A secure mobile payment system*

LI Xi, HU Han-ping

(Institute of Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: The considerable increase of mobile device users in recent years causes a strong demand on secured wireless information services and reliable mobile commerce (m-commerce) applications. Since mobile payment (m-payment) is a critical part of most wireless information services and mobile commerce applications, how to build secured m-payment systems becomes a research hotspot. This paper presents an effective Mobile Payment System (MPS) in wireless insecure environments using mobile devices. The proposed framework provides a secure and convenient payment mechanism. Moreover, the mobile payment protocol and the security solution of the MPS are described. At last application examples are given to demonstrate the functions and feasibility of this system.

Key words: m-commerce; m-payment; MPS; m-payment protocol; MPS security

1. Introduction

The widespread adoption of digital mobile devices has paved the way for the development of many innovative applications. Among them, one intriguing possibility is to use mobile devices for m-commerce purpose. As a critical component in m-commerce applications, m-payment on mobile devices will provide excellent business opportunities in the coming years. Therefore, developing secure and cost-effective wireless solutions to support mobile device users not only provides good business opportunities, but also brings new technical challenges and issues to engineers. In recent years, there are a number of papers discussing business markets, payment process, payment methods and standards in m-payment[1-4]. However, few discuss how to build m-payment systems, including protocols, design issues and security solutions[5-8]. This paper reports current research efforts on building an m-payment system. Furthermore, the security solution of MPS is integrated with the m-payment protocol.

This paper is structured as follows. Section 2 reviews related work on m-payments. Section 3 presents design of the system, including architecture, processes, as well as used technologies. Section 4 introduces the m-payment protocol. The security solutions are described in section 5. Section 6 presents application examples of MPS. Finally, conclusions and future work are included in section 7.

2. Background and Related Work

M-payment is payment in which one part of the transaction is conducted by using a mobile device (such as a mobile phone, smart phone, and personal digital assistant) over a mobile telecommunications network, or via various wireless technologies. In general, m-payment systems can be used by wireless-based merchants, mobile content vendors, and wireless information and commerce service providers to process and support payment transactions driven from wireless-based commerce applications. This would include wireless-based trading systems, mobile portals, wireless information and commerce service applications[9].

Many mobile payments are somewhat determined by regional differences and individual market dynamics. For example, in Japan, the success of mobile Internet services can be attributed to the high concentration of

* Acknowledgements: This work is supported by the Foundation of Science and Technology of Huawei of China (No. YJCB2006046MT).

LI Xi (1981-), female, Ph.D. candidate; main research field: information security; E-mail: lixi13@tom.com.

HU Han-ping (1960-), male, Ph.D., professor; main research fields: information security and artificial intelligence.

populations in urban areas, long commute times, consumers comfort with small electronic devices, and the lack of a ubiquitous fixed-line Internet infrastructure. In Europe, mobile top-up for prepaid phone services is popular. In individual markets in Asia-pacific, Europe and U.S., there is a drive to implement proximity payments in environments such as road-tolling, fast-food drive-through, and service stations. Despite the regional variations, there is a shared requirement for payment to be secure, interoperable and easy to use.

As discussed in reference [6], existing m-payments can be classified into three methods.

The first one is an alternative payment method on the Internet. By giving a cell phone number, users can use their phone to complete their transactions and be charged on their mobile carrier phone bill. The main advantages are that it is a fast method giving the opportunity to consumers to pay without a credit card and it does not require that the merchant invest in any special component or equipment. A disadvantage is that only fixed amount of money can be transferred, in order to be charged on the mobile phone carrier bill.

The second method of mobile payment is to pay at a POS (point of sale) with a mobile phone. Consumers must synchronize with the merchant system to complete a transaction. An advantage of this method is that it is useful for micro-payments. When consumers do not have coins available, they can buy goods with their mobile phone. A disadvantage is that most of the applications require a mobile phone modification and the installation of a device in the merchant payment system.

