Research of Utility Prepayment System based on Wireless Communication

PAN Tie-Jun[1], ZHENG Lei-na[2], ZHANG Hua-jun[1], FANG Chen-bin[1]
Department of Computer and Information[1], Department of Business School[2]
ZheJiang WanLi University
NingBo 315100
China
http://www.zwu.edu.cn

Abstract: - This paper seeks to clarify differences and similarities among impressive array of radio access technologies which can be used in utility prepayment, analyzes the requirements of wireless prepayment utility meter system. It present a set of mobile prepayment solution in which the prepayment meter (PM) system is implemented without smart card and user need not go to agency by oneself for prepayment. For the purpose of solving the difficult problem of utility meter prepayment at the specific location in person, mobile payment client (MPC) with graph user interface (GUI) located on mobile device which is responded for business initiation. PM is connected to PS via Zigbee network or WLAN in short range access network and via the 3rd generation wireless communication infrastructure (3G) in long range access network, and utility meter may connect Zigbee node via RS485 bus. By means of identification and mutual authentication which generating different session key with time stamps every time, the cross validation mechanism among PM, MPC and PS improve the security of mobile prepayment system. The security mechanism is given in the end including user identification, mutual authentication, and data integrity and data confidentiality. In the end, ZigBee node hardware design and meter interface design is introduced and a practical application is given. The result of the present work implied that mobile phone is gradually becoming a data access and exchange platform of mobile payment, and WiMax is another competitive technology which will be used in the utility wireless prepayment solution.

Key-Words: - mobile payment; OTA; Zigbee; WiMax; 3G; meter; RS485
Supported by Ningbo Municipal Natural Science Foundation of China (2007A610041)

1 Introduction

At present, as mankind has marched into the new generation communication age, informationization in electricity, gas and water utilities are developing rapidly, increasingly changing people's ordinary lives. Traditional manual meter-reading is time-consuming and laborious without insurance of accuracy and timeliness, which led to the marketing and related enterprises application software can not get enough detailed and accurate data; manual meter-reading in general have a monthly meter reading, which is feasible to the user, but is not enough for the supply of related departments to carry out in-depth analysis and management decision-making, the actual needs of the industry bring forward the birth of an automatic meter reading（AMR） technology and applications development. PM is a kind of new-style meter that purchase electricity by smart card and adopt micro-electronics techniques that can help the power company to accomplish prepayment function. Both potential and realized benefits of prepayment are obviously to the power company. Smit and Daniel have proposed a kind of electronic meter reader system and method. A utility metering system includes a plurality of distributed utility meter readers. Each reader is associated with a respective electronic utility meter at a respective utility user station. Each meter reader comprises a transceiver for transmitting metered data received from the respective meter to a remote station via a GSM cellular infrastructure in the form of an SMS message [1]. But the GSM transceiver is too slow and expensive for individual user to afford.

With the wireless communications technology development in recent years, there have been the technology for low-cost wireless networking equipment requirements, called Zigbee, it is a close-up, low-complexity, low-power, low data rate, low-cost and two-way wireless communications technology, which is suitable for automatic control, remote control and home networking equipment, especially to household meter. At the same time, with the coming of the 3rd Generation mobile communication (3G) age and the progressive popularization of smart phones, mobile payment is accelerating development. Analysis International released that China's mobile payment market will reach 1.974 billion RMB in 2009 and the average annual compound growth rate will reach 70.40 percent from 2006 to 2009. (Fig. 1) The users will be able to enjoy mobile payment services with up to 2 Mbps data rate and the broadcast nature of 3G will greatly increase popularity of wireless devices and data rate of AMR. We have adopted Zigbee and 3G technologies for household meter to provide wireless meter reading and prepayment solution. [2, 3]

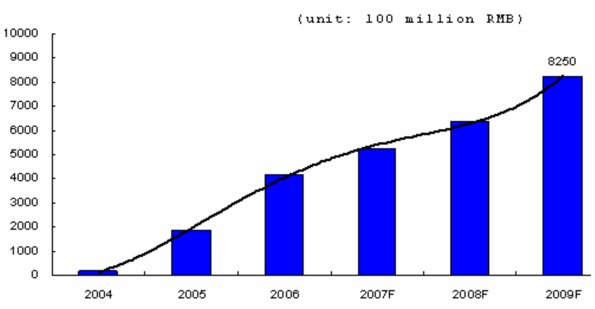

Fig. 1 Mobile payment market forecast from 2007 to 2009

2 Wireless Prepayment Solution

An impressive array of radio access technologies already in play — from cellular in its various forms, to 3G and HSPA data networks, to short-range connectivity technologies, such as Bluetooth, Zigbee, UWB etc. along with location-position technology GPS, and Wi-Fi. (Fig. 2) It expects more devices to connect via multiple networks so users can be assured of connectivity and can select a preferred network based on factors such as availability, cost and speed.

