World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:2, No:11, 2008

Privacy in New Mobile Payment Protocol

Tan Soo Fun, Leau Yu Beng, Rozaini Roslan, and Habeeb Saleh Habeeb

Abstract**—**The increasing development of wireless networks and the widespread popularity of handheld devices such as Personal Digital Assistants (PDAs), mobile phones and wireless tablets represents an incredible opportunity to enable mobile devices as a universal payment method, involving daily financial transactions. Unfortunately, some issues hampering the widespread acceptance of mobile payment such as accountability properties, privacy protection, limitation of wireless network and mobile device. Recently, many public-key cryptography based mobile payment protocol have been proposed. However, limited capabilities of mobile devices and wireless networks make these protocols are unsuitable for mobile network. Moreover, these protocols were designed to preserve traditional flow of payment data, which is vulnerable to attack and increase the user's risk. In this paper, we propose a private mobile payment protocol which based on client centric model and by employing symmetric key operations. The proposed mobile payment protocol not only minimizes the computational operations and communication passes between the engaging parties, but also achieves a completely privacy protection for the payer. The future work will concentrate on improving the verification solution to support mobile user authentication and authorization for mobile payment transactions.

Keywords**—**Mobile Network Operator, Mobile payment protocol, Privacy, Symmetric key.

I. Introduction

THIS mobile payment is defined as any transaction that is carried out via mobile device, involves either direct or indirect exchange of monetary values between parties [5], [13], [6]. An interesting aspect about mobile payment is that mobile phone can be used as payment device for all types of payment situations. Optimists are of the opinion that the new world economy will witness the transition of mobile devices from a simple communication device to a payments mechanism [10].

Currently, several mobile payment protocols were proposed, however, most of them are based on public key infrastructure (PKI) which are inefficiently applied to wireless networks [14], [7], [8], [2]. Some of them are keep information about the engaging parties' credit card is either stored on their mobile devices or used in the transaction without protection, which makes it vulnerable to attack [9], [7], [8]. Most of these payment protocols were designed to preserve the traditional flow of payment data (Client - Merchant - Merchant's Bank), [11], [2], [7], [9] that is transaction are carried out between client and merchant. Therefore, it is vulnerable to attacks like transaction or balance modification by merchant and increase the user's risk which their credit or debit cards can be captured and used later to access a customer account without authorization. Besides that, there is no notification to the client from the client's bank after the successful transfer. The user has to check his/her balance after logging on to his/her bank's website again [15].

Furthermore, some mobile payment protocol design schemes are not concerned about the customer privacy issues [14], [9], [7], [8]. The customer privacy such as customer identity and transaction details is revealed not only to merchant, but also to the payment gateway and the banks [3].

By addressing these problems, the research objective is to create a private mobile payment protocol by involving mobile network operator which employing symmetric key operations. The rest of this paper is organized as follows. Some existing mobile payment protocols are briefly explained in section II. Section III details our new protocol for mobile payment and followed by the comparison on privacy protection among several existing mobile payment protocol with our proposed protocol in section IV. Finally, section V concludes this research.

II. Related Work

In this section, several existing payment protocols will be delved. In general, these payment protocols composed of five principals, including client (C), merchant (M), issuer (client's financial institution), acquire (merchant's financial institution and payment gateway (PG) which acts as medium between them and both client and merchant for clearing purpose. Three primitive payment transactions have occurred within these payment protocols [1] as below:

1) *Payment*:
   Client makes a payment to merchant
2) *Value Subtraction*:
   Client requests issuers or payment gateway to debit his account.
3) *Value Claim*:
   Merchant requests acquirer or payment gateway to credit transaction amount into his account.

Manuscript received March 16, 2008.

Tan Soo Fun is with the School of Informatics Science in Universiti Malaysia Sabah, Labuan International Campus, 87000 Labuan F. T., Malaysia (e-mail: soofun4818@yahoo.com).

Leau Yu Beng is with the School of Informatics Science in Universiti Malaysia Sabah, Labuan International Campus, 87000 Labuan F. T., Malaysia (e-mail: leauyubeng@gmail.com).

Rozaini Roslan is with the School of Informatics Science in Universiti Malaysia Sabah, Labuan International Campus, 87000 Labuan F. T., Malaysia (e-mail: rozaini@ums.edu.my).