The third one is payment for mobile commerce applications. In this method of mobile payment, user chooses what he/she wants to buy and conducts the transaction with a secure mobile payment system. The main advantage of this method is that consumers can pay at anytime, anywhere. A disadvantage is that the current mobile phone technology is not 100% appropriate to mobile commerce. With the third generation of mobile phones and the development of wireless technologies, mobile payment solutions will likely gain a significant market share.

3. The Architecture of Mobile Payment System

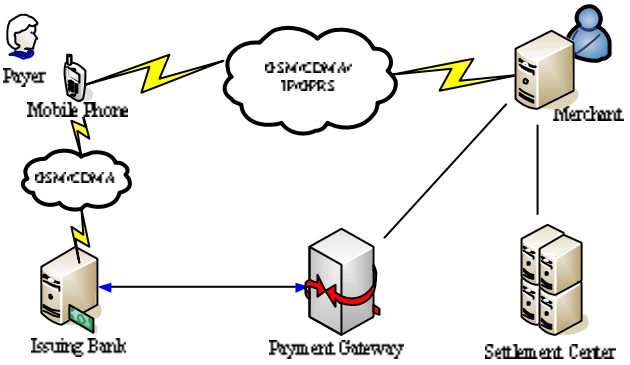


Fig. 1 The architecture of mobile payment system

In the proposed framework, as shown in Fig. 1, the main entities of MPS are the payer, the network operator, merchant, the payment gateway, the issuing bank and the settlement center.

The application is installed into the SIM card of mobile phone and implemented with the SMS technology. The complete application functionality for the payment is provided on the SIM. Certainly the interoperability between SIM card and terminals is achieved through Global Platform standards [10].The application installation and personalization on the phone's SIM will be done Over-The-Air (OTA). The merchant server works with an application by communicating with the payer and the payment gateway. After accepting the payment information from the mobile phone over the wireless network, the merchant server sends a payment request to the issuing bank over the payment gateway. The issuing bank accepts the payment request and verifies its validity and authenticity. Also the system checks the payer's account for efficient balance. None but all information of the payment message is right as well as having enough fund, the issuing bank will perform the transaction. Otherwise the transaction cannot be

completed and the message with fault information will be sent both to the payer and the merchant. Based on all confirmed transactions of previous day, clearing and settlement process is done between banks periodically.

4. Mobile Payment Protocol

In the scenario where the service provider initiates the transaction, for example, at the beginning of the m-payment process, the transaction details should have been presented to the consumer, stating minimum details such as service provider identifier, order serial number, transaction amount and currency. The presentment interaction may be voice-based or visual (e.g. Internet or WAP). This paper supposes the payer has made an order from the merchant and has received the information described as above.

4.1 Mobile payment protocol

The purpose of designing the protocol is to provide a convenient, secure and brief protocol for supporting m-payment transactions. The m-payment protocol can be divided into two parts: session key generation protocol and payment transaction protocol.