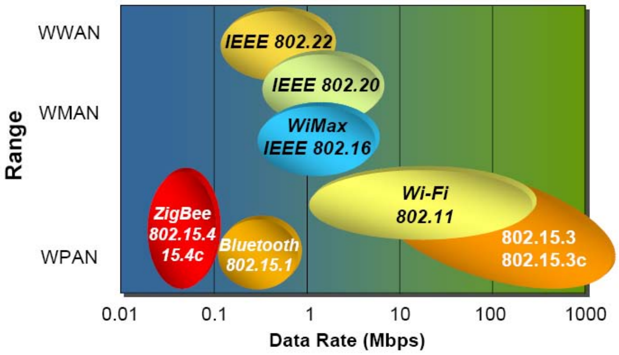

Fig. 2 Mainstream wireless technologies

There are many difficult problems in the utility meter field in the past years, such as management, maintenance etc. especially to payments. Therefore, the prepayment solution is developing which enhancing the level of utility meter management greatly at present. In some special conditions, the wireless technology will improve the function and performance of the utility meter prepayment system in the future.

2.1 Requirements

Wireless Prepayment Solution (WPS) of utility meter on wireless data transmission have high demands, which require high reliability of data; due to the use of battery-powered, so power requirements are harsh. WPS not only make mobile prepayment for utility to be true, but also can get rid of the manual meter-reading methods using data communication protocol. For these reasons, the design of WPS should have an accurate measurement, reliable communications, meter reading convenient, low-power advantages of remote meter reading system, as well as the function of mobile prepayment, labor-saving, remote monitoring, remote maintenance. Compared with the power meter, water meter and gas meter reading system have more technical problems, mainly reflected in the design of meter-reading terminal, utility meter reading terminals must be to address the following technical requirements: [4, 5]

2.1.1 Mobil prepayment

For the purpose of solving the difficult problem of everyone should pay the utility fee at the specific location in person, which will take users too much time and cost for waiting and going, WPS should provide the mobile prepayment solution for convenience at first.

2.1.2 Power supply

As water meter and gas meter reading terminals using battery-powered, the power requirements are harsh. In general, the battery useful life need to be at least 3 to 6 years, depending on the capacity of the battery, power equipment, equipment operation and so on.

2.1.3 Costs

Whether home users or business users, the cost of meter-reading terminal has always been the focus topic, especially home users with the more cost-sensitive. The cost is of two parts: one is the one-time installation or transformation costs, and the other is the operation cost. The best option should be one-time investment costs is as low as possible and operation costs is very low or no cost.

2.1.4 Fault detection

In addition to the manual meter-reading activity, it is also responsible for checking whether the meter is normal. So WPS should also have the function of automatic fault detection. Of course, this requires the cooperation of meter and WPS.

2.1.5 Reliability of communications

This is the basic requirement of WPS, but at the same time, it is not easy to solve the problem.

2.1.6 Self-organizing and self-healing

Self-organizing and self-healing features of wireless networks is an extremely advantage to WPS.

Self-organizing: no human intervention, network node has the capability of node-aware of the existence of other, and exterminating of the connection relationship, organizing of the structural network;

Self-healing: in the scenario of increasing or removing a node, changing a node location, node failure, and so on, the network will be able to self-repair, adjust network topology accordingly without human intervention to ensure that the entire system can still work properly.

With self- organizing, self-healing ability, WPS network will be the best network. Zigbee technology is able to support the kind of intelligent networks. Zigbee Network is suitable for short-range wireless connection and communication while 3G is suitable for wireless wide coverage of long distance and large amount of data transferring. Both of them can be cooperated for providing a completed mobile prepayment solution in the field of utility meter.

2.2 Short-range wireless network

Zigbee and Bluetooth technology was developed to create a short-range wireless voice and data link between a broad range of devices such as PCs, notebook computers, PDAs, mobile phones and digital cameras. At its heart, they are about creating a Wireless Personal Area Network (WPAN) consisting of all the Short-range-access-enabled electronic devices immediately surrounding a user, wherever that user may be located. The IEEE 802.11b standard was designed to be the best solution for a single specific application: wireless Ethernet. At its heart, Wi-Fi is about enabling wireless LAN access for computer and other portable device users. We seek to clarify the differences and similarities between the IEEE 802.11b WLAN(Wireless Local Area Network) standard, also known as Wi-Fi™, and the IEEE 802.15 WPAN standard, also known as Zigbee and Bluetooth™. The complementary nature of the two technologies is used in the last mile solution of residential area and the role that each technology can play in LAN and Internet access is different.

ZigBee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2006 standard for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio. The technology is intended to be simpler and cheaper than other WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking. To domestic meter which are idle (not transmitting/receiving) for long periods, it only need the low data rates (less than 250kbps). Normally, it is difficult to set up or modify the meter network in the residential area where cables would be difficult or expensive to install, so that ZigBee technology may be the best choice.