Habeeb Saleh Habeeb is with the Saudi Stock Exchange (Tadawul), NCCI Building, North Tower, King Fahd Rd., P. O. Box 60612, Riyadh 11555, Kingdom of Saudi Arabia (e-mail: habeeb.habeeb@tadawul.com.sa).

A. Secure Electronic Transaction (SET) Protocol

The SET protocol is the well-known credit card payment protocol, which consists of request/response message pairs. All principals in SET payment protocol are required to obtain public key certificates. The SET protocol consists of five transaction steps, which is payment initialization, purchase order, authorization, capture payment and card inquiry phase [8], [11], [4].

B. Internet Key Protocol (iKP)

The *i*KP protocols are based on public key cryptography and differ from each other based on the number of principal those posses their own public key pairs. This number indicated by the name of the individual protocols: 1KP, 2KP and 3KP. The greater number of principals that hold public-key pairs, the greater the level of security provided. The principal of *i*KP are including customer, merchant and payment gateway (acquirer) [8], [11], [2].

C. KSL Payment Protocol

The SET and *i*KP payment protocols are well-established payment protocols, which are successfully implemented for electronic commerce in fixed network such as Internet. However, Tellez *et al*. [14] and Kungpisdan *et al*. [7] argued that both payment protocols are inapplicable for mobile payment transaction in wireless network due to theirs heavy computational operations and communication passes. Kungpisdan *et al*. [7] enhanced SET and *i*KP payment protocol by reduce the number of principals who posses own public key pairs. All principals except client are required to have their own certificates. Hence, the client's computation is reduced. The KSL payment protocol consists of two sub-protocols, which are merchant registration protocol and payment protocol. Both client and issuer shared Y_i. Before starts making payment, client is required register with merchant and sends generated share symmetric key X_i with merchant.

D. Tellez et al. Anonymous Payment Protocol

Tellez *et al*. [14] proposed anonymous payment protocols based on client centric model, which employs a digital signature scheme with message recovery using self-certified public keys. It consists of five principals, which including client, merchant, acquirer, issuer and payment gateway. This payment protocol also consists of two-sub protocols, which are merchant registration protocol and payment protocol.

E. Kungpisdan's et al. Mobile Payment Protocol

Kungpisdan *et al.* [9] proposed another secure account based mobile payment protocol to enhance his KSL protocol [7]. This payment protocol is employing symmetric key operations which require lower computation at all engaging parties. In general, there are five principals involved in this protocol, which are client, merchant, issuer, acquirer and payment gateway. Kungpisdan *et al.* protocol is composed of two-sub protocols, which is merchant registration protocol and payment protocol. Before starts making payment, client is required register with merchant by running merchant registration protocol. After completion of registration protocol, client and merchant share a set of secret key X_i. The client also shared secret Y_i with issuer and secret Z_j is shared between merchant and payment gateway.

III. Proposed Protocol

To protect payer privacy and resolve the problem of traditional flow of payment data, the proposed mobile payment protocol is designed based on client centric model, where the payee does not have a direct communications with payer's MNO and transaction flow is completely control by the Payer. The proposed mobile payment protocol is composed of four principals, including payer, payee, payer's MNO and payee's MNO. The proposed protocol is working well with the assurance secret X_i, where i = 1,…,n is only shared between payer and payer's MNO and secret Y_i is only shared between payee and payee's MNO. The following symbols are used in proposed mobile payment protocol:-

TABLE I
NOTATIONS

Symbol	Description
{Payee, Payer, Payee's MNO, Payer's MNO}	A set of engaging parties, which are Payee, Payer, Payee's MNO, and Payer's MNO repestively.
TSC	Time Stamp Center
PN_P	Phone Number of Party *P*
PIN_P	Party *P* selected password identification number
ID_P	Identity of Party *P*, which identifies Party *P* to *MNO*; computed as $ID_P = PN_P + H(PN_P, PIN_P)$
AI_P	Account Information of Party *P*, which including credit limit for each transaction and type of account (post-paid or prepaid account)
NONCE	Random Number and timestamp generated to protect against replay attack, that is ensure old communication cannot reused in replay attack.
R	Random Number and timestamp generated by Payer act as Payer's pseudo-ID, which uniquely identifies Payer to Payee
DATE	Date of payment execution
AMOUNT	Payment transaction amount and currency
DESC	Payment Description, which may includes delivery address, purchase order details and so on. Payer will include only the information that he/she wish to disclosure to Payee.
TID	The Identity of transaction
TID_{Req}	The request for *TID*
$PayeeID_{Req}$	The request for payee identity.
{M}X	The message M symmetrically encrypted with shared key X.
H(M)	The one way hash function of the message *M*

i	Used to identify the current session key of X_i and Y_i
$K_{P\text{-}P}$	The secret key shared between Payer's MNO and Payee's MNO.
Success/Failed	The status of registration, whether success or failed
Yes/No	The status of transaction, whether approved or rejected
Received	Payment receivable update status, which may includes the received payment amount

