A Lightweight Agent-based Secure Mobile Payment Protocol Supporting Multiple Payments

Pensri Pukkasenung
Faculty of Information Science and Technology
Mahanakorn University of Technology
Bangkok, Thailand
pensri.puk@csit.rru.ac.th

Rongrooj Chokngramwong
Faculty of Information Science and Technology
Mahanakorn University of Technology
Bangkok, Thailand
roongroj@mut.ac.th

***Abstract*—Payment for goods and services on mobile devices via an agent-based mobile payment protocol is gaining popularity amidst today's fast-paced lifestyles. These protocols offer fast, easy, and secure services with global reach. However, existing mobile payment systems still have problems with performance and security. One of the main problems is the computation time, requiring long and complex calculation for data transmission. This paper proposed a new, secure and lightweight mobile payment protocol for making payments on mobile devices. This protocol supports not only the necessary security properties but also multiple payment types including chain payments.**

Keywords— Mobile Payment; Mobile Protocol; Mobile Payment Protocol; Multiple Payments

I. INTRODUCTION

Mobile payment, also referred to as mobile money, mobile money transfer, or mobile wallet, is payment service operated under financial regulations and performed via mobile devices. Instead of making payments by cash, checks, or credit cards, a consumer uses a mobile device to pay for a wide range of services, including digital or hard goods [1]. Nowadays, mobile payments have been improved in supporting various payment scenarios based on security and performance requirements. This section presents three concepts of mobile payment.

A. The Relationship between a Payer and Payee

For a payment system, there are three types of payer-payee payment relationships. The details of them are shown below:

- *Simple Payment*: A customer sends a single payment to a single merchant. For example, the customer has one telephone bill to pay at the payment counter. The relationship between the customer and merchant is a one-to-one relationship $(1:1)$. In this scenario, there is one transaction in the payment system on the client side and one on the merchant side. This is so called a traditional type of payment. This relationship is depicted in Fig. 1(a).
- *Parallel Payment*: A customer sends a single parallel payment to multiple merchants by making more-than-one payments depending on the number of merchants. For example, a customer pays for goods and services received from several merchants with multiple payments. The relationship between the customer and merchant is one-to-many $(1:m)$. In this scenario, there are many transactions in the payment system on the client side. This relationship is depicted in Fig. 1(b).
- *Chain Payment*: A customer sends a single payment request to an intermediate connection, who manages the transaction and distributes the payment amongst multiple merchants. For example, a customer pays his telephone, water, and electricity bills in one payment or one transaction redistributed into multiple transaction payments via the intermediary and automatically transferred to each merchant. This relationship between the customer, agent and merchant is one-to-one-to-many $(1:1:m)$, as depicted in Fig. 1(c).

Fig. 1 shows the concept of a payment system which can handle simple, parallel, and chain payments. All three payment types are common for mobile payment, but the chain payment type is increasingly popular due to the convenience it provides to users. In addition to supporting chain payments, the new mobile payment protocol aims to satisfy the security properties (CAIN) – Confidentiality (C), Authentication (A), Integrity (I), and Non-repudiation (N).

B. The necessity of Security Properties

In any payment system, the transaction security properties must be satisfied [2]. The security properties, CAIN, are described below:

- *Confidentiality*: The system must ensure that private or confidential information is not made available or disclosed to unauthorized individuals.
- *Authentication*: The system must ensure that the origin of a message is correctly identified, with an assurance that the identity is not false.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