For those traditional residential area whose have the legacy network with RS485 bus, the ZigBee node only is responsible for transparent data transferring and routing as shown in Fig. 3. Data collector is responsible for utility meter data collection and transmission through RS485 bus. At the same time, download command from utility server is also be received by data collector which dispatch these command to meter.

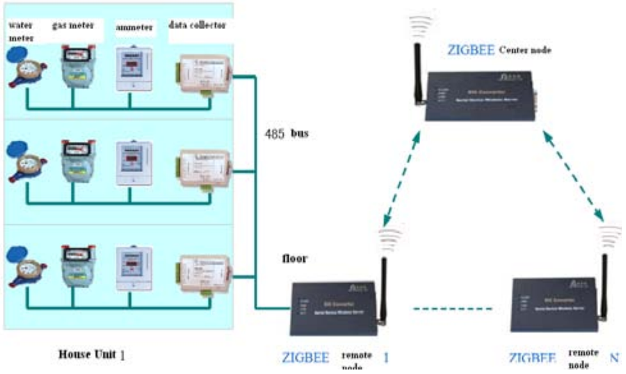

Fig. 3 Zigbee network with RS485 bus

For those house units in residential area which have deployed WLAN using Wi-Fi technology, a star network topology may be the preference to a domestic wireless network. It has a central node, named coordinator (Full Functional Device, FFD), which is linked to all other nodes including router and end devices (Reduced Function Device, RFD or FFD) chiefly deployed at the turns or fixed positions of the passage in charge of meter data collection in the network. (Fig. 4) All messages travel via the central node which connects with the domestic gateway via COM and responsible for transmitting data to it. In the end, meter data is transmitted to remote utility server via WLAN and Internet. Obviously, WLAN can be replaced by LAN if possible.

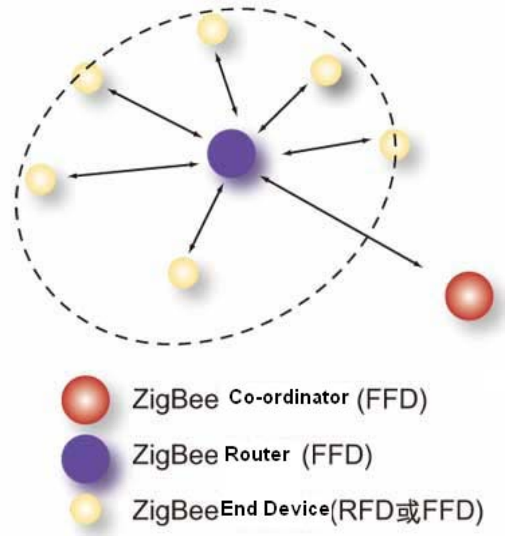

Fig. 4 Domestic Zigbee wireless network topology

For those high-density house units in residential area without WLAN or LAN, a mash network topology may be the preference. (Fig.5) There is always one node that takes a co-ordinating role in a network - the central node in a Star topology, the top node in a mesh topology. There must also be nodes with the role of relaying messages from one neighboring node to another. The most difference is the Concentrator deployed in the residential area take the place of domestic gateway now. Concentrator stands in a critical position in the entire system, it is the throat site which is connecting the zigbee network and the utility server together. Concentrator performs intensive information gathering and processing on the detected information which is provided by the zigbee network in the building through the zigbee module, then packs and sends data to the utility server through cable network for further processing.

Concentrator would be settled in the entrance of power, water or gas to residential area, transmit the data to Router complying UDP through cable network, and then Router will send data to utility server. After utility server received the data, it would analyze and process on it. If data show that some meter monitored by zigbee node is in trouble or back charge, utility server will send alarm information back to concentrator through cable network, and then concentrator will send data to zigbee network in the building. The in-trouble zigbee node would alarm as soon as it receive the return information.

From a network point-of-view, each meter software agent running on a node is a unique network entity where messages can originate and terminate. This entity is termed an endpoint. Each node can have 240 user endpoints, numbered 1 to 240, the endpoint addresses which can meet prepay and AMR requirements of most residential area. A particular endpoint in the network is identified by means of the network address of the host node and its endpoint address on the node. The ZigBee stack in a meter network will use or extend the relevant 'Stack Profile' from the ZigBee Alliance. The stack profile determines the type, shape and features of the network, and depends on the field of application, e.g. the Home Controls profile. A Prepayment Profile is associated with a particular stack profile and addresses the needs of a mobile prepayment application; it has defined the Home Controls-Prepayment (HCP) application profile for use in controlling meter in the home. It defines a number of devices and functions which are needed or are useful for controlling domestic meter, such as switches, meters, occupancy sensors and load controllers (which control the power sources).

