A Security Enhanced Lightweight Mobile Payment Scheme Based on Two Gateways

Hakjun Lee, Jiye Kim, Jongho Moon, Dongwoo Kang, Dongho Won*
Department of Computer Engineering, Sungkyunkwan University, 2066 Seoburo, Suwon, Gyeonggido 16419, Republic of Korea

* Corresponding author. Tel.: +82-31-290-7213; email: dhwon@security.re.kr
Manuscript submitted October 12, 2016; accepted March 14, 2017.
doi: 10.17706/ijcce.2017.6.2.83-90

Abstract: The number of m-commerce users is exponentially increasing and the m-commerce has become popular because m-commerce allows us to pay for goods or services anytime, anywhere using mobile devices. A number of the mobile payment scheme has been proposed to ensure security requirements on m-commerce. However, several of them are vulnerable to various attacks. This paper proposes an enhanced lightweight mobile payment scheme based on two gateways. We show that the proposed scheme ensures necessary security requirements such as accountability, untraceability, unlinkability and double spending prevention. In addition, it is suitable for lightweight mobile payment environments by analyzing and comparing it with the related mobile payment scheme.

Key words: m-commerce, mobile payment, accountability, untraceability, unlinkability.

1. Introduction

With the rapid development of network technologies, the number of m-commerce user is exponentially increasing because users can make the electronic payment on mobile devices such as tablets and smartphones [1] [2]. Since such mobile devices have low-power, limited memory and low-computational capacity, the m-commerce needs to employ lightweight payment protocols. In recent years, various authentication protocols for secure mobile payment have been proposed using NFC, smart card, and biometrics [3]-[9].

Sureshkumar et al. [10] introduced two gateway based payment scheme, and then Sureshkumar *et al*. [11] also proposed an enhanced lightweight protocol based on two gateways using dynamic identity. They claim that their scheme satisfies security requirement for mobile payment such as unlinkability, accountability and untraceability, and reduces computational complexity than other related works. However, their schemes have some drawbacks.

In this paper, we propose a security enhanced lightweight mobile payment scheme based on two gateways to solve the drawbacks of existing schemes. Our proposed scheme meets the various security requirements such as accountability, untraceability, unlinkability, double spending prevention and DoS attack prevention. The comparisons of security and computational complexity with related works show that our scheme is definitely improved and more practical in lightweight mobile payment environments.

The remainder of this paper is organized as follows. We briefly discuss related payment schemes in Section 2. Our proposed scheme is shown in detail in Section 3. We analyze the security of the proposed

scheme and compare it with those of related works in Section 5. Section 6 is a brief conclusion.

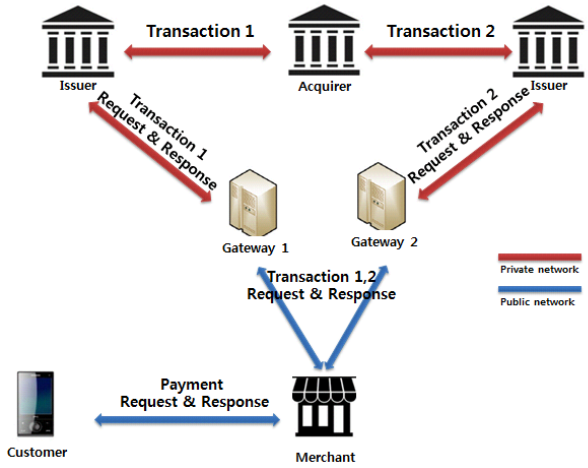

Fig. 1. Mobile payment mechanism based on two gateways.

2. Related Works

In 2015, Luo *et al.* [2] proposed an NFC-based user registration scheme for mobile payment to provide user's anonymity and unlinkability in the further transaction process. They use a virtual account issued by the issuer and a virtual card issued by the payment gateway to ensure anonymity of users and unlinkability in transactions. However, their scheme is vulnerable to DoS attacks and has symmetric key leakage problems. Furthermore, they use the public key cryptography and signature. Therefore, their scheme is not suitable for lightweight payment environments. In 2016, Sureshkumar *et al.* [9] proposed a lightweight two gateway based payment scheme with dynamic identity. Their scheme uses a symmetric key encryption. Therefore, their scheme is suitable for lightweight payment environments. However, their scheme also is vulnerable to DoS attacks and does not prevent double spending.