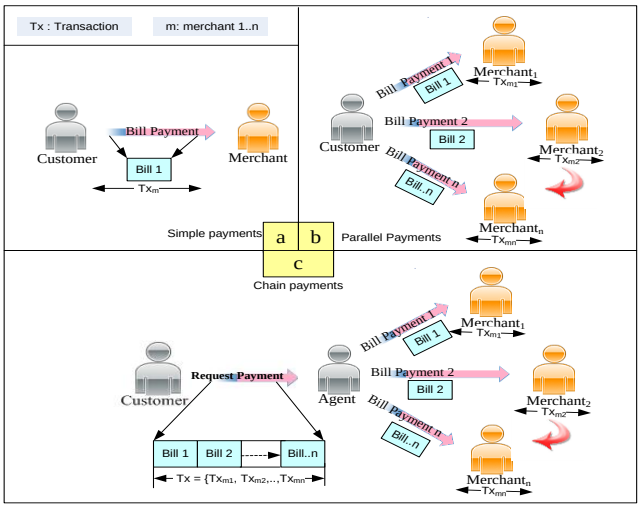

Fig. 1. Payment concept.

- *Integrity*: The system must ensure that only authorized parties are allowed to modify computer system assets and transmitted information.
- Non-repudiation: The system must ensure that the user cannot deny a completed transaction unless proof is provided.

C. The Limitations of Mobile Payment Devices

In the context of mobile payment, the limitations of mobile payment devices should be considered and are summarized as follows [3, 4]:

- The processor has lower computation capability and is not as powerful as that of a personal computer.
- The battery requires recharging and only lasts for short periods of time.
- The storage has limited capacity for processing the complex algorithms normally required for secure mobile payment protocols.
- The wireless network has less bandwidth and longer latencies compared with fixed networks.
- Data transmitted over wireless networks has higher risks of being compromised.
- Connection cost of wireless networks is higher than fixed networks.

Due to the high demand of mobile payment, researchers are continuously looking for solutions to overcome these limitations and design better and newer mobile payment systems.

The rest of the paper is organized as follows. Section 2 presents recent related works. Section 3 presents the proposed mobile payment model. Section 4 analyzes the proposed protocol and provides a comparison of protocols. Section 5 presents our conclusion and future works.

II. RELATED WORKS

This section presents some existing secure mobile payment protocols described in [5, 6, 9].

- Limpittaya *et al*. [5] proposed a secure agent-based mobile bill payment protocol for bulk transactions. The protocol facilitates clients and merchants with the assistance of more reliable intermediaries that may reside in a fixed network. The proposed protocol is based on symmetric cryptography and hash function that result in a more lightweight system. The security is increased by the deployment of a secure offline session key generation and distribution system. This protocol achieves security requirements including message confidentiality, message integrity, message authentication, and non-repudiation. By comparing the number of cryptographic operations, Limpittaya's protocol shows higher security than the one proposed by Turach *et al* [8]. The design of this protocol deploys lightweight cryptographic operations e.g. symmetric key and MAC operation (Message Authentication Code). Hence, it can be noted that a lower number of cryptographic operations and lightweight operations lead to better transaction performance of a security protocol.
- Carbonell *et al*. [6] proposed a secure e-payment protocol with new involved entities. This protocol proposed an e-payment model with an intermediary (IN) that links one customer with multiple merchants. The model is based on a client-centric approach which focuses on the protection of the end-to-end e-payment transactions that are transmitted through a powerful handheld client device. The e-payment model which features the interaction of five basic entities: the customer on the client side (C), a virtual merchant (M), the issuer bank (I), the acquirer bank (A) and a Payment System Provider (PSP). All transactions between the merchant and PSP have to be transported through an untrustworthy intermediary IN. This protocol guarantees the security required in the multiple e-payment transactions. The cryptographic mechanism is based on an asymmetric key and digital signatures that guarantee the security properties: confidentiality, integrity, authentication of the participating entities, and ensures the non-repudiation of origin for the whole message exchange.
- Qiongqiong and Mingjun [9] proposed a secure payment protocol based on multi-agents, using available online protocols and existing internet e-commerce resources for wireless communications. Transactions are secured using public key encryption technology. The payment protocol consists of five parties: the client (C), merchant (M), financial institutions including a bank (B), a payment system (PS) and a trusted third-party certification authority (CA). The encryption algorithms use the elliptic curve cryptosystem which has lower demand in storage capacity, computing capacity and communication volume. Compared with the prior traditional payment protocols based on a single mobile agent, a multi-agents protocol has more advantages in robustness, stability, and traceability.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

III. PROPOSED MODEL

The proposed conceptual mobile payment model is designed based on the integration of the best features of the related work as highlighted in the previous sections.

