Vol.2016-DPS-166 No.11
Vol.2016-CSEC-72 No.11
2016/3/3

An Enhanced Mobile Payment System in a Disaster Area using Endorsement Delegation

Babatunde Ojetunde[1,a)] Naoki Shibata[1,b)] Juntao Gao[1,c)] Minoru Ito[1,d)]

Abstract: Recently we introduced an endorsement-based mobile payment system (MPS) to allow people in a disaster area to do electronic transactions for buying necessities. However, our MPS may cause heavy communication overhead for merchants, due to the fact that a merchant may do excessive communication to search for enough endorsers to endorse a transaction. To reduce merchant communication overhead and also the time for completing a transaction, we propose in this paper an enhanced mobile payment system using endorsement delegation. Specifically, primary endorsers to a customer in our new mobile payment system delegate their endorsement capabilities to the secondary endorsers such that the merchant can send the billing message directly to the primary and secondary endorsers at the same time, thus reducing merchant communication used to search for the endorsers. By simulation, we evaluate the usability of our proposed payment system in a disaster area in terms of successful transaction completion ratio, frequency of breakage of event chain and merchant communication overhead. Our simulation results show that our endorsement mobile payment system is useful in disaster areas. The newly introduced endorsement delegation mechanism achieves better transaction completion ratio with an increase of 11% to 52% when compared with our previous mobile payment system.

1. Introduction

The importance of payment system cannot be over emphasis in disaster areas (like earthquake and flooding areas) where people need to buy necessities such as groceries, clothing, and medical supplies. Although physical cash is adjudged to be the easiest means of performing a transaction, it may be impossible to get cash in a disaster situation as access to a bank is restricted both physically (roads to a bank may be blocked or bank is destroyed) and electronically (communication infrastructures, like wired networks and cellular networks, may fail due to earthquake and flooding). To enable people to do transactions even in disaster areas, we proposed recently an infrastructureless mobile payment system (MPS) by utilizing flexible and robust mobile ad hoc networks (MANETs) formed via smart mobile devices (smart phone, iPad, etc.) ubiquitous in daily life [1] [2], where endorsers instead of central bank provide payment guarantees.

Challenges for designing such a MANET-based mobile payment system are as follows [3]:

- **Unreliability of the wireless link between nodes**
- **Constantly changing topology**
- **Lack of incorporation of security features**

In our previous system [1] [2], each customer selects other users to serve as his/her endorsers. An endorser provides payment guarantees for a customer to a merchant. To prove that a transaction is endorsed, an endorser puts his/her digital signature on every transaction. In a situation where a customer fails to pay for an item purchased, the money is deducted from the endorser's account. In addition, we adopted the endorsement chain mechanism where direct endorsers to a customer are known as primary endorser and endorsers to the primary endorsers are known as secondary endorsers. The secondary endorsers can endorse a customer transaction only when the primary endorsers are not available. We also introduced transaction monitoring from neighboring users to ensure transaction validity and reliability. Our payment system also addresses other security concerns, such as reset and recovery attacks, collusion among customers and endorsers, double spending, by adopting mechanisms of e-coin balance checking, event-chain and bloom filter. Our approach is similar to that of Bitcoin [4] where transactions are broadcast to neighboring nodes for monitoring, but differs in techniques as users do not need proof of work, rather users compute hash value of a transaction and append their signatures to event chain as a proof. However, our MPS may cause heavy communication overhead for merchants, due to the fact that a merchant may do excessive communication to search for enough endorsers to endorse a transaction if the primary endorsers are not available.

To reduce merchant communication overhead and also the transaction completion time, we propose in this paper an enhanced mobile payment system using endorsement delegation. The endorsement delegation mechanism allows the primary endorsers to delegate their endorsement capabilities to their own endorsers, thus, making their endorsers to serve as secondary endorsers to the customer. Beforehand, the customer selects primary endorsers with which the bank forms an endorser list, which

[1] Nara Institute of Science and Technology
[a)] ojetunde.babatunde.nq3@is.naist.jp
[b)] n-sibata@is.naist.jp
[c)] jtgao@is.naist.jp
[d)] ito@is.naist.jp

includes the primary and secondary endorsers for the customer. During the transaction, the customer attaches the list to the transaction order message and sends it to the merchant. Unlike our previous system, the merchant sends the billing message directly to the primary and secondary endorsers at the same time, thereby avoiding the use of excessive communication needed to search for secondary endorsers when there are a limited number of endorsers to endorse a transaction. Hence merchant overhead and transaction completion time is reduced. To evaluate performances of our enhanced MPS, we developed a customized simulator in Java. Specifically, our simulation focuses on (i) successful transaction completion ratio, (ii) frequency of breakage of event chain, (iii) merchant communication overhead, and (iv) effect of node mobility speed, endorser density, monitoring user density and merchant density on transaction completion ratio. Finally, we present our simulation results.