3. The Proposed Scheme

In this section, we propose a security enhanced lightweight mobile payment scheme based on two payment gateway. The mobile payment mechanism for the proposed scheme is illustrated in Fig. 1. Our proposed scheme has four participants: the customer, the merchant, and two payment gateways. We assume that there is an internally secure network among the two issuers, the acquirer and the two gateways. That is, they communicate each other in secure channel. Therefore, in this paper, we focus on a lightweight payment process along with the customer, the merchant, and the gateways. The notations used in proposed scheme are shown in Table I.

3.1. Assumptions

- The customer has a bank account issued by the issuer, and two credit cards.
- The customer individually registers credit information with credit cards and account information to the two gateways, respectively.
- The gateways associate them to provide mobile payment service to the customer after verifying the customer's identity. Next, the gateways and the customer share the initial dynamic identities ID_{CG_1} and ID_{CG_2} for ensuring customer anonymity and symmetric keys K_{CG_1} and K_{CG_2} for secure communications using the key establishment protocols.
- Likewise, the merchant registers to the two gateways and shares symmetric keys K_{MG_1} and K_{MG_2}.

- The customer wants to purchase goods or service through the merchant's website. However, the balance in any one of the credit cards is not enough to pay. But, the sum of balance for two cards is enough. Therefore, the customer will buy the product using two cards via different gateways.

Table 1. Notations

Values	Description
M	Merchant
C	Customer
G_1	Gateway one
G_2	Gateway two
TID	Temporary transaction identity
p_1	Part of the amount customer pays through gateway G_1
p_2	Remaining amount customer pays through gateway G_2
OD	Order description containing the chosen items
$TInfo$	Information of transaction including serial numbers, time and date
T	Timestamp
K_{AB}	Symmetric key between the two entities A and B
$h(m)K_{AB}$	The keyed hash of the message m using the key K_{AB}
$h(m)$	Hash of the message m
$\{m\}K_{AB}$	Cipher of the message m with the key K_{AB}
ID_{CG_i}	Customer dynamic session ID corresponds to the gateway G_i

3.2. Lightweight Mobile Payment Protocols

Fig. 2 illustrates our lightweight mobile payment protocols. Detail is as follows:

3.2.1. Phase 1 – Initiating payment

Initially, the customer selects goods or services through the merchant`s website, and starts initial payment phase with the merchant.

Step 1. The customer C generates his temporary transaction identity TID and order description OD, and sends the payment request $m_1 = \{TID, OD, h_1\}$ to merchant M, where the keyed hash value $h_1 = (TID, OD)K_{MC}$.

Step 2. After receiving the m_1, the merchant generates transaction information $TInfo$ and computes $h_2 = (TInfo, h2)$. The M then sends $m_2 = \{TInfo, h_2\}$ to C

3.2.2. Phase 2 – payment with gateway

Step 1. The C computes $m_3 = \{TID, G_1, G_2, p_1, p_2, h_3, T_1\}K_{MC}$, $m_4 = \{ID_{CG_1}, TID, p_1, T_1, h_3\}K_{CG_1}$ and $m_5 = \{ID_{CG_2}, TID, p_1, T_1, h_3\}K_{CG_2}$, where the hash value $h_3 = (TID, TInfo, T_1)$. The C sends transaction request message $\{m_3, m_4, m_5\}$ to M.

Step 2. After receiving the messages, the M decrypts m_3 and checks whether T_1 is within a tolerable period and $p =? p_1 + p_2$. If they hold, the M computes $m_6 = \{TID, TInfo, p_1, T_2, h'_3\}K_{MG_1}$, where $h'_3 = (TID, TInfo, T_1)$, and sends the transaction request $\{m_4, m_6\}$ to gateway G_1.

Step 3. The G_1 decrypts the received messages m_4 and m_6, and verifies whether the timestamp T_1 and T_2 are within a tolerable period, and whether h_3 and h'_3 are equal. If they hold, the G_1 checks the credit limit of ID_{CG_1}. If p_1 is larger than credit limit of ID_{CG_1}, then sets $acp_1 = F$, else $acp_1 = T$. The G_1 then computes the response message $m_7 = \{TID, p_1, acp_1\}K_{MG_1}$, and sends it to M.

Step 4. The M computes $m_8 = \{TID, TInfo, p_1, T_2, h'_3\}K_{MG_2}$ and sends the transaction request $\{m_5, m_8\}$ to gateway G_2.

Step 5. The G_2 decrypts the received messages m_5 and m_8, and verifies whether timestamp T_1 and T_2 are within a tolerable period, and whether h_3 and h'_3 are equal. If they hold, the G_2 checks the credit limit of ID_{CG_2}. If p_2 is larger than credit limit of ID_{CG_2}, then sets $acp_2 = F$, else $acp_2 = T$. The G_2 then computes the response message $m_9 = \{TID, p_2, acp_2\}K_{MG_2}$, and sends it to M.