There are four entities in our model:

- *Customer (C)*, also known as client, buyer, or purchaser, is the recipient of goods and services obtained from a seller, vendor, or supplier for a monetary or other valuable consideration.
- *Merchant (M)* is a businessperson who trades in commodities produced by others for profit.
- *Intermediary (IN)* is a virtual mechanism connected to all parties for distribution of messages.
- *Payment Service Provider (PSP)* is a trusted third party that supplies money for businesses. A *PSP* can be a bank or non-bank.

A. The Connections in the Payment Model

The concept of the proposed payment model, as shown in Fig. 2(a), can be stated as follows:

1) The network connection is divided into two types: wireless and fixed network.
2) Only the customer is on the client side (wireless area), and all others are on the server side.
3) The customer device is a mobile phone, and the others are servers or computers.
4) All parties communicate with each other by a shared secret key for authentication.
5) A shared secret key between customer and merchant, and customer and payment service provider are offline, and the others conduct online.
6) The intermediary is a distributor of bill payments to multiple merchants and connects to payment service provider for confirming the updates of the account of customer and merchant.

B. Notation and Terms

The notation used in the proposed model is listed below:

TID: Transaction Identifier of the payments
ID_X: Unique Identifier of entity X
$Billno_{M_i}$: Unique Identifier of bill number for each merchant
$Price_{M_i}$: The price of goods and service from each merchant
T_{Amount}: Total amount for payment order each of TID
$Date_{M_i}$: The date and time of bill report from merchant i
T_P: Starting timestamp of transaction processing
A_{CC-M_i}: Account number of merchant i
A_{CC-C}: Account number of customer
$Status$: Set of Confirm Payment for each merchant i; $Status_{M_i}$ ="$Approved/Unapproved$"

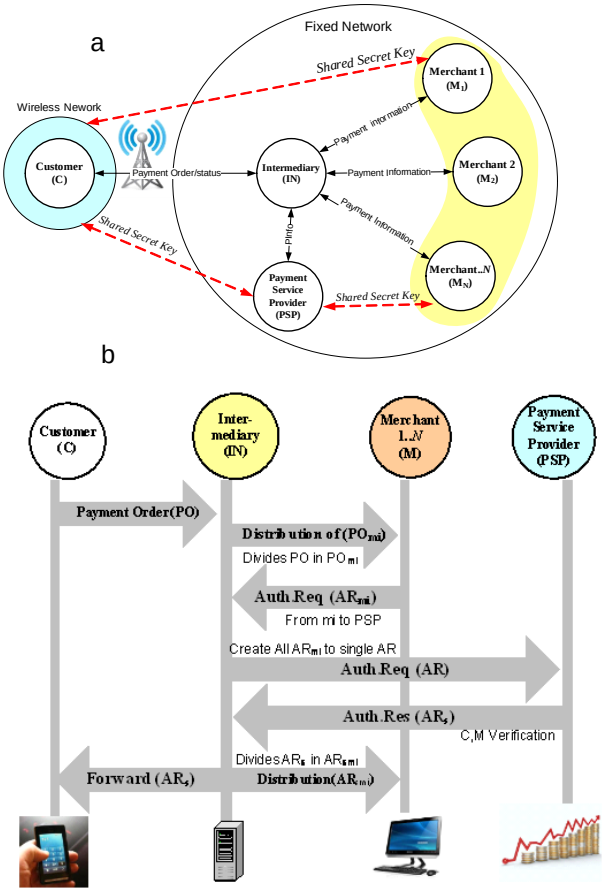

Fig. 2. Proposed secure mobile payment model.