The rest of this paper is organized as follows. In Section 2, we review related literature on mobile payment systems. In Section 3, we present the overview of our previous endorsement-based mobile payment system, In Section 4, we introduce the endorsement delegation mechanism to enhance our system, reducing merchant communication overhead and the response time of service. Finally, we give in Section 5 the performance evaluation process for the enhanced system, the results of our simulation and conclude the whole paper in Section 6.

2. Related Work

In this section, we review existing mobile payment systems. Many researches have been conducted on mobile payment systems, however, they require the support of communication infrastructures to enable secure transactions, therefore not suitable for disaster areas without communication infrastructures. Patil *et al.* [5] introduced a credit-based and off-line micro-payment scheme called e-coupons. The scheme allows users to delegate their spending capability to their own devices or other users. The e-coupon scheme delegation protocol is based on multi-seed payword chains using Simple public key infrastructure/ Simple Distributed Security Infrastructure (SPKI/SDSI) authorization certificates. Their scheme focuses on minimizing the computational cost of mobile devices with limited resources.

Similarly, Chen *et al.* [6] proposed a scheme that focuses on e-payment systems with electronic cash. To reduce merchants' burden of having an account for depositing electronic cash received from customers with multiple banks, Chen's scheme introduced the concept of deposit delegation, which allows a merchant to maintain a single account at its trading bank and delegates all deposits from various banks into the account. The protocol adopts a cryptographic mathematical model that is based on solving discrete logarithm difficult problem or solving factorization difficult problem to secure the system against fraud. Kiran *et al.* [7] proposed a robust payment system which adopts public key infrastructure and hash chain to secure transactions. The proposed system seeks the cooperation of intermediate nodes to ensure secure and reliable transaction by allocating payment to nodes that permit relaying of packets, thereby providing service. In addition, the proposed payment system uses chains of delegates in which a customer can delegate the authorization to transfer money from the customer's account to other clients (such as a vendor). The system allows clients to carry out transactions both on-line and off-line. Dai *et al.* [8] developed an offline payment system, which, however, is only for digital goods. The proposed mobile payment system adopts mechanisms from Dai's previous works, where they introduced a debit-based payment protocol called NetPay, and NetPay-based systems for client-server, vendor and customer networks and e-wallets system to manage e-coins.

Other researches focus on providing secure online payment system, for example, Hu *et al.* [9] proposed a payment mechanism that allows a customer to make a purchase either from his/her local domain or from a remote domain. However, the payment protocol is not optimized for subsequent payments by the customer, and the protocol depends on a trusted third party, which is a performance bottleneck of the system. In addition, the protocol allows a customer and a merchant to authenticate each other indirectly, while preventing a merchant from knowing the customer's real identity. Wang *et al.* [10] presented a novel e-cash payment system which reduces online computational cost of transactions. The computational cost reduction is achieved by integrating the trapdoor hash function into the system. Wang's payment system requires only integer multiplication and addition operations for computation, similar to [11], [12]. When payment is required during the transaction, the customer uses an electronic payment certificate issued by a bank to request payment from the bank. The money is deducted directly from the customer's account after the merchant supplies the item.

Chang *et al.* [13] focuses on e-payment system by introducing a novel electronic check scheme to address the inflexibility of the electronic check proposed in [14], [15]. The scheme adopts cryptographic techniques such as one-way hash function, blind signature and RSA cryptosystems to enhance the security of the system. The scheme allows a customer to attach the cost of goods to be purchased and the merchant information to the electronic check during a transaction, thereby achieving mutual authentication between the customer and the merchant. Liaw *et al.* [16] also adopted a similar concept to introduce an electronic traveler check scheme, similar to Chang's electronic check mechanism; however, Liaw's scheme, unlike Chang's electronic check, uses one-way hash function which improves efficiency and reduces cost of the system. A customer's identity is included in the traveler's check to ensure that only the customer can use a specific electronic traveler's check. It also supports on-line and off-line traveler's check system. Li *et al.* [17] introduces an electronic payment protocol that allows a vehicle to pay for a transaction in a restricted connectivity scenario, but it requires a wireless connection between the merchant and the bank during transaction, therefore, cannot be used to provide the needed services for people in a disaster area.