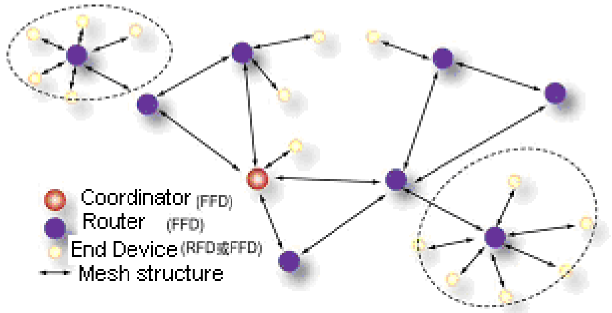

Fig. 5 Residential area Zigbee network topology

2.2 Long-range wireless network

Zigbee and Wi-Fi network is only used for metered data collection and transparent transferring in short distance; it can not transfer metered data to the utility administration department in long distance. The difference of relative wireless technologies is shown as table 1. Then it is an important problem to transfer data to Payment-center, especially to the remote enterprise or farm on the country.

There are two way at present, one is the cabled solution while the other is wireless solution. Cabled solution is comprised by ADSL, Power line carrier (PLC) and etc. However ADSL is not available in some rural area and mountains in China, PLC meter reading using the existing power line network, saving the line cost, but owing to the power line with complicated and ever-changing environment, the carrier signal is vulnerable to disturbance, stability and reliability of meter reading data is very low, power line carrier meter reading in the market system is rarely used.

Using GSM technology, wireless automatic meter reading system for the use of telecommunications service provider of wireless communication networks, is able to meet the rural areas and the city's wide coverage on reading, but the GSM technology required to pay Internet access fees and the higher cost of hardware, so that the GSM wireless automatic meter reading cost is too high, the market can not be widely accepted. With the development of 3G, the Internet access fees is reduced enormously and the hardware cost is ignored depending on residential users on shares during a long time. [6, 7, 8]So that, we bring forward a utility metering system includes a plurality of distributed utility meter readers which connect to server via 3G infrastructure and Zigbee network as shown in Fig. 6.

Table 1 difference of wireless technologies

Item	Zigbee	3G	WLAN
Network occupation and expenses	2.4GHz,free-to-air channels	not free	free-to-air channels
Power dissipation	very low	high	high
Network scale	65536	1	32
Transmition distance	1-1000m	long distance	1-50m
Transmition bandwidth	256K	128K	11M
Technology advantage	low cost and power dissipation, large capability, high safety	wide coverage	high data transfering rate

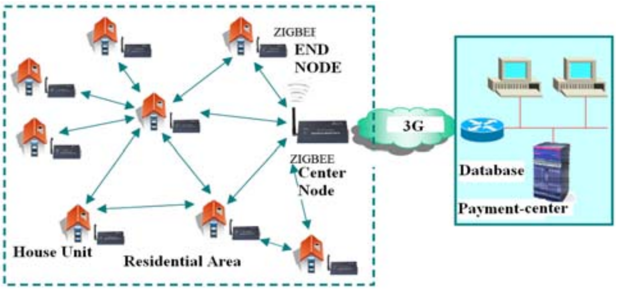

Fig. 6 Zigbee network with 3G infrastructure

Each reader is associated with a respective utility meter at a respective utility user station. Each meter reader comprises a transceiver for transmitting metered data received from the respective meter to a remote station via a 3G cellular infrastructure in the form of data stream. The data received is stored in a database in relation to a unique identification code number. In the case of meters for pre-paid utilities, the system enables users to obtain credit readings from the station from positions remote from the meters and also to replenish credits on the meters from such positions, by causing the station to transmit credit data prepaid for via the infrastructure to the meters [1].

2.3 Mobile Prepayment Procedure

The development of smart phone technologies for supporting downloads over the air (OTA). In response to this, user achieves prepaying and checking records with GUI through process bellow [4, 5] as shown in Fig.7.

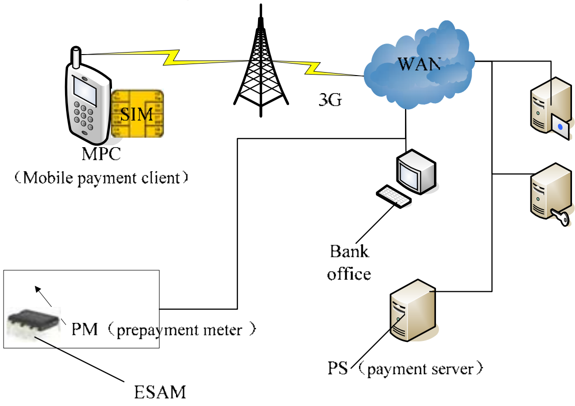

Fig. 7 Mobile Prepayment Solution Network

Firstly, user takes his or her own valid ID and bank card to any agency or banking offices of bank which has contract with power company and fills in "Personal Mobile Payment Banking Service Application Form" to apply for the service and obtain authorization code. Following the procedure stated in User's Guide, user can install mobile payment client software on their mobile phone via OTA. All the signed information including MSISDN, IMSI, IMSI, user name, password, authorization code etc. is stored in PS database for future transaction verification and authentication.