PO_{M_i}: Payment Order (detail of each bill and each merchant) e.g. $PO_{M_i} = \{ID_{CM_i}, Billno_{M_i}, ID_{M_i}, Price_{M_i}, Date_{M_i}, A_{CC-M_i}\}$
PO: Multiple Payment Order (compound of $PO_{M_i;\, i=1..n}$) e.g. PO $= \{PO_{M_i}\}$
AR_{M_i}: Authorization Request from each merchant e.g. $AR_{M_i} = \{PO\}$
AR: Multiple Authorizations Request from all merchants e.g. $AR = \{AR_{M_i}\}$
AR_{SM_i}: Authorization Response from each merchant e.g. $AR_{SM_i} = \{AR_{SM_1},\ AR_{SM_2}, .., AR_{SM_n}\}$
AR_S : Multiple Authorizations Response from all merchants e.g. AR_S= $\{AR_{SM_i}\}$
$\{M\}_K$: Encryption Message M by key K
$SK_{(X-Y)_j}$: A session key that shares a secret key between entity X and Y, where the session key uses only one in order to protect from replay attack and regeneration.
$h(m, K)$: Message Authentication Code (MAC) or HMAC of a message m and a key K.
T_X : Payment Transaction = $\{TID,\ PO,\ Tp,\ A_{CC-C},\ T_{Amount}\}$

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

C. Initial Assumption

The initial assumptions for proposed protocols can be stated as follows:

1) Exchange session shared secret key between two parties:

a) Offline: $SK_{(C-M_i)}$, $SK_{(C-PSP)}$, $SK_{(PSP-M_i)}$

b) Online: $SK_{(IN-C)_j}$, $SK_{(IN-M_i)_j}$, $SK_{(IN-PSP)_j}$

where $j=1..m$ stands for session keys shared between the party X and Y. Note that the session key can use only one time in order to protect all parties from replay attack and regeneration.

2) Scenario: This scenario illustrates a payment for a public utility. The C party is a member of the M_i party for contacting the business. C and M_i are members of the same PSP, which have each account number such as A_{CC-C} and A_{CC-M_i}. The M_i presents a hard copy bill to the customer for payment. The customer can make payments to multiple merchants via mobile applications that can select many bill payments per one transaction. The flow of information is shown in Fig. 2(b).

3) Description of Proposed Protocols: This proposed model consist of six steps as follows:

Step 1:

$$\boldsymbol{C \rightarrow IN}:$$
$$\{TID, T_P, PO, T_{Amount}, \{A_{CC-C}\}_{SK_{(C-PSP)}},$$
$$h((\{A_{CC-C}\}_{SK_{(C-PSP)}}),\ SK_{(IN-C)_j})\}_{SK_{(IN-C)_j}}$$

In this Payment Order PO step, C sends T_X to IN that contains multiple bill payments for various merchants. The transaction message is encrypted by the session key $SK_{(IN-C)_j}$. In addition, hash function and secret key or HMAC also provide the integrity and non-repudiation properties.

Step 2:

$$\boldsymbol{IN \rightarrow M_i}:$$
$$\{TID, T_P, PO, T_{Amount},\ \{A_{CC-C}\}_{SK_{(C-PSP)}},$$
$$h((\{A_{CC-C}\}_{SK_{(C-PSP)}}), SK_{(IN-M_i)_j})\}_{SK_{(IN-M_i)j}}$$

This step involves the payment distribution process in which IN decrypts the message received in Step 1 and forwards the PO to each merchant. However, IN does not know the user account because it is encrypted by the session key between C and PSP. This provides the confidentiality and authorization properties.

Step 3:

$$\boldsymbol{M_i \rightarrow IN}:$$
$$\{Status, TID, T_P, T_{Amount}, \{A_{CC-C}\}_{SK_{(C-PSP)}}, AR_{M_i},$$
$$h((\{A_{CC-C}\}_{SK_{(C-PSP)}},\ AR_{M_i}),\ SK_{(IN-M_i)_j})\}_{SK_{(M_i-IN)_j}}$$

In this step, authorization request is made from $M_i \rightarrow IN$ to PSP. The merchant M_i checks if the PO_{M_i} is matched, then updates status and authorized request to PSP through the IN. This step ensures the CAIN properties.

