, and has all the functions in 802.15.4 standard. ZigBee can work in 2.4GHz (Universal), 868mhz (European) and 915MHz (U.S.), with the highest transmission rates of 250kbit / s, 20kbit / s and 40kbit / s respectively. Its transmission distance is in the range of 10-75m, but it can continue to increase. Because of its low power consumption, low cost, short time delay, large network capacity, reliability, security and other characteristics, it is widely used in intelligent home, intelligent medical, intelligent agriculture and other Internet of things industries.

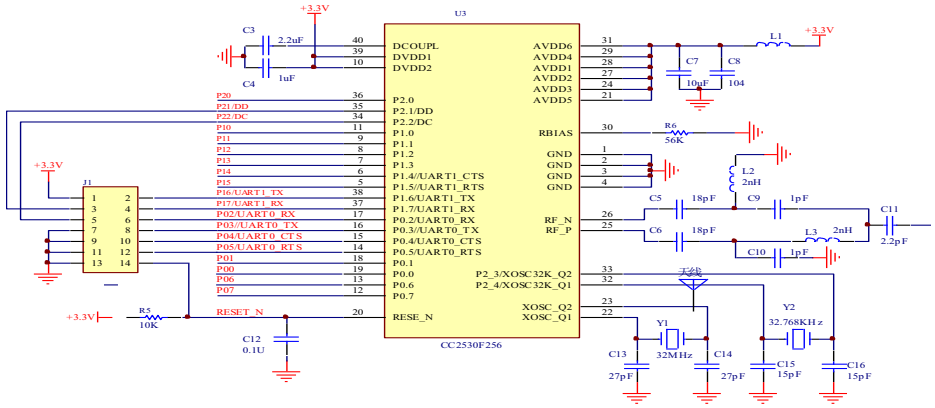

Figure 2. CC2530 system circuit diagram

3.3 Access Control Terminal Design

Access control terminal consists of three parts, NFC module, ZigBee module and door magnetic module. The NFC module Hsu_TX and Hsu_RX are respectively connected with pin P0.2 and pin P0.3 of ZigBee module to realize data interaction between NFC module and ZigBee module; the relay in pin is connected with pin P0.0 of ZigBee module to realize access control, and the corresponding pin is set in the program. CC2530 program flow chart is shown in Figure 3.

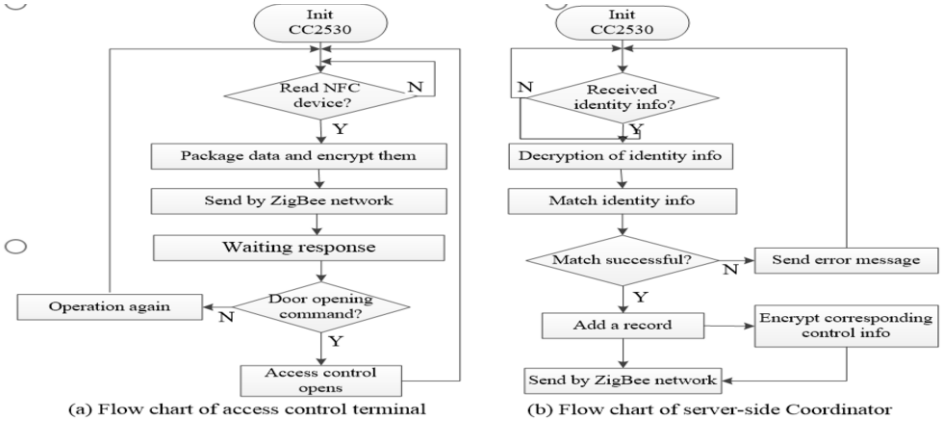

Figure 3. CC2530 program flow chart

Actual operation scenario: the system is installed on the door. When the NFC smart phone is close to the NFC reading device, the read information is transmitted to ZigBee module for data encryption and packaging. The data frame is sent to the server through ZigBee network to decrypt the package and match the data with the database. If the information matching is successful, the server will return the corresponding response command to control the opening and closing of the door; otherwise, it will remind the user to repeat the above steps; if the information matching still fails, it will send a warning message to the administrator for management.

