Mobile Prepayment Solution for Meter based on New Generation Communication

PAN Tie-Jun, ZHENG Lei-na, FANG Cheng-bin, ZHANG Hua-jun, JIN Jian-suai, WU Gui-yang
Department of Computer and Information
ZheJiang WanLi University
NingBo 315100
China
http://www.zwu.edu.cn

Abstract: - We 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 and the 3rd generation wireless communication infrastructure (3G) and utility meter may connect Zigbee node via RS485 bus. By means of identification and mutual authentication which generating different session key with time stamp every time, the cross validation mechanism based on PKI 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, data integrity and data confidentiality. The result of the present work implied that mobile phone is gradually becoming a data access and exchange platform of mobile payment. It will be an important role in mobile prepayment meter system.

Key-Words: - mobile payment; OTA; Zigbee; SIM; 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. 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]

2 Mobile Prepayment Solution

Zigbee Network is suitable for short distance 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.

2.1 Zigbee Network

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. 1. Obviously, ZigBee node is also responsible for data collection without RS485 bus.

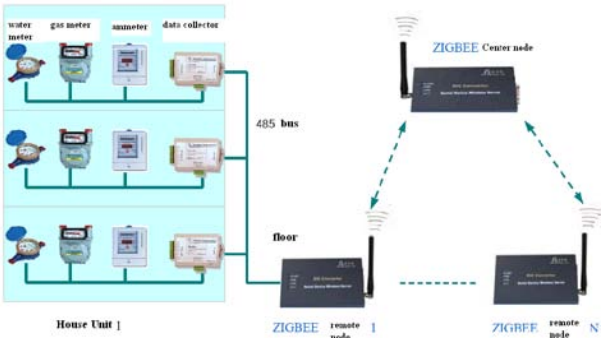

Fig. 1 Zigbee network with RS485 bus

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).

2.2 3G Network

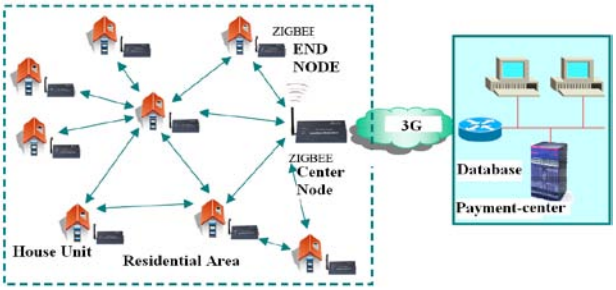

Fig. 2 AMRS based on 3G and Zigbee network

Zigbee 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. Then it is an important problem to transfer data to remote Payment-center.

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. 2.

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.3.

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.

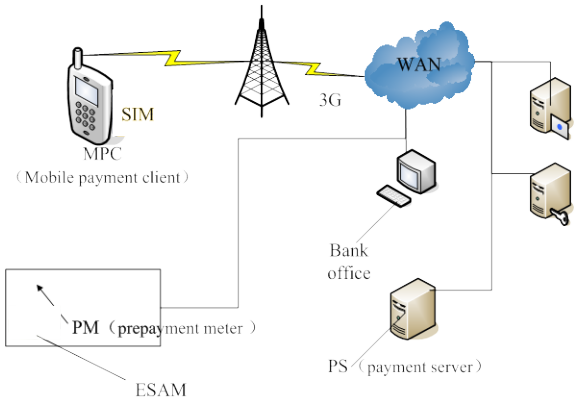

Fig. 3 Mobile Prepayment Solution Network

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 eKey and web server etc. 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:

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. 4). 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.

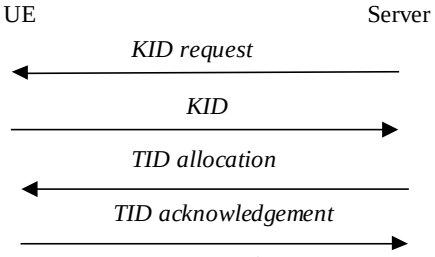

Fig.4. User confidentiality

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. 5). 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.