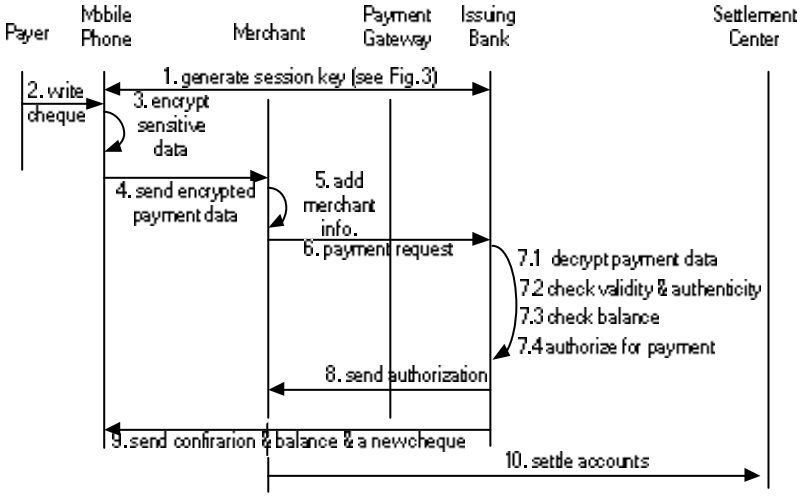


Fig. 2 M-payment transaction protocol

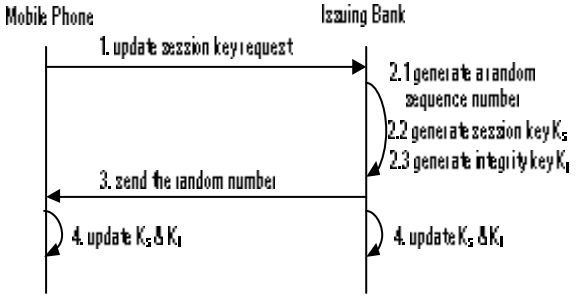


Fig. 3 Session key generation protocol

Fig. 2 encapsulates the m-payment transaction sequence in MPS. It mainly involves ten steps:

(1) The mobile phone and the issuing bank generate the share session key which is used for encrypting/decrypting data generated for each session. Fig. 3 explains more on the key generation.

(2) The payer inputs the payment information.

(3) Sensitive data are encrypted, such as the payer's account, payment password and so on.

(4) The mobile phone sends the message with the encrypted payment data to the merchant.

(5) In the payment transaction the merchant information about the account is necessary. So the merchant has to add the acquiring bank ID and the acquiring account info to the message before requesting for the payment.

(6) The m-payment message is sent to the issuing bank over the payment gateway.

(7) After decrypting the payment data, the issuing bank verifies its validity and authenticity. At the same time the system checks the sufficiency of the payer's

balance. None but all information of the payment message is right, as well as has enough money, the issuing bank will perform the transaction.

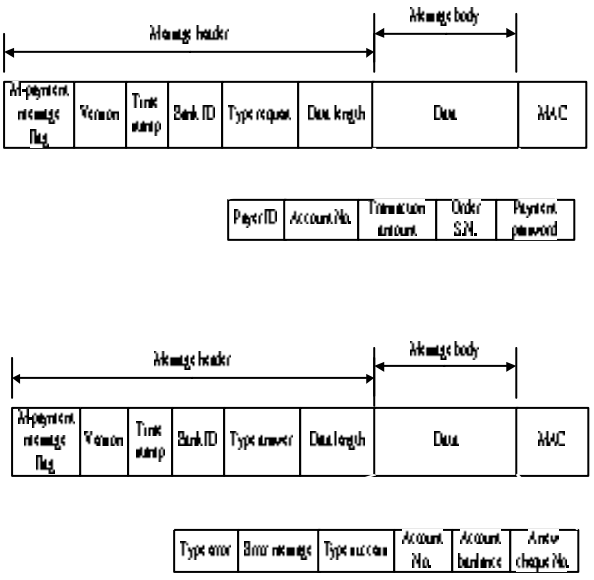
(8) The issuing bank sends the authorization for payment to the merchant over the payment gateway.

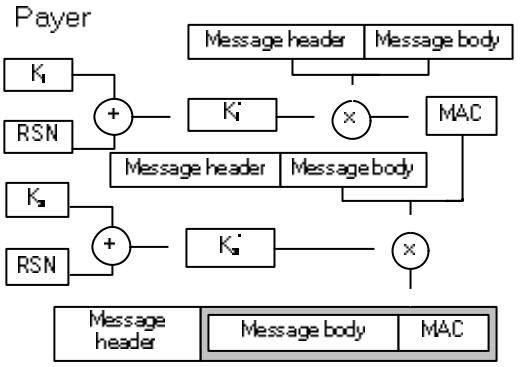
(9) The payment transaction result is sent to the payer. Additionally, the account balance and a new cheque are involved if the transaction is successful.