Secondly, user starts MPC, selects mobile payment item, inputs contract ID (e.g., power meter id, MSISDN, bill id), selects account and confirms. In addition, password needed for non-registered account.

Thirdly, the mutual authentication is used by prepayment applications to authenticate MPC to PS and vice versa. MPS and PS complete mutual authentication with MSISDN, IMSI, IMSI, user name, password, and authorization code used for single or crossed verification and authentication. The prepayment transaction information is transferred on data stream channels in 3G mobile networks. In response to this, MPS is implemented by STK, J2ME or WAP. The encrypted prepayment information returned from PS is saved to SIM with special SMS.

Finally, PS sends the payment information to PM after mutual autentication via cellular infrastructure and Zigbee network. At the same time, The timestamp in the ciphertext can protect prepayment information from reply attack and digital signature for authentication is used to keep data integrity and non-reputation, the payment record is saved in database for audit.

3 Security mechanism

We provides mobile prepayment security procedure for application layer, which implements all kinds of mobile security services for the sake of convenience: User identification and administration (IMSI/ISDN/EID), AKA (Authority and Key Agreement), DI (Data Integrity), DC (Data Confidentiality), authentication information translation between meter with ESAM(embeded secure access module) and Prepayment-center. It is based on object oriend design technology, which provides compatible API with 3GPP security protocol, user can flexible configure the security service and main algorithms library according to different requirements. At the same time, It provides the concrete realization of the core algorithms clear defined of 3GPP, including: the f1, f2, f3, f4, f5, f1* and f5* in AKA, the f6 and f7 in EUIC, and data encryption algorithm f8 and data integrity algorithm f9. All algorithms are realized based on two core encryption modules: KASUMI and AES.

The mechanism of this security system service is as follows:

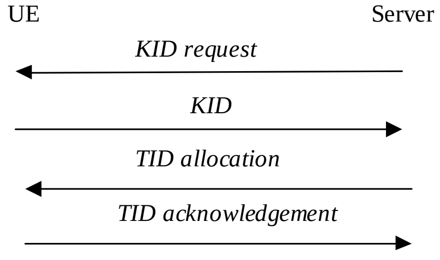

Fig.8 User confidentiality

3.1 User confidentiality

Permanent user key identity (KID) and user mobile prepayment services cannot be determined by eavesdropping which achieved by use of temporary identity (TID) which is assigned by UE through web server. KID is sent in cleartext when establishing TID (Fig. 8). KID is generated from IMSI, ISDN, IMEI and main key which is distributed by utility administrator or bank officer. It can be stored in the flash or SIM of smart phone, even the SD or MMC card which can be access by MPC.

3.2 Mutual authentication

During Authentication and Key Agreement (AKA) the meter and server authenticate each other, and also they agree on cipher and integrity key (CK, IK). CK and IK are used until their time expires. On the assumption of trusted server and CA, and trusted links between them, after AKA which assure UE and server that CK/IK have not been used before, security mode must be negotiated to agree on encryption and integrity algorithm (Fig. 9). Meter and server share user specific secret K, message authentication functions f1, f1* and f2, and key generating function f3,f4, and f5. Server has a random number generator, and has scheme to generate fresh sequence numbers. Meter has scheme to verify freshness of received sequence numbers.

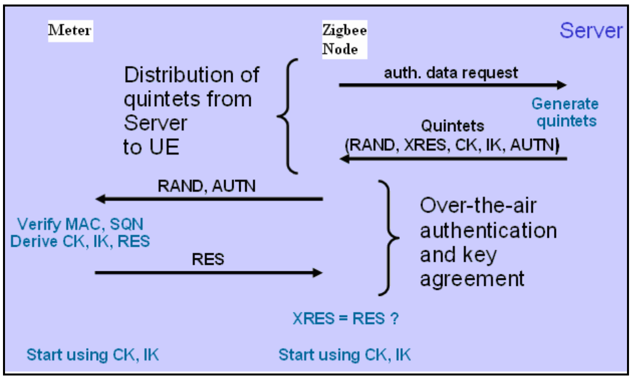

Fig.9 AKA process

AKA Variables and Functions:

RAND= random challenge generated by Server

XRES= $f2_K$ (RAND) = expected user response computed by Server

RES = $f2_K$ (RAND) = actual user response computed by eKey

CK = $f3_K$ (RAND) = cipher key

IK = $f4_K$ (RAND) = integrity key

AK = $f5_K$ (RAND) = anonymity key

SQN = sequence number

AMF = authentication management field

MAC= $f1_K$(SQN || RAND || AMF) = message authentication code computed over SQN, RAND and AMF

AUTN = SQN⊕AK || AMF || MAC = server authentication token, concealment of SQN with AK is optional

Quintet = (RAND, XRES, CK, IK, AUTN)

Generation of authentication data at server is shown as Fig. 10.