The proposed mobile payment protocol consists of two-sub protocols, which are registration protocol and payment protocol. Both payer and payee are required to register with their own mobile network operator (MNO) before any transaction could take place. Payer and payer's MNO generate session key, K_1 by running Diffie-Hellman Key Agreement protocol. Then payer sends registration details such as account information, payer identity and phone number, encrypted with session key K_1 to payer's MNO.

Payer→Payer's MNO: $\{PN_{Payer}, ID_{Payer,} AI_{payer}\}K_1$

During the registration process, payer is required to set his password identification number, $PIN_{payer,}$ for later access to his mobile wallet application. This implementation uses of two-factor authentication, that is an important principle for physical and mobile devices access control [12]. The two-factor authentication applies two means to authenticate users to access the mobile wallet system, that is mobile device with mobile wallet application (something he has) and password (something he know only). Then the $ID_{payer,}$ is computed by hashing the PN_{Payer} and PIN_{payer}.

$$ID_{Payer} = PN_{Payer} + H\,(PN_{Payer}, PIN_{Payer})$$

Payer's MNO decrypts message with shared session key, K_1 to retrieve payer's information. Payer's MNO stores required information into their database. If registration process is successful, payer's MNO sends confirmation message to inform payer. The confirmation message is encrypted with the session key K_1.

Payer's MNO→Payer: $\{Success/\ Failed\}K_1$

After registration process, payer receives mobile wallet application through email or downloading from payer's MNO site. The mobile wallet application contains symmetric key generation and payment software. After installed successfully, a set of symmetric key $X = \{X_1, X_2, \ldots, X_n\}$ is generated, store into payer's mobile devices and send to payer's MNO. Similarly, payee must go through the similar registration process with his/her MNO that enable his/her to receive payment from payer. The payee generates a set of symmetric key $Y = \{Y_1, Y_2, \ldots..Y_n\}$ with payee's MNO and store into his/her terminal and MNO database.

The proposed payment protocol consists of seven phases as illustrates in Fig. 1.

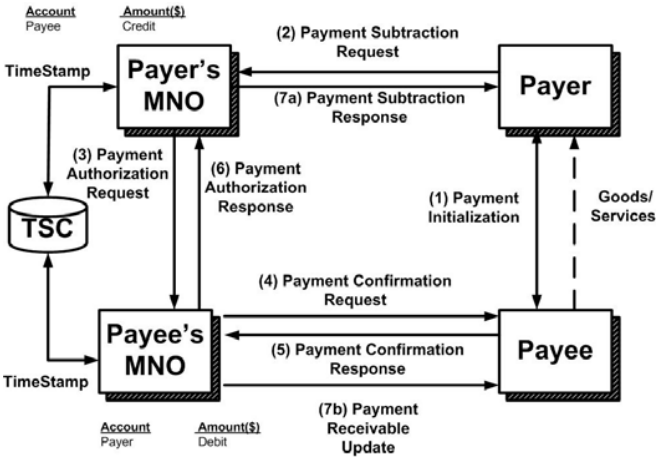

Fig. 1 Proposed mobile payment protocol

***Phase 1 Payment Initialization*:**
Payer → Payee: $R, TID_{Req}, PayeeID_{Req}$
Payee → Payer: $\{ ID_{Payee}, TID, ID_{MNO} \}K_2$

***Phase 2 Payment Subtraction Request*:**
Payer → Payer's MNO: $\{ ID_{Payee}, ID_{MNO}, R, TID, AMOUNT, DATE, NONCE, H(ID_{Payee}, ID_{MNO}, R, TID, AMOUNT, DATE, NONCE), \{R, DESC\}K_2 \}X_i, i, ID_{payer}$
Payer's MNO → TSC: $H[\{ID_{Payee}, ID_{MNO}, R, TID, AMOUNT, DATE, NONCE, H(ID_{Payee}, ID_{MNO}, R, TID, AMOUNT, DATE, NONCE), \{R, DESC\} K_2 \}X_i, i, ID_{payer}]$
TSC → Payer's MNO: *TimeStamp1*