Step 6. After receiving the response messages, the M decrypts the messages m_7 and m_9, and computes $acp = acp_1 \wedge acp_2$, total amount $p = p_1 + p_2$ and the response message $m_{10} = \{TID_2, p, acp, T_3\}K_{MC}$. The M then sends m_{10} to C.

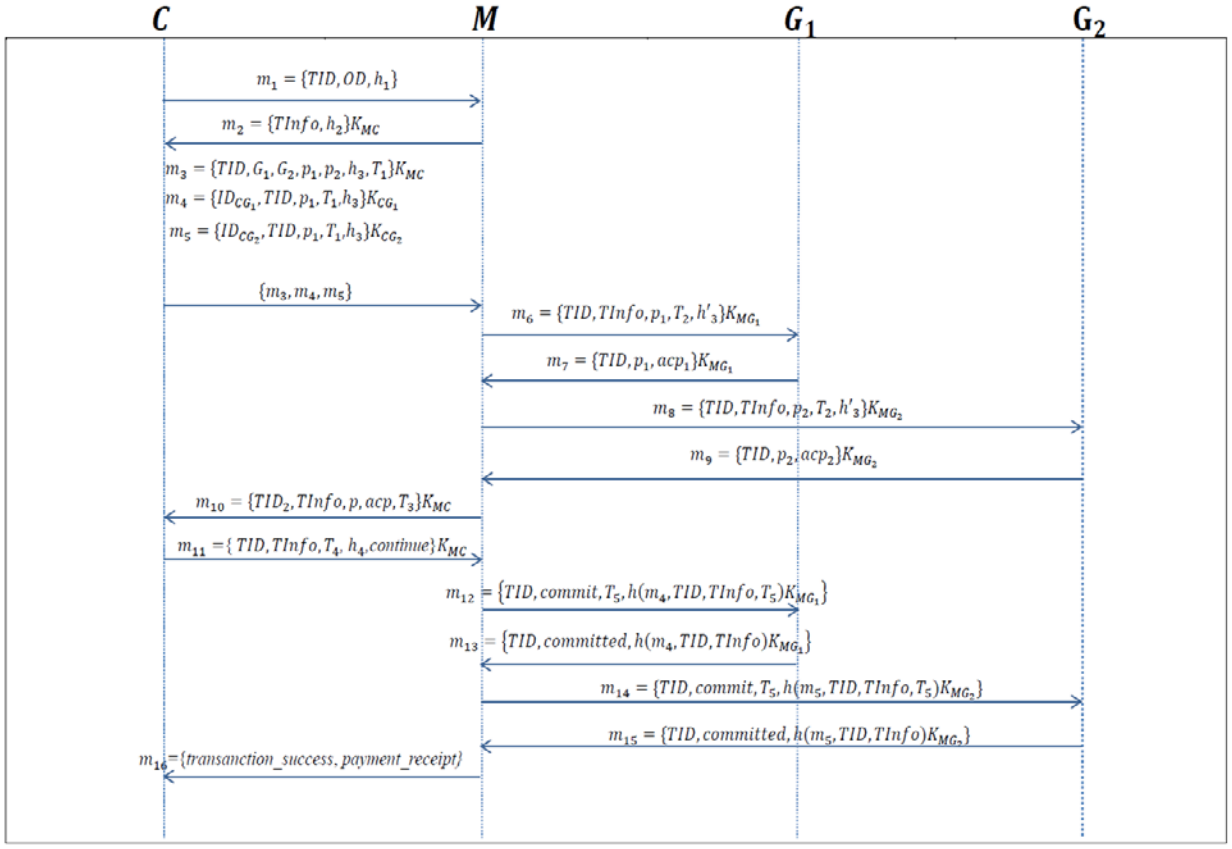

Fig. 2. An enhanced lightweight mobile payment scheme based on two gateways.

3.2.3. *Phase 3 – Commitment phase*

Step 1. After receiving the m_{10}, the *C* checks whether the total amount p is correct and acp is true. If it holds, the *C* computes $m_{11} = \{TID, TInfo, T_4, h_4, continue\}K_{MC}$, and sends it to *M* in order to express that he/she wants to continue the payment processes, otherwise the customer aborts payment, where $h_4 = (TID, TInfo, p, T_3)$.

Step 2. After receiving the m_{11}, the merchant checks whether timestamp T_4 is within a tolerable period and the customer wants to continue. If it holds, the merchant computes the commit message $m_{12} = \{TID, commit, T_5, h(m_4, TID, TInfo, T_5)K_{MG_1}\}$ and sends it to gateway G_1.