Nakamoto [4] proposed a decentralized electronic cash system known as Bitcoin, which requires no central control. New transactions are broadcasted to all nodes in the system, and each node accepts the transaction into a block. Then all nodes try to do a reverse calculation of a hash function, which takes a large amount of computation, as proof-of-work to validate the transaction in their blocks (the validation process is called mining and each miner is rewarded for every block validated). Nodes accept the block only if the transactions are valid and not already spent. The hash of an accepted block is used in the next block to form a block chain, and the network can thereby agree on the order in which transactions occurred. However, Bitcoin requires a device with high power and transactions are computationally irreversible, so that Bitcoins can never be replaced once a user's private key was forgotten or destroyed.

In our previous system [1] [2], we introduced a secure payment system that adopts infrastructureless MANETs to allow users to purchase necessities in disaster areas. Also, we proposed a mechanism to detect double spending before a transaction is completed, unlike existing systems that detect double spending when e-coins are deposited in a bank or deducted from a customer's account. Our previous system adopts a similar approach to Bitcoin in that transactions are broadcast to neighboring nodes. However, our method differs, since users in our system do not need proof of work. Rather, users compute the hash value of a transaction log, and neighboring nodes append their signature to the log to form an event chain (similar to block chain). The event chain can be verified by surrounding neighboring nodes. Unlike most existing payment systems, our proposed mechanism does not depend on a central authority or mint to detect double spending. In this paper, we adopt the new concept of delegation mechanism to our system for reducing merchant communication overhead and also the response time of service. However, our delegation approach differs from previous works [5] [6] [7] in that we focus on using the delegation for our endorsement mechanism instead of depositing of money or for micro-payment.

3. Overview of Endorsement-Based Mobile Payment System

In this section, we provide a brief overview of our endorsement-based mobile payment system in disaster areas and then explain various schemes adopted to ensure secure transactions in our system.

3.1 Endorsement-Based Mobile Payment System

Endorsement: In a payment system, an endorsement is a mechanism by which a user agrees to make payment for a customer in the case that the customer fails to pay. The endorser should have real money deposited in a bank before a disaster occurs. In the proposed method, multiple endorsers that are available guarantee each transaction such that the endorsement liability for one transaction is shared among all the endorsers, thus reducing endorsing risks if a customer buys an item, but defaults afterwards. To encourage endorsers to stay honest and support the mobile payment system, some part of the transaction amount (e.g., 3%) is awarded to endorsers.

An endorser agrees to directly serve as a customer's endorser by signing an endorsement agreement, thereby acknowledging to personally guarantee the customer's transaction and pledge to make payment for up to the deposited amount for every transaction in which the customer defaults in payment. The endorsement agreement comes with a condition that the real money deposited in the endorsement account will be restricted (locked) to endorsing a customer alone and the endorsement amount for each transaction has a limit. The endorsement agreement is made during registration before disaster happens.

3.2 Participant

All the entities (customer, endorser, merchant, and bank) that join and are involved in the payment system will be referred to as users. All users communicate through MANETs.

- **Merchant** - a user that provides goods, services, products or software.
- **Customer** - a user that buys goods, services, products or software from a merchant.
- **Endorser (also known as Primary Endorser)** - a user who pledges to fulfill the customer's obligation in a situation where the customer fails to pay for items bought.
- **Secondary Endorser** - an endorser to the primary endorser who pledges to fulfill the primary endorser's obligation to a customer in a situation where the customer fails to pay for items bought and the primary endorser is not available.
- **Monitoring Customer (referred to as a Monitor hereafter)** - a customer that checks every transaction within the radio range to make sure that each message is valid and reliable.
- **Bank** - an organization that maintains users' accounts.
- **Bank Truck** - A bank agent that is responsible for delivery of messages to/from users (endorsers) in a disaster area.

3.3 Setup Process

The setup process in our system can be divided into three stages, namely merchant registration, customer registration and endorser selection.