4. System Communication

4.1 NFC Communication Protocol

The reliable transmission between NFC module and ZigBee ensures the accuracy of authentication. Therefore, the communication protocol is developed in the system, and the data frame structure is shown in Figure 4. For the communication mode between NFC communication module and ZigBee module in the system, the baud rate is set to 9600, the data bit is none, and the stop bit is 1.

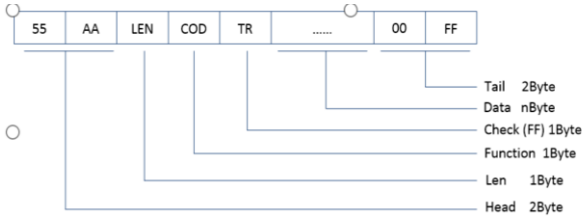

Figure 4. NFC frame format

For NFC communication frame format, frame header takes up 2 bytes, fixed as 55 and AA; len is frame length takes up 1 byte, which is the sum of function code, check sum and data; COD is function code takes up 1 byte, which is used to set the mode of NFC reading equipment, specific function code settings are shown in Table 1, fixed as 12 in the system, that is, point-to-point mode; check sum takes up 1 byte, fixed as FF; data bits take up n bytes It is used to store data; the frame end occupies 2 bytes, fixed as 00, FF.

Table 1. Function code table

Pattern	Function Code
Reader mode	0x10
Card simulation mode	0x11
Point to point mode	0x12
Query firmware version	0x25

4.2 Modbus Communication Protocol

After the ZigBee module packs the data transmitted from NFC, it needs to send the identity authentication data to the server through ZigBee. The international Modbus communication protocol is adopted in ZigBee wireless network. Modbus protocol is a general language applied to electronic controller. Through this protocol, communication between access control terminal and server can be realized, identity information of NFC can be authenticated and access control command can be sent.

Table 2. Frame format

Address	Function Code	Data Area	CRC Check
1Byte	1Byte	nByte	2Byte

The format of Modbus protocol frame is shown in Table 2, and the order of register transmission is from high to low. When the devices communicate with each other in the network, they need to know their device addresses.

4.3 Communication Encryption Algorithm

4.3.1 R_AES

R-AES is a simplified version of Advanced Encryption Standard AES. AES encryption algorithm [16] is a group encryption method, AES-128 algorithm is based on 128 bit length as the main standard to achieve encryption design. R-AES inherits the advantages of AES advanced encryption, considering the limited speed and resources of embedded system, on the basis of AES, firstly, the encryption steps that occupy large resources of embedded system are cut; at the same time, the number of encryption and decryption rounds is reduced. In the case of ZigBee security and encryption, the resource overhead of embedded system is reduced and the encryption speed is improved.

4.3.2 R_AES Workflow

AES algorithm [17] mainly consists of five steps: 1) Extended key; 2) Byte replacement ; 3) Row shift; 4) Mix Columns; 5) Round key addition, which has undergone 10 rounds of operation.

The R-AES algorithm is a simplified AES algorithm, and its workflow is shown in Figure 5. Compared with the traditional AES advanced encryption algorithm, it cuts out the column confusion that takes up a lot of resources in the algorithm steps. At the same time, the number of encryption rounds is reduced from the traditional 10 rounds to 3 rounds, which reduces the system resource occupation and greatly improves the running speed of the embedded system on the premise of ensuring the system security. The A-AES algorithm consists of four steps: extended key, byte replacement, row shift and round key addition.