Step 4:

$$\boldsymbol{IN \rightarrow PSP}:$$
$$\{Status, TID, T_P, T_{Amount}, \{A_{CC-C}\}_{SK_{(C-PSP)}}, AR,$$
$$h((\{A_{CC-C}\}_{SK_{(C-PSP)}}, AR), SK_{(IN-PSP)_j})\}_{SK_{(IN-PSP)_j}}$$

This is the authorization request step made from IN to PSP. The intermediary IN creates a single authorization request and forwards it to PSP. The security technique in this step also provides the CAIN properties.

Step 5:

$$\boldsymbol{PSP \rightarrow IN}:$$
$$\{Status, TID, T_P,\ T_{Amount}, \{A_{CC-C}\}_{SK_{(C-PSP)}}, AR_S,$$
$$h((\{A_{CC-C}\}_{SK_{(C-PSP)}},\ AR_S),\ SK_{(IN-PSP)_j})\}_{SK_{(IN-PSP)_j}}$$

In this step, an authorization response is sent from PSP to IN. The PSP decrypts the message by using the shared session key between the IN and PSP. The PSP first checks the status and updates the request information from M_i, then sends the authorization response to IN.

Step 6:

$$\boldsymbol{IN \rightarrow C}:$$
$$\{Status, TID, T_P, T_{Amount}, \{A_{CC-C}\}_{SK_{(C-PSP)}},\ AR_S,$$
$$h((\{A_{CC-C}\}_{SK_{(C-PSP)}}, AR_S), SK_{(IN-C)_j})\}_{SK_{(IN-C)_j}}$$
$$\boldsymbol{IN \rightarrow M_i}:$$
$$\{Status,\ TID,\ T_P,\ T_{Amount},\ \{A_{CC-C}\}_{SK_{(C-PSP)}},\ AR_{SM_i},$$
$$h((\{A_{CC-C}\}_{SK_{(C-PSP)}},\ AR_{SM_i}),\ SK_{(IN-M_i)_j})\}_{SK_{(IN-M_i)j}}$$

The last step is the authorization response distribution process, which includes messages sent from IN to C and IN to M_i. The intermediary IN sends a single authorization response to C and distributes the authorization response to each merchant M_i. In summary, all steps use the symmetric key encryption and HMAC technique that can ensure the necessary security properties (CAIN).

IV. ANALYSIS OF PROPOSED PROTOCOL AND COMPARISON OF PROTOCOLS

Three aspects of our framework (Mobile Payment Protocol Security) are the core of this mobile payment protocol which includes Methodology, Security, and Performance. The MPPS framework is shown in Fig. 3.

- *Methodology*: The proposed protocol uses symmetric key and hash function. Our method offers higher speed than the ones that use asymmetric keys. It also provides more security because the key distributions are both online and offline.
- *Security:* Encryption by shared secret key and the use of hash function provide CAIN properties that are suitable and reliable in a mobile payment system.
- *Performance:* The proposed protocol focuses on reducing the number of operation encryptions and the number of messages, leading to lower computation and better performance.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

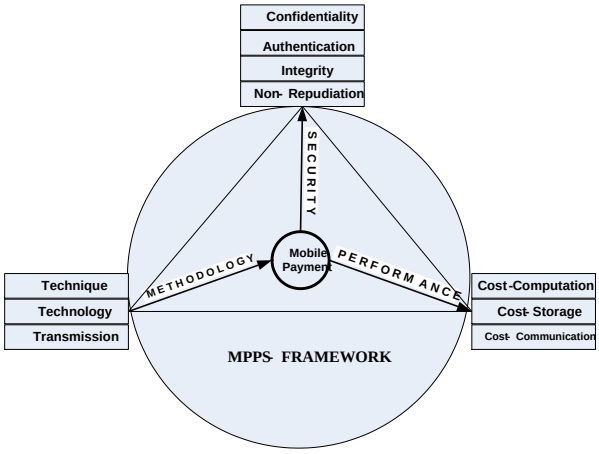

Fig. 3. The MPPS Framework.