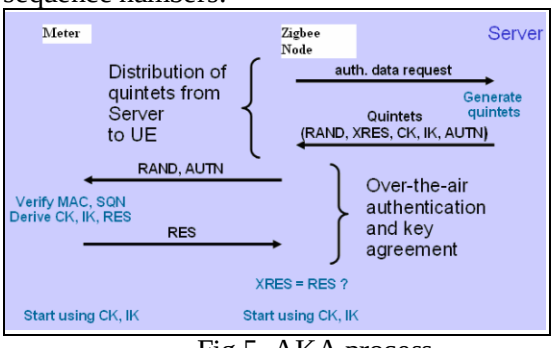

Fig.5. AKA process

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. 6.

Generation of authentication data in meter is shown as Fig. 7.

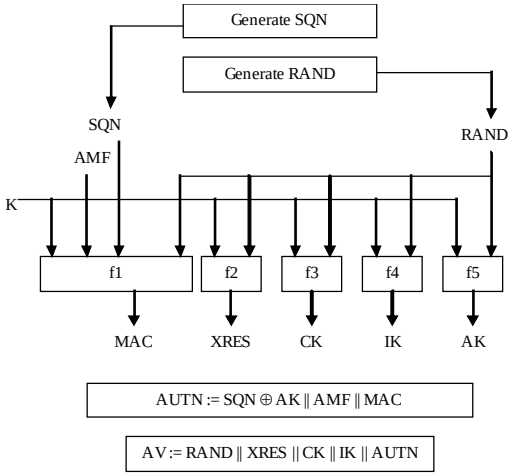

Fig.6. Generation of authentication data at server

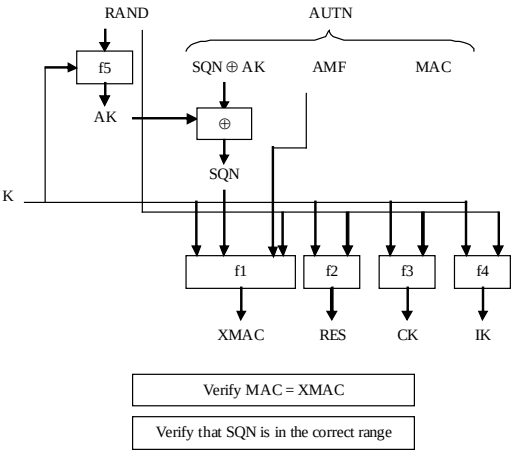

Fig.7. Generation of authentication data in meter

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.8).

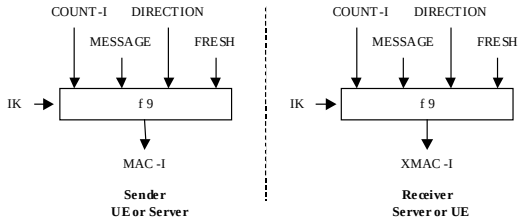

Fig.8. Data integrity

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.9).

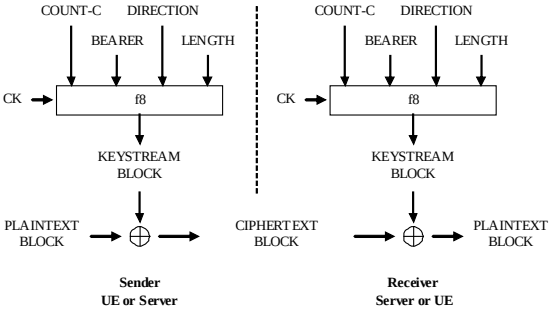

Fig.9. Data confidentiality

4 Conclusion

Given the interoperation between meter and server via Zigbee network and 3G cellular infrastructure 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 prepayment process and hardware design, a practical application.

In terms of future work, there is a need to provide mobile prepayment 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.