Generation of authentication data in meter is shown as Fig. 11.

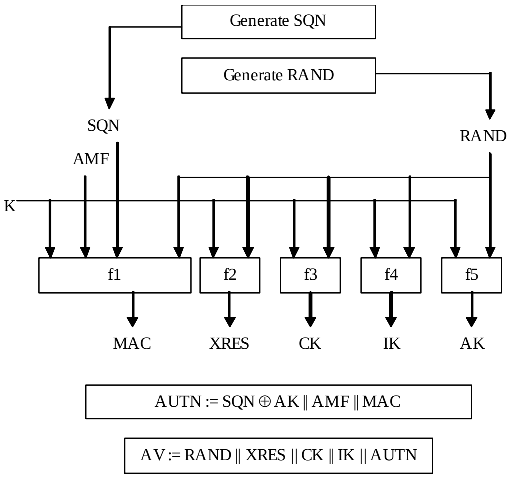
Generate SQN
Generate RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Fig.10. Generation of authentication data at server

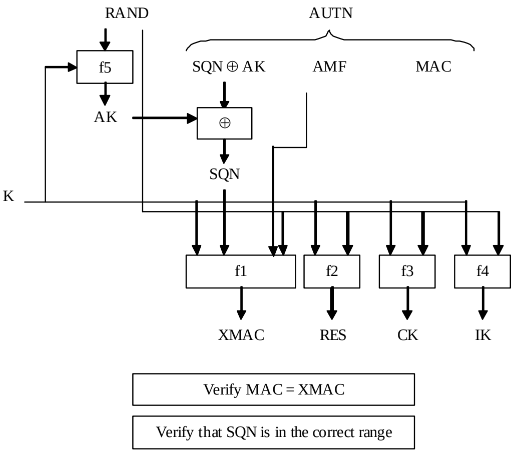

Fig.11. Generation of authentication data in meter

3.3 Data integrity

Integrity of data and authentication of origin of mobile prepayment signaling data must be provided. The user and server agree on integrity key and algorithm during AKA and security mode set-up (Fig.12).

3.4 Data confidentiality

Signaling and user data should be protected from eavesdropping. The user and server agree on cipher key and algorithm during AKA and security mode set-up (Fig.13).

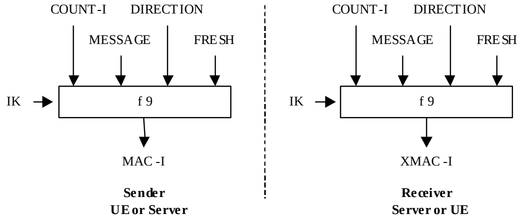

Fig.12 Data integrity

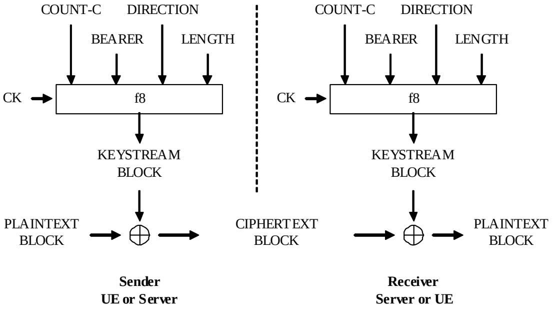

Fig.13 Data confidentiality

3.5 ZigBee Security Measures

ZigBee networks are highly secure. They incorporate measures to prevent intrusion from potentially hostile parties and from neighboring ZigBee networks. To this end, a “Security Toolbox” is included with ZigBee, offering the following features:

3.5.1 AES-based Encryption

A very high-security, key-based encryption system is used to prevent external agents from interpreting ZigBee network data. Data is encrypted at the source and decrypted at the destination using the same key - only devices with the correct key can decrypt the encrypted data.

A 128-bit encyption system is employed based on the AES (Advanced Encryption Standard) algorithm.

3.5.2 Message Timeout

This feature allows timed-out messages to be rejected, preventing message replay attacks on the network.

A frame counter is added to a message, which helps a device determine how old a received message is - the appended value is compared with a value stored in the device (which is the frame counter value of the last message received). This value only indicates the order of messages and does not contain time/date information. This allows protection against replay attacks in which old messages are later re-sent to a device.

An example of a replay attack would be a malicious individual recording the open command for a garage door opener, and then later replaying it to gain entry to the property.

3.5.3 Access Control Lists

A provision of the underlying IEEE 802.15.4 standard is that a node is able to select the other network nodes with which it is prepared to communicate. This is achieved using an Access Control List (ACL), maintained in the device, which contains the MAC addresses of nodes with which communication is allowed.

The source node of an incoming message is compared against this list, and the result is passed to the higher layers which decide whether to accept or reject the message. However, note that if messages are not encrypted, the alleged source of a message could be falsified.