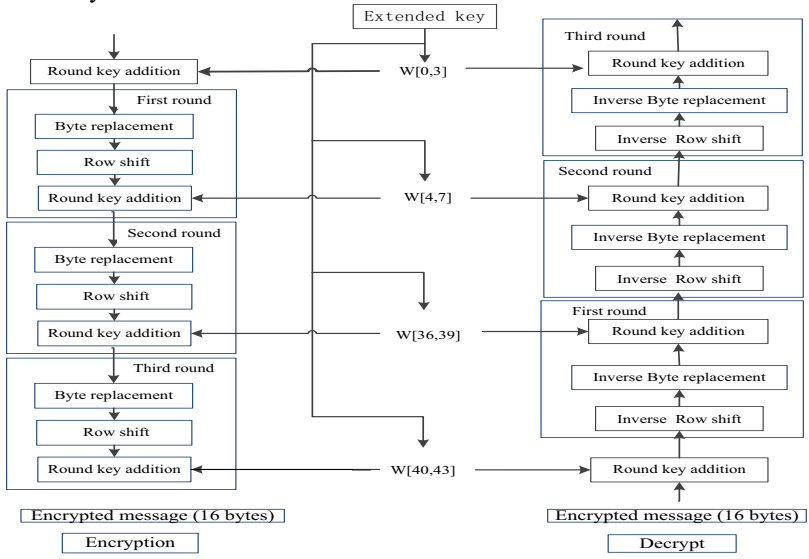

Figure 5. R-AES algorithm workflow

4.3.3 Application of R_AES

After passing the NFC demonstration, ZigBee wirelessly transmits the Modbus message, as shown in the door access command: 20050000ff008c3a, and encrypts and decrypts the data in the system as shown in Figure 6

```
The key is:
2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
Message to be encrypted:
20 05 00 00 ff 00 8c 3a
Encrypted Message:
b7 e2 49 7e c1 cf d2 b5 c1 e6 10 00 c4 40 49 3c
Decrypted Message:
20 05 00 00 ff 00 8c 3a
```

Figure 6. Sample of message encryption and decryption data

R-AES key is: 0x2b, 0x7e, 0x15, 0x16, 0x28, 0xae, 0xd2, 0xa6, 0xab, 0xf7, 0x15, 0x88, 0x09, 0xcf, 0x4f, 0x3c. 8 bytes Messages is:0x20,0x05,0x00,0x00,0xff,0x00,0x8c,0x3a.Because AES adopts block encryption, 16 bytes are one group, and the Messages is insufficient to fill zero.The Messages after R-AES encryption is: 0xb7,0xe2,0x49,0x7e,0xc1,0xcf,0xd2,0xb5,0xc1,0xe6,0x10, 0x0,0xc4,0x40,0x49,0x3c.

It is almost impossible for attackers to decrypt ciphertext, so as to achieve the effect of encryption security.

5. System Testing

During the test, when the Android mobile terminal registered and authorized in the access control system is close to the NFC data reading area, the identity information is encrypted and transmitted to the server. After the server decrypts the information, it can query and confirm to open and close the corresponding door lock. Compared with the traditional IC card, NFC technology saves a lot of unnecessary troubles. At the same time, if the mobile intelligent terminal is lost or maliciously stolen by others, it can't be unlocked because it doesn't know the AES password of the terminal. In addition, it can't be unlocked if communication attack is used, which guarantees the security of the system. The physical test diagram of mobile terminal in access control system is shown in Figure 7.