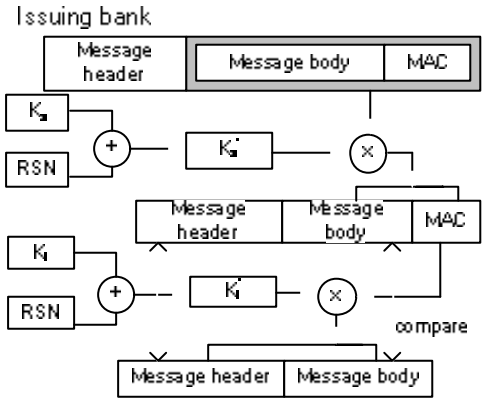
(10) Periodically, clearing and settlement process is done between banks based on all confirmed transactions of previous day.

Fig. 3 shows the session key generation procedure in MPS. Before operating on the payment functions, the mobile phone and the issuing bank have already generated the session key K_s and the integrity key K_i, both of which are generated offline by a Random Sequence Number (RSN) shared by them. The procedure is at the background and invisible to the payer.

4.2 Message format of mobile payment







concerned, the principal security requirements for successful m-payments are: authentication, confidentiality, data integrity, non-repudiation and usability. GSM provides a basic range of security features to ensure adequate protection for both the operator and the customer[11]. However, business cases should show the effect of fraud and the costs of protection. The core process for MPS security can be categorized as follows:

(1) Registration for the payment service: typically, the mobile phone is a device that is sold by a phone company or its agents, and is not packaged with applications such as payments. To use the payment service, a user would likely be needed to perform a registration.

(2) Secure mechanisms: secure electronic digital signature, session key and presentment of completion of transaction.

In this proposed framework, the SIM of a phone supports GSM 03.48 security[11]. Key updating with each session supports the confidentiality. The session key is generated offline by the last time session key and a random sequence number. All the secret data created in the data preparation process is encrypted under the session key shared with the phone, and the issuer and the data sent to the issuer is MACed for data integrity.

Furthermore, PKI provides the authorization and non-repudiation properties. X.509 digital certificate is used on the merchant terminal for non-repudiation of the transaction[12].

The message encryption and decryption mechanisms as shown in Fig. 6 and Fig. 7 respectively are designed to provide the desired security properties in an insecure pervasive communication environment.

6. Application Examples

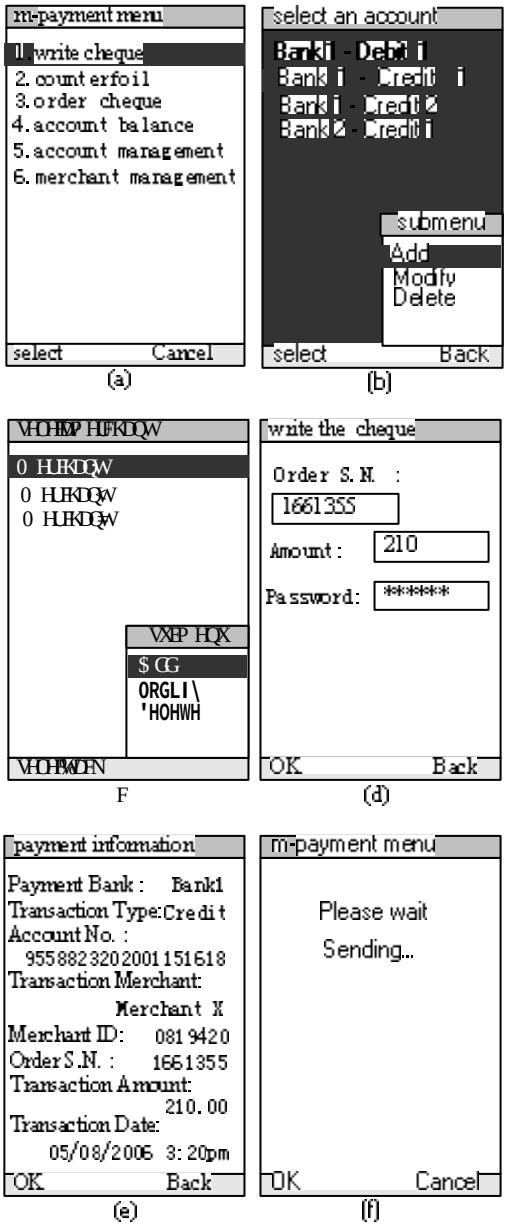


Fig. 8 Mobile payment system scenarios

Fig. 8 shows MPS for mobile payer to perform payment transactions and management. They are described as follows:

(1) Main menu: after successfully making an order, the payer begins to pay for it. If the payer uses MPS for the first time, the normal payment accounts and the ID of the familiar merchants may be input into the mobile by the submenu of account management and merchant management respectively.