4 Development

4.1 ZigBee Node hardware design

As the Zigbee node module to be used in conjunction with the meter or be used independently and battery-powered, it is required to be small, low-power and high reliability. It can reduce the size to the minimum by selecting small patch package device circuit design and using PCB wireless antenna. It can reduce the power consumption to the minimum in the state of idle and sleep by using PIC18LF4620 single-chip as core processor. It can maintain stable performance by selecting the integrated transceiver chip, Chipcon CC2420 in line with the standard agreement of Zigbee with only a few external components. (Fig. 14) It uses direct sequence spread spectrum technology to ensure the effectiveness and reliability of short-range communications. It works in the 2.4G band with data rates up to 250Kbps.

4.2 Meter interface design

With the development of Automatic Meter Reading (AMR) technology, RS485 has become the mainstream communication technology for collecting the meter data and transmitting them to utility server in China. Most of prepayment meter has the RS485 communication interface. Since the RS485 network can afford the AMR task, its reliability can also afford the prepayment data QoS requirements. RS485 AMR network has been set up in many area of China which promotes the advanced mobile prepaid solution developments.

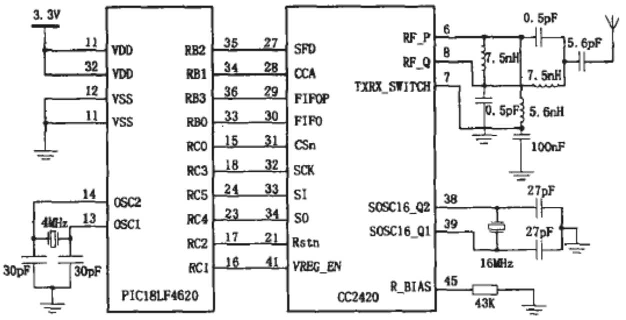

Fig. 14 Zigbee node schematic diagram

In response to the prepayment requirements, the meter with RS485 adaptable interface is designed (Fig. 15). S3C2410 is a high performance and low cost ARM9 Micro Control Unit (MCU) of Sumsung Company for meter. Its GPE0 pin conjoins with ESAM IO pin for data exchange and GPE4 pin conjoins with ESAM RST pin for resetting. 74HC08 aims to provide appropriate clock to ESAM. UART2 of S3C2410 conjoins with MAX13085 that is an RS485 chip of MAXIM Company. Meter can communicate with Prepayment-Center via RS485 bus, WPAN, WMAN and WWAN etc. In this way, PM doesn’t communicate with MPC directly. The solution adopts two phase commutation methods to complete a long prepayment transaction. Firstly, MPC commits prepayment information to PS with mutual authentication. Secondly, PS commits processed information to PM with mutual authentication. Each phase failed will lead to rollback the whole transaction. Considering the Qos of RS485 AMR network, the second phase can retry three times before failure.

We apply the safety access module (ESAM) in the meters. The important data and keyword which decides the system safety are saved in ESAM. The appliance of the hardware DES encryption technology makes the system safety, reliability and stability as a whole. At the same time it presents new safety approaches, compact the password length and supply the consumers and management agents with the convenient services. We apply the international up-to-date chips to ensure the calculating accuracy of the meters; apply anti-interfere and anti-ruin approaches to ensure the stability of the meters; preserve RS-485 port to be able to expand the function of telecommunication.

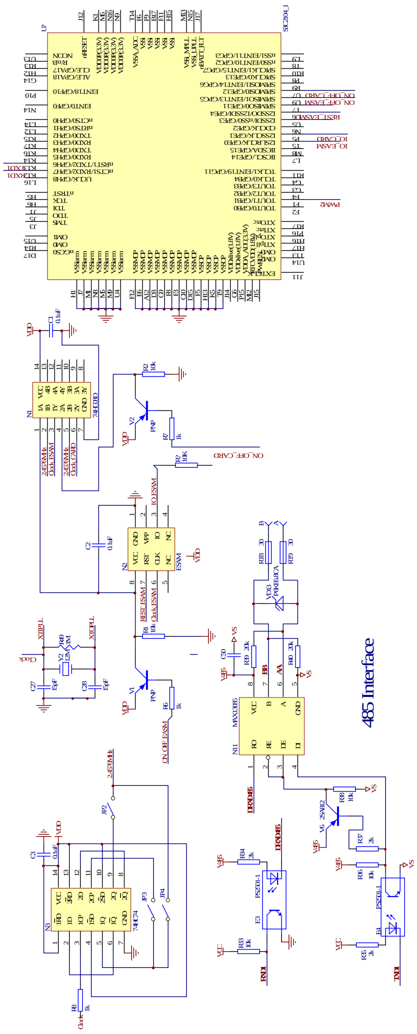

Fig. 15 meter with RS485 adaptable interface

The main program design is shown as fig. 16. The main function is described as follow:

Debug: it is for system debug and error information collection.

RCC_Configuration:System Clocks Configuration.

NVIC_Configuration:NVIC configuration.