Step 3. The G_1 decrypts the received message m_{12}, and checks whether timestamp T_5 is within a tolerable period. If it holds, the G_1 verifies keyed hash message value using K_{MG_1}. If it is valid, the G_1 computes the response message $m_{13} = \{TID, committed, h(m_4, TID, TInfo)K_{MG_1}\}$, and sends this committed message to merchant.

Step 4. The *M* computes the commit message $m_{14} = \{TID, commit, T_5, h(m_5, TID, TInfo, T_5)K_{MG_2}\}$ and sends it to G_2.

Step 5. The G_2 decrypts the received message m_{14}, and checks whether timestamp T_5 is within a tolerable period. If it holds, the G_2 verifies keyed hash message value using K_{MG_2}. If it is valid, the G_2 computes the response message $m_{15} = \{TID, committed, h(m_5, TID, TInfo)K_{MG_2}\}$, and sends this committed message to *M*.

Step 6. After receiving the m_{13} and m_{15}, the *M* verifies whether keyed hash values contained in the both messages are valid. If it holds, the *M* sends traction success messages and payment receipt to the *C*.

After the successful commitment phase, the gateways perform the remainder of transaction process with concerned issuer and acquirer via the internally secure channel. The customer also receives the result of the transaction for the purchased goods or services. Then, the dynamic IDs between the gateways and the customer is updated and the gateways carry out update process as follows:

$$ID_{CG_1}(new) = h(ID_{CG_1}(old)||T_5)K_{CG_1}$$

$$ID_{CG_2}(new) = h(ID_{CG_2}(old)||T_5)K_{CG_2}$$

Table 2. Security Comparison of the Proposed Scheme and Other Related Schemes

Features	[12]	[2]	[10]	Proposed scheme
Accountability	Yes	Yes	Yes	Yes
Untraceability	Yes	Yes	Yes	Yes
Unlinkability	No	Yes	Yes	Yes
Anonymity	No	Yes	Yes	Yes
Double spending prevention	No	Yes	No	Yes
DoS attack prevention	Yes	No	No	Yes

Table 3. Computational Complexity Comparison of the Proposed Scheme and Other Related Schemes

Features	[12]	[2]	[10]	Proposed scheme
Public-key en/decryptions	0	6	0	0
Digital signature	0	7	0	0
Symmetric-key en/decryptions	10	7	10	10
Hash functions	3	0	4	2
Keyed hash functions	3	0	10	6

4. Security Analysis

In this section, we analyze our proposed scheme in terms of security and computational complexity. Table II shows security comparisons of our scheme and other related schemes. Table III shows a computational complexity comparison of the proposed scheme and other related schemes. These two tables said that the proposed scheme is lightweight in terms of computational complexity, and more secure than other mobile payment scheme.

4.1. Accountability

In the proposed scheme, accountability issues are not caused because the commitment phase is performed after confirming the customer's consent. In addition, the freshness of commitment messages is guaranteed by symmetric keys and timestamps. So the customer is able to start a fresh transaction for buying products or services.

4.2. Untraceability

The customer uses a temporary transaction identity and different dynamic identities for the two gateways. Thus, different payments of a same customer cannot be linked. Therefore, our scheme satisfies untraceability property because an attacker is unable to distinguish a particular customer.

4.3. Unlinkability

Unlinkability is a strong anonymity. In our scheme, an adversary cannot know a customer's real identity. If the transaction information is revealed, nobody knows who the customer is. Thus, our scheme satisfies unlinkability property.

4.4. Double Spending Prevention

In [9], it is possible to implement double spending by replay attacks. However, the proposed scheme is secure against replay attacks by adding the timestamp into the messages. Though an adversary intercepts

the previous authentication message, and sends it to the merchant or gateway, the merchant and gateway can check the illegality of the message using checking the timestamp. In addition, because every authentication message is encrypted as well, the adversary cannot forge the timestamp. Thus, the proposed scheme can prevent double spending.

4.5. DoS attack Prevention

In [9], the attacker can perform DoS attacks in the payment agreement phase because the merchant accepts any message and then response with encrypted messages. However, in the proposed scheme, the customer sends keyed hash value h_1. To verify h_1, both of the customer and the merchant need to have a key K_{MC}. Therefore, the merchant checks if the customer is vaild. So the proposed scheme can prevent DoS attacks.