***Phase 3 Payment Authorization Request*:**
Payer's MNO → Payee's MNO: $R, ID_{Payee,} TID, AMOUNT, DATE, \{R, DESC\}K_2$

***Phase 4 Payment Confirmation Request*:**
Payee's MNO → Payee: $\{R, TID, AMOUNT, DATE, \{R, DESC\}K_2, NONCE, H(R, TID, AMOUNT, DATE \{R, DESC\}K_2, NONCE), H(K_{P\text{-}P}) \}Y_i, i$

***Phase 5 Payment Confirmation Response*:**
Payee → Payee's MNO: $\{Yes/No, NONCE, H(K_{P\text{-}P}), H(R, TID, AMOUNT, DATE, \{R, DESC\}K_2, NONCE), \{Yes/No, TID, AMOUNT, DATE\} K_2\}Y_{i+1}$

***Phase 6 Payment Authorization Response*:**
Payee's MNO → TSC: $H(\{ Yes/No, NONCE, H(K_{P\text{-}P}), H(R, TID, AMOUNT, DATE, \{R, DESC\}K_2, NONCE), \{Yes/No, TID, AMOUNT, DATE\} K_2\}Y_{i+1})$
TSC → Payee's MNO: *TimeStamp2*
Payee's MNO → Payer's MNO: $Yes/No, TID, AMOUNT, DATE, \{Yes/No, TID, AMOUNT, DATE\} K_2$

***Phase 7 Payment Subtraction Response*:**
Payer's MNO → Payer: $\{Yes/No, NONCE, H(K_{P\text{-}P}), H(ID_{Payee}, ID_{MNO}, R, TID, AMOUNT, DATE, NONCE), \{Yes/No, TID, AMOUNT, DATE\} K_2\}X_{i+1}$
Payee's MNO → Payee: $\{Received, NONCE, H(K_{P\text{-}P}), H(R, TID, AMOUNT, DATE, \{R, DESC\}K_2, NONCE) \}Y_{i+1}$

If all the transaction processes are successfully completed, payee will release or deliver the purchased goods or services to payer. To prevent replay of the secret key from payer and payee, both payer's MNO and payee's MNO make sure that the symmetric key X_i and Y_i have not been used before proceed the payment transaction. The MNO will maintain a list of generated secret key by discarding used or expired symmetric key X_i and Y_i from the list. If symmetric key X_i and Y_i were compromised, there must be revoked. Both payer and payee may receive an update notification from MNO when their key was expired. To update their secret key, they connect to their MNO to generate a new session key, K_1 by running Diffie-Hellman Agreement protocol. Then, offline generates a new set of secret key X and Y with a new session key K_1.

IV. Comparison on Privacy Protection

In this section, the proposed mobile payment protocol is comparing with five existing payment protocols from aspect privacy protection. The privacy protection is includes identity privacy protection and transaction privacy transaction. Table II presents comparison of privacy protections of proposed mobile payment protocol with five existing payment protocols.

TABLE II
Comparison on Privacy Protection

Payer's Privacy Protection	**SET**	***i*KP**	**KSL**	**Tellez *et al*.**	**Kung-pisdan *et al.***	**Proposed**
Identity Protection From Payee	No	No	No	Yes	No	Yes
Identity Protection From Eavesdropper	Yes	Yes	Yes	Yes	Yes	Yes
Transaction Privacy Protection From Eavesdropper	Yes	Yes	Yes	Yes	Yes	Yes
Transaction Privacy Protection From TTP or Related Financial Institution	No	No	No	No	No	Yes