SysTick_Config :SysTick configuration

GPIO_Configuration: Configure the GPIO ports

EXTI_Configuration:Configure the EXTI Controller

ESAM is a kind of smart card which is handled by function of SC_Handler. SC_Handler have six sub functions as follow.

SC_DeInit: Deinitializes all ressources used by the Smartcard interface.

SC_Init: Initializes all peripheral used for Smartcard interface.

SC_AnswerReq: Requests the reset answer from card.

SC_decode_Answer2reset: Decodes the Answer to reset received from card.

SC_Detect: Detects whether the Smartcard is present or not.

SC_SendData: Manages the Smartcard transport layer: send APDU (Application Protocol Data Unit) commands and receives the APDU response.

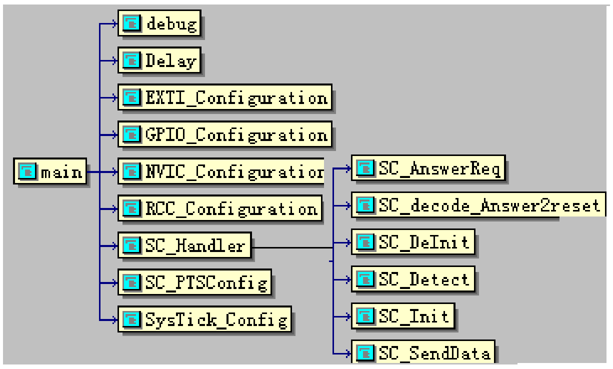

Fig. 16 main program structure

5 Conclusion

Given the interoperation between meter and server via Zigbee network and 3G cellular infrastructures feasible, there is a new way to solve the inconvenience of the typical meter prepayment system [9, 10]. In this paper, we have presented such a mobile prepayment solution that can be used for utility meter without going to the agency. Furthermore, we have shown the system integration project, prepayment process, hardware design and practical application.

In terms of future work, since WiMax radios are also eventually expected to appear in smaller devices, after initially finding their way into laptop-sized PCs, the analyst added. Wi-Fi trade association the Wi-fi Alliance said Wi-Fi is increasingly being added to mobiles, as having wireless and cellular radios offers advantages for both users and operators; the users get the best of both worlds and the carrier gets the best of the spectrum management. Key factors expected to shape handsets in the coming five years include the Apple iPhone, alternative networks such as Wi-Fi and WiMax, according to In-Stat. These coming changes will gradually developing the infrastructure of our solution in the future. WiMax will take the place of 3G providing wider band for long range data transmit because the transmitting distance of utility meter data is always in the range of a city, even take the place of the short range network access of WiMax in the new building of the modern residential area. At the same time, there is a need to provide united mobile adaptable interface which connect to family network gateway in particular that will allow us to better show the applicability of our solution to a wide variety of application domains. In addition, the use of actuators will eventually improve the development of our mobile prepayment solution.

References:

[1] Smit, Daniel, Electronic meter reader system and method [P], U.S.: 489217, January 20, 2005.

[2]Muhammad Sher and Thomas Magedanz, Network Access Security Management (NASM) Model or Next Generation Mobile Telecommunication Networks, in Proc. of MATA 2005, 2005, pp. 263-272.

[3]Muhammad Sher and Thomas Magedanz, Network Access Security Management (NASM) Model for Next Generation Mobile Telecommunication Networks, in Proc. of MATA 2005, 2005, pp. 263-272.

[4] Baris Kayayurt and Tugkan Tuglular, End-to-end security implementation for mobile devices using TLS protocol, Journal in Computer Virology, Vol.2, No.1, 2006, pp. 87-97.

[5]Vijayalakshmi Atluri and Heechang Shin, Efficient Enforcement of Security Policies Based on Tracking of Mobile Users, in Proc. of 20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, 2006, pp. 237-251.

[6]H. Lee, J. Alves-Foss, and S. Harrison, The use of encrypted functions for mobile agent security, in Proc. 37th Annual Hawaii International Conference on System Sciences (HICSS'04), Big Island, Hawaii, 2004.

[7]G. Cabri, L. Leonardi, and F. Zambonelli, Engineering mobile agent applications via context-dependent coordination, IEEE Trans. on Software Engineering 28(11) (2002),pp. 1040-1056.

[8]S. T. Vuong and P. Fu, A security architecture and design for mobile intelligent agent systems, ACM SIGAPP Applied Computing Review 9(3) 2001, pp. 21-30.

[9]S. Guan, T. Wang and S. Ong, Migration control for mobile agents based on passport and visa, Future Generation Computer Systems 19(2) (2003), pp.173-186.

[10]A. L. Murphy, G. P. Picco, and G.-C. Roman, LIME: A middleware for physical and logical mobility, in Proc. 21st Int. Conf. on Distributed Computing Systems (ICDCS-21), April 2001, Phoenix, Arizona, pp. 524-533.