To join the system, customers and merchants register with the bank before a disaster happens. Then the bank issues digital certificates to all users. The notations for user's public and private keys are shown in Table 1.

Table 1 Proposed System Keys

User	User Identity	Public Key	Private Key	Digital Signature
Bank	B	K_B	K_B^{-1}	$S_{K_B^{-1}}$
Merchant	M	K_M	K_M^{-1}	$S_{K_M^{-1}}$
Customer	C	K_C	K_C^{-1}	$S_{K_C^{-1}}$

Each customer selects a photograph that will be digitally signed by the bank. This serves as an additional authentication means during a transaction and protects the other party in case of a stolen phone. (This is the same as checking an individual photograph on an identity card, though here the merchant will also confirm the bank's and the customer's digital signatures on the photograph.) The system may use some other methods of biometric authentication.

In order to ensure the security of transactions in the system, all messages are digitally signed and encrypted. This will prevent repudiation of transactions. Also, other users can monitor each transaction and thereby identify a dishonest user in the network.

3.3.1 Merchant registration

STEP 1: A merchant submits registration request to the bank to join the mobile payment system.

STEP 2: The bank accepts the registration request and generates public and private keys for the merchant.

3.3.2 Customer registration

STEP 1: A customer submits a registration request to the bank to participate in the mobile payment system.

STEP 2: The bank accepts the registration request and generates public and private keys for the customer.

STEP 3: The customer selects a photograph and requests the bank to sign the photograph with its digital signature.

STEP 4: The bank signs the customer photograph with its digital signature.

3.3.3 Endorser selection

STEP 1: The customer submits the list of users that will serve as his/her endorsers in the system.

STEP 2: If a user agrees to endorse other specific users, the user deposits real money in the bank. Then the bank generates electronic coins equivalent to the amount deposited by the user (now as endorser).

STEP 3: The bank generates an endorsement tree. This will be explained later in Section 3.4.5

With the above setup, a merchant authenticates a user as follows:

STEP 1: A user sends digitally signed picture with the transaction order message to the merchant.

STEP 2: Merchant checks and compares digitally signed picture with customer's appearance.

STEP 3: The merchant confirms the digital signature of the bank.

STEP 4: Then the merchant uses the digital certificates as additional authentication mechanism. If the customer's appearance, the digital signature and digital certificates are valid, then the merchant authenticates the customer as a valid customer.

The same process is used by other users, to authenticate each other while the merchant is authenticated using only the digital certificates.

3.4 Schemes for Secure Transaction

In this subsection, we briefly explain various schemes adopted to secure transactions in our endorsement-based mobile payment system.

3.4.1 E-coin

We employ the e-coin technique to check the bank balance of endorsers, thereby preventing collusion between endorsers and a customer.

E-coin : The bank creates unique e-coins for an endorser, similar to tokens, in [18], [19]: e_{T_1}, e_{T_2}, e_{T_3},. e_{T_n}, for example. The sum of these e-coins will be equal to the account balance of the endorser. The e-coin contains the endorser's identity, e-coin identifier (signed with the bank digital signature), e-coin value, and predefined expiration date.

When endorsing a transaction, an endorser attaches to an endorsement message, an e-coin equivalent to the endorsed amount of that transaction. (The e-coin is part of the endorsement message and every endorsement message is signed by the endorser.). If the endorsed customer does not default in payment, the bank will reissue the e-coin to the endorser. Otherwise, the corresponding amount of deposit will be paid by the endorser. Therefore, colluding by the customer and the endorser is prevented by checking whether there is an e-coin attached to the endorsement message.

3.4.2 Event Chain with Light Weight Scheme

We adopt an event chain scheme with a light weight scheme as a solution to double spending in our system. A Bloom filter is used to represent all the spent e-coins since the beginning time of the event chain, i.e., all spent e-coins are mapped into the Bloom filter. Instead of recording all the IDs of the spent e-coins in the event chain, only the hash value of the latest Bloom filter is recorded in the event chain. To spend a new e-coin, the endorser calculates the hash value of the last block, and sends it with his/her endorsement message to a monitor. On receiving the endorsement message, a monitor checks the validity of the event chain, and if the event chain is valid then the monitor confirms if the e-coin is already added to the Bloom filter. Hence, the monitor adds the e-coin to the Bloom filter, and signs on the combination of hash values, GPS coordinates, timestamp, and a new event to the event chain. The latest hash value of the Bloom filter is added to the event chain as part of the new event by the monitor. Then the monitor broadcasts the updated Bloom filter to other neighboring users.