(2) The payer needs to select a bank with an account which has already existed in the mobile phone. Note that if there is no bank or the account that the payer wants to use, the payer is able to add them by submenu. In a single mobile phone, multiple debit and/or credit accounts from different banks can be configured without compromising security.

(3) The payer needs to select the right merchant. Each merchant has an only ID which the payer has input into the mobile phone.

(4) The payer needs to input the order serial number, transaction amount and the payment account password.

(5) Confirm: the payer overviews the whole detailed description of this payment transaction.

(6) Make a payment: after the payer confirms the transaction, the mobile phone sends the message to the merchant.

7. Conclusions and Future Work

This paper presents a secure mobile payment system, which support mobile phone users to pay any merchant who has a wireless terminal. This paper introduces the system architecture, design, payment protocol, and security strategy. Moreover, application examples of the prototype are presented.

There is enormous potential for mobile payment as it saves huge operational load and also deployment cost, for it does not require any huge investment on terminal infrastructure. The proposed framework can support and process transactions for e-commerce, m-commerce and proximity commerce payments. Moreover, this can be further utilized into remote payments (e.g. Internet, faceless payments and card-not-present payments) and local payments (over-the-counter payments). However, there are considerable hurdles to be overcome before ubiquitous and easy-to-use payment on a mobile device become reality.

References:

[1] Jean-Michel Sahut and Malgorzata Galuszewska. Electronic payment market: A non-optimal equilibrium. *Proceedings of the 2004 International Symposium on Applications and the Internet Workshops* (*SAINTW'04*), 2004: 3-8.

[2] Antovski, L. and Gusev, M. M-payments. *Proceedings of the 25th International Conference Information Technology Interfaces* (*ITI'03*), 2003: 95-100.

[3] Agnieszka Zmijewska. Evaluating wireless technologies in mobile payments—A customer centric approach. *Proceedings of the International Conference on Mobile Business* (*ICMB'05*), 2005: 354-362.

[4] Ondrus, J. and Pigneur, Y. A disruption analysis in the mobile payment market. *Proceedings of the 38th Hawaii International Conference on System Sciences* (*HICSS-38'05*), 2005: 84c-84c.

[5] Ashutosh Saxena, Manik Lal Das and Anurag Gupta, MMPS: A versatile mobile-to-mobile payment system. *Proceedings of the International Conference on Mobile Business* (*ICMB'05*), 2005: 400-405.

[6] Delic, N. and Vukasinovic, Ana. Mobile payment solution-symbiosis between banks, application service providers and mobile network operators. *Proceedings of the Third International Conference on Information Technology: New Generations* (*ITNG'06*), 2006: 346-350.

[7] Ondrus, J., Camponovo, G., Pigneur, Y. A proposal for a multi-perspective analysis of the mobile payment environment. *Proceedings of the International Conference on Mobile Business* (*ICMB'05*), 2005: 659-662.

[8] Nambiar, S. and CHANG T. L. M-payment solutions and m-commerce fraud management. Available at: http://europa.nvc.cs.vt.edu/~ctlu/Publication/M-Payment-Solutions.pdf. Accessed September 9, 2004.

[9] GAO J., Edunuru, K., CAI J., Shim, S. P2P-paid: A peer-to-peer wireless payment system. *Proceedings of the Second IEEE International Workshop on Mobile Commerce and Services* (*WMCS'05*), 2005: 102-111.

[10] Global platform. Available at: http://www.globalplatform.org.

[11] GSM. Available at: http://www.gsmworld.com/technology.

[12] Public-key infrastructure (X.509). Available at: www.ietf.org/html.charters/pkix-charter.html.

(Edited by Susan, Candy)