Achievement of payer's privacy protection is one of the most significant security properties of the proposed mobile payment. Note that, five existing mobile payment protocols and proposed mobile payment protocol are provide basic privacy protection for payer, that is protecting payer's identity and transaction details from eavesdropper. However, only Tellez *et al*. protocol and proposed protocol achieve payer's identity protection from payee. In Tellez *et al*. protocol, payer (client) only reveals temporary identity or called Client's Nickname (NID_C) to Payee (merchant) when sending the request for the transaction identity. The proposed mobile payment protocol protects payer's identity by sending a random generated number, R, to payee when requesting the transaction identity from payee. R represents one-time payer's identity together with regarding transaction identity (TID) uniquely identifies payer to payee. This avoids revealing the real payer's identity (ID_{Payer}) to payee. The comparison results also shown that only the proposed mobile payment protocol provides the transactions privacy from trusted third party (TTP) or related financial institution. The payment subtraction request that sent from payer to payer's MNO consist the transaction details, which is $\{R, DESC\}K_2$. Note that, the transaction details such as which stock that payee interested or delivery address is protected from both payer's MNO and payee's MNO by encrypted with the payer and payee shared session key, K_2. Hence, only the corresponding payee can decrypts and retrieves the transaction details. Besides that, both payment subtraction request message and payment confirmation response message are applied a hash function before sending it to TSC. This prevents revealing of any payment transaction details to TCS. In the nutshell, after compared with five existing payment protocol as presented in literature review, only the proposed mobile payment protocol satisfies all privacy protection requirements.

V. Conclusion

Many mobile payment protocols have been presented today, but none of them has taken dominant position as yet. This paper is to suggest a more private mobile payment protocol by involving MNO. We applied client centric model, one time payer's identity and transaction details encrypted with the payer and payee shared session key in our payment protocol in order to achieves a completely privacy protection for the payer. Due to the time constraint, our work only serves to demonstrate a preliminary result in comparing the privacy protection with other existing mobile payment protocols.

References

[1] Abad-Peiro J. L., Asokan N., Steiner M. & Waidner M, "Designing a generic payment service", *IBM System Research Journal*, Vol.37(1), 1998, Pp. 72-88.

[2] Bellare, M., Garay, J., Hauser, R., Herzberg, A., Steiner, M., Tsudik, G., Van Herreweghen, E., and Waidner, M, "Design,Implementation, and Deployment of the *i*KP Secure Electronic Payment system", *IEEE Journal of Selected Areas in Communications*, 2000, pp. 611-627.

[3] C. Wang & H-f. Leung, "A Private and Efficient Mobile Payment Protocol", *London: Springer-Verlag*, LNAI, 2005, pp.1030-1035.

[4] http://www.setco.org/set_specifications.html

[5] Jun Liu, Jianxin Liao, Xiaomin Zhu, "A System Model and Protocol for Mobile Payment", *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'05)*, 2005.

[6] Krueger, M, *The future of M-Payments–business options and policy issues*, Seville. Spain, 2001.

[7] Kungpisdan, S., Srinivasan, B., and Phu Dung, L, "Lightweight Mobile Credit-Card Payment Protocol", *Berlin Heidelberg: Springer –Verlag*, 2003a, pp. 295-308.

[8] Kungpisdan, S., Srinivasan, B., and Phu Dung, L., "A Practical Framework for MobileSET Payment", *Proceedings of International E-Society Conference*, 2003b, pp. 321-328.

[9] Kungpisdan S., Srinivasan B., and Phu Dung Le, "A Secure Account-based Mobile Payment Protocol", *Proceedings of the International Conference on Information Technology: Coding and Computing,* Vol. 1, Las Vegas, USA, 2004a, pp. 35-39.

[10] M. Ding and C. Unnithan, *Mobile Payments (mPayments) -An Exploratory Study of Emerging Issues and Future Trends*, Deakin University, 2002.
[11] Mohony D.O., Peirce M. and Tewari Histesh, *Electronic Payment Systems for E-Commerce*, *Artech House*, United States of America, 2001.
[12] Panko R. R, *Corporate Computer and Network Security*, *Prentice Hall*, Upper Saddle River, New Jersey, 2004.
[13] Pousttchi, K, "Conditions for Acceptance and Usage of Mobile Payment Procedures", *Proceedings of the M-Business Conference*, 2003.
[14] Tellez J. & Sierra J, "Anonymous Payment in a Client Centric Model for Digital Ecosystem", *IEEE DEST*, 2007, pp. 422-427.
[15] Tiwari, A., Sanyal, S., Abraham, A., Knapskog, J. S. & Sanyal, S., "A Multi-factor Security Protocol for Wireless Payment-Secure Web Authentication Using Mobile Devices", *IADIS International Conference Applied Computing*, pp.160-167, 2007.