The proposed protocol has been compared with two related works, focusing on seven characteristics. The overall results illustrate the benefits of this protocol as shown in Table I. The proposed protocol requires fewer number of messages and cryptographic operations. As a result, it takes less time to complete all information transaction when compared to existing protocols. The ratio of the numbers of messages (the proposed protocol : Carbonell et al.'s protocol : Limpittaya et al.'s protocol) is 1:1.33:2.67. Likewise, the proposed protocol provides multiple payments as the Carbonell et al.'s protocol [6]. Both protocols give more convenient than the Limpittaya et al.'s protocol [5]. All protocols, however, satisfy the CAIN properties. The proposed protocol is a new model that is designed based on the advantages of the related works which is suitable for the new lifestyle.

V. CONCLUSIONS AND FUTURE WORK

This paper proposed a lightweight secure mobile payment protocol supporting multiple payments by using symmetric cryptography and hash function for protecting the messages transmitted via the Internet. This model is focused on short and lightweight messaging, leading to high performance that is suitable for wireless network application. Our protocol provides better performance than the other related works. The future work will be developed and analyzed in detail using this conceptual model.

TABLE I
COMPARISON OF THE PROPOSED PROTOCOL WITH RELATED WORKS

Protocol Name	Crypto-Technique	Number of M: E: H	Rate of M	Tx of C: Mc	Security Properties
Limpittaya et al. [5]	Symmetric Key	16: 12 : 8	2.67	1:1	CAIN
Carbonell et al. [6]	Asymmetric Key	8: 22: 2	1.33	1:m	CAIN
Proposed Protocol	Symmetric Key	6: 8: 6	1.00	1:m	CAIN

M = message, E = encryption , H = hashing function, Tx = transaction, C = customer, Mc = merchant , CAIN = confidentiality, authentication, integrity, non-repudiation.

REFERENCES

[1] Wikipedia. (Jan 2015). Mobile Payment [Online]. Available: http://en.wikipedia.org/wiki/Mobile_payment
[2] W. Stalling, *Cryptography and Network Security: Principles and Practice*, 6th Edition, Prentice Hall International, 2013.
[3] S. Kungpisdan, *Modelling, Design, and Analysis of Secure Mobile Payment Systems*, Doctor of Philosophy Thesis, Faculty of Information Technology, Monash University, 2005.
[4] K. Wrona, M. Schuba, and G. Zavagli, "Mobile payments – state of the art and open problems," *Lecture Notes in Computer Science*, Springer-Verlag, vol. 2232, pp. 88–100, 2001.
[5] P. Lumpittraya, M. Warasat, and S. Kungpisdan, "Design and analysis of a secure agent-based mobile bill payment protocol for bulk transactions," in Proceedings of the 9th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2012, pp. 71–76.
[6] M. Carbonell, J. Torres, D. Suárez, J. M. Sierra, and J. Téllez, "Secure e-payment protocol with new involved entities," in Proceedings of the International Symposium on Collaborative Technologies and System (CTS), IEEE, 19–23 May 2008, pp. 103–111.
[7] M. Carbonell, J. M. Sierra, J. Torres, and A. Izquierdo, " Security analysis of a new multi-party payment protocol with intermediary service," in Proceedings of the 18th International Workshop on Database and Expert System Applications (DEXA 07), IEEE, 2007, pp. 698–702.
[8] P. Turach, et al., "A bill payment system via an intermediary supporting bulk transactions," in Proceedings of the 7th International Joint Conference on Computer Science and Software Engineering (JCSSE 2010), 14 May 2010, Bangkok.
[9] Q. Wang and M. Xin, "Research on a secure mobile payment based on multi-agents," in Proceedings of the 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), IEEE, 2010, pp. 663–666.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731