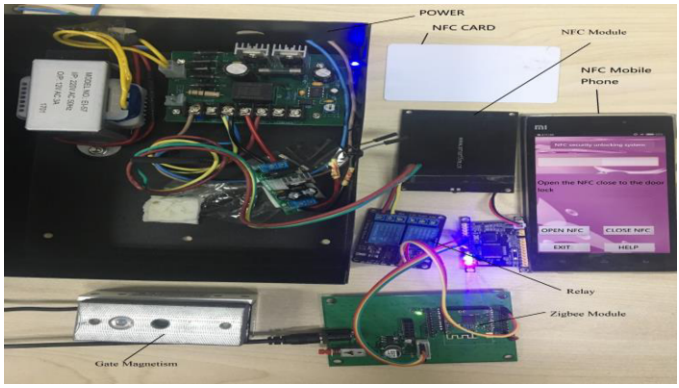

Figure 7. Physical map of mobile terminal in access control system

6. Conclusions

In this paper, the Ad-Hoc network access control system has been developed and applied to a large number of access control, The result is effective management of access control security. When the door needs to be opened, just take out the smart phone, close to the reading area, the door can be opened and closed; ZigBee wireless network transmits information to the server, which enables administrators to manage access control in batches more effectively; wireless transmission R-AES advanced encryption can ensure the safe transmission of information. Compared with other access control systems on the market, the system has the advantages of convenient operation, strong stability, safety and reliability. The smart access control system of Ad- hoc network for mobile NFC terminal has a high promotion value.

Acknowledgement

This work is supported by Natural Science Foundation Project of China (61976118), Key topics of the '13th five-year plan' for Education Science in Jiangsu Province (B-b /2020/01/18).

References

[1] Ye Chen. Design of Intelligent Access Control System Based on RFID [J]. Information System Engineering, 2018 (06): 34-36.
[2] Răzvan Andrei Gheorghiu, Iordache V, Minea M . Messaging capabilities of V2I networks[J]. Procedia Manufacturing, 2018, 22:476 – 484.
[3] Pi Haitao, Jiao Huirong, Hao Kui et al. Design of bus IC card real-name system based on ZigBee [J]. Computer measurement and control, 2014, 22 (11): 3754-3756.
[4] Sun Heng. Design and implementation of a new access control system based on NFC technology and cloud service [J].Laboratory Research and Exploration, 2016,35(01): 114-120.
[5] Li Manling. Design of digital intelligent access control system based on NFC [J]. Journal of Ezhou University, 2014, 21 (06): 108-110.
[6] Jin Zhigang, Jie Bingshan. A highly secure access control system authentication protocol combining fingerprint identification and NFC technology [J]. Journal of Nankai University (Natural Science Edition), 2017, 50 (05): 1-7.
[7] Ritrovati G , Maso-Gentile G D , Scavongelli C , et al. Active role of a NFC enabled smartphone in EV-EVSE charging process[C]// 2014 IEEE International Electric Vehicle Conference (IEVC). IEEE, 2019.
[8] T B , Tran V T , Chung W Y . Pressure Measurement-Based Method for Battery-Free Food Monitoring Powered by NFC Energy Harvesting[J]. Scientific Reports, 2019, 9(1):17556.
[9] Huang Ting, Liu Gang, Zhang zhiting, et al. Geological and mineral data acquisition system based on NFC and geoml [J]. Computer application and software, 2019 (9).
[10] Chabbi S , Boudour R , Semchedine F , et al. Dynamic array PIN:A novel approach to secure NFC electronic payment between ATM and smartphone[J]. Information Security Journal A Global Perspective, 2020, 29(4):1-14.
[11] Lu Kailang, Wang Huo, Zhao Ming. Design and Implementation of Intelligent Access Control System Based on NFC [J]. Electrical Applications, 2013, 32 (S1): 639-641.
[12] Ran Junjun, Liu Zhiqin, Zhong Min. WiFi interference avoidance method based on channel state prediction in ZigBee networks [J]. Computer measurement and control, 2017, 25 (06): 124-127.
[13] Li Manling. Design of digital intelligent access control system based on NFC [J]. Journal of Ezhou University, 2014, 21 (06): 108-110.
[14] Wu Y, Liu K S, Stankovic J A, et al. Efficient Multichannel Communications in Wireless Sensor Networks[J]. Acm Transactions on Sensor Networks, 2016, 12(1):1-23.
[15] Bao Yiqin, Xu Wenbin. Research and Design of Intelligent Network Switch Based on Human Infrared and Light Intensity Sensors [J]. Internet of Things Technology, 2018,8(05): 16-18+23.

[16] Bi Ganbin. Research and application of encryption algorithm based on ZigBee [D]. Guizhou University, 2017:30-56.
[17] Zhang Yao, Ye Ling. WSN Encryption Algorithms Based on AES [J]. Computer Engineering and Design, 2015, 36 (03): 619-623.