5. Conclusion

This paper proposes an enhanced lightweight mobile payment scheme based on two gateways. The security analysis and comparisons show the proposed scheme meets the necessary security properties such as double spending prevention, DoS attack prevention, and etc. Furthermore, the proposed is efficient in terms of computational complexity, compared to other existing schemes. Therefore, the proposed mobile payment scheme is more suitable and practical for lightweight mobile payment environments. In the future work, we will simplify the proposed scheme to provide a more lightweight m-commerce protocol and maintain the security requirements. In addition, performance evaluation to analyze the actual operating time will be performed.

Acknowledgment

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning (2014R1A1A2002775).

References

[1] Yang, J. H., & Lin, P. Y. (2016). A mobile payment mechanism with anonymity for cloud computing. *Journal of Systems and Software*, *116*, 69-74.

[2] Luo, J. N., Yang, M. H., & Huang, S. Y. (2016). An unlinkable anonymous payment scheme based on near field communication. *Computers & Electrical Engineering*, *49*, 198-206.

[3] Chen, W., Hancke, G. P., Mayes, K. E., Lien, Y., & Chiu, J. H. (2010). NFC mobile transactions and authentication based on GSM network. *Proceedings of 2010 Second International Workshop on Near Field Communication (NFC),* (pp. 83-89). *IEEE*.

[4] Moon, J., Choi, Y., Kim, J., & Won, D. (2016). An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. *Journal of medical systems*, *40(3)*, 1-11.

[5] Choi, Y., Lee, Y., & Won, D. (2016). Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction. *International Journal of Distributed Sensor Networks*, *12 (1).*

[6] Moon, J., Choi, Y., Jung, J., & Won, D. (2015). An improvement of robust biometrics-based authentication and key agreement scheme for multi-server environments using smart cards. *PloS one, 10(12)*, e0145263.

[7] Choi, Y., Nam, J., Lee, D., Kim, J., Jung, J., & Won, D. (2014). Security enhanced anonymous multi-server authenticated key agreement scheme using smart cards and biometrics. *The Scientific World Journal*.

[8] Kim, J., Lee, D., Jeon, W., Lee, Y., & Won, D. (2014). Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks. *Sensors, 14(4),* 6443-6462.

[9] Tan, Z. (2010). An enhanced three-party authentication key exchange protocol using elliptic curve cryptography for mobile commerce environments. *Journal of Communications*, *5 (5)*, 436-443.

[10] Sureshkumar, V., Anitha, R., Rajamanickam, N., & Amin, R. (2016). A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity. *Computers & Electrical Engineering*.

[11] Sureshkumar, V., Anitha, R., & Rajamanickam, N. (2016). Hash based two gateway payment protocol ensuring accountability with dynamic ID-Verifier for digital goods providers. *In Computational Intelligence, Cyber Security and Computational Models* (pp. 369-384). Springer Singapore.

[12] Isaac, J. T., & Zeadally, S. (2012). An anonymous secure payment protocol in a payment gateway centric model. *Procedia Computer Science, 10*, 758-765.

Hakjun Lee received the B.S. degree in Software Engineering from Korea National University of Transportation, Korea, in 2015. He is currently a master student at Electrical and Computer Engineering from Sungkyunkwan University, Korea. His current research interest is in the area of cryptography, authentication protocol, and mobile payment.

Jiye Kim received the B.S. degree in Information Engineering from Sungkyunkwan University, Korea, in 1999 and the M.S. degree in Computer Science Education from Ehwa University, Korea, in 2007. She also worked as a software engineer for mobile phone manufacturers in Korea or Japan between 1999 and 2013. She is currently pursuing the Ph.D. degree in Electrical and Computer Engineering at Sungkyunkwan University. Her current research interests include cryptography, security protocols, and security of sensor networks in IoT environments.

Jongho Moon received the B.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2012 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2014. He also worked as a malware analyzer in SECUI between 2014 and 2015. He is currently pursuing the Ph.D. degree in electrical and computer engineering at Sungkyunkwan University. His current research interest includes cryptography, malware, forensic, and authentication or key management protocols.

Dongwoo Kang received the B.S. degree in Electrical and Computer Engineering from Sungkyunkwan University, Korea, in 2015. He is currently pursuing M.S. degree in Electrical and Computer Engineering at Sunkyunkwan University. His current research interest includes cryptography, malware and authentication or key management protocols.

Dongho Won Received B.S., M.S. and Ph.D. in Electronic Engineering from Sungkyunkwan University, South Korea. After working in Electronics and Telecommunication Research Institute for two years, he joined Sungkyunkwan University, where he is currently a leader professor at Information and Communication Engineering. He also served as a President of Korea Institute of Information Security and Cryptography. His research interests are cryptology and Information Security.