In a situation where an endorser tried to use an already spent e-coin in a new transaction, a monitoring user after accepting the endorsement message will detect that the e-coin is already added to the Bloom filter. All past events of the endorser are recorded to form an event chain, which can be verified by any user. Each user retains the event chain as their transaction log. When a new event is created, a new block is concatenated to the previous event chain. We also incorporate the technique called Markle Tree [4] to reduce the size of log to be checked. During a transaction, only the pruned event chain and the Bloom filter need to be checked.

3.4.3 Location Information Based Monitoring

In our endorsement-based mobile payment system, a location information-based monitoring scheme is used to prevent collusion using stolen phones. Each endorser will constantly exchange HELLO messages with monitoring nodes to show that the endorser is in a particular location at a particular time. A HELLO message contains a tag with the coordinates obtained from the GPS of the endorser's phone; and the same event chain block is appended to the end of each HELLO message each time a new event is created. By collecting HELLO messages signed by other nodes, a node can prove that it is at a particular point at that time. Other users of the system can monitor the endorser's transaction location by checking the endorser's log of the event chain (or the log since the e-coin was received) and compare it with the event chain at the end of the previous HELLO message exchanged by the endorser. If an endorser fails to exchange HELLO messages with other users for several time intervals, this would indicate that the endorser is no longer within the range or connectivity loss happens. Phones that share similar location histories cannot be used as monitoring nodes.

3.4.4 Blind Signature

A monitoring node may check through the message to see the user information such as transaction message, the type of item to buy, customer identity information and so on. Having access to such information, the monitoring node may try to impersonate the customer by copying the personal information, transaction message or the information to profile the customer. We adopt the blind signature techniques to restrict the monitoring node access to only the information (such as event chains, e-coin information) needed for monitoring purposes alone, thereby ensuring that users' anonymity is protected in the system.

3.4.5 Chains of Endorsers

According to this method, it is possible that the number of endorsers available does not suffice to cover the transaction amount, or the customer does not know enough people to endorse him, this will lead to a shortage of money to pay to the merchant. This can be detected by checking the e-coin attached to every endorsement message, but it will lead to the merchant declining the endorsement message every time the e-coin is less than the transaction amount.

To prevent this and to ensure that the customer can buy an item even when some of the endorsers are not available or when the endorsers' money is insufficient, we introduce chains of endorsement where endorsers have their own endorsers that can inherit transactions to be endorsed. Each customer has multiple levels of endorsers. When an endorser is not available to endorse a transaction, the merchant can search for other level endorsers of the customer (for example, level two endorsers, who are the endorsers of the unavailable level-one endorsers). The information on how the merchant can access the secondary endorsers is provided in the endorsement tree. The root of the endorsement tree is included in the customer transaction message and contains the information of the customer's secondary endorsers up to level 5.

The process is repeated until the e-coin value equals or exceeds the transaction amount. If no secondary endorser is available, the merchant can reject the transaction. In the process of searching for secondary endorsers, the merchant incurs additional communication overhead. Hence, we propose an endorsement delegation mechanism to address this problem.

4. Endorsement Delegation Mechanism

In this section, we explain our endorsement delegation mechanism for mobile payment system for disaster areas.

4.1 Payment Delegation

An endorsement delegation mechanism is a three-way agreement by which an endorser (known as primary endorser) and their own endorser (known as secondary endorser) agrees to guarantee and pay for a transaction instead of a customer. The primary endorser delegates its endorsement capabilities to the secondary endorsers whether the primary endorsers are available to endorse the same transaction or not. The merchant can access the list of the primary and secondary endorsers from the transaction message sent by the customer. The list is created before hand (that is during registration) and signed with the bank signature to avoid forgery. The endorsement delegation mechanism uses two approaches, the first approach is the half delegation and the second approach is the full delegation.

4.1.1 Half Endorsement Delegation

In this type of endorsement delegation, the secondary endorsers can only serve as proxy for primary endorsers, but are not responsible to pay the merchant in a situation where the customer fails to pay. For example, customer *A* purchases an item from merchant *M* using half endorsement delegation, only the direct endorsers to customer *A* will be charged in a situation where customer *A* fails to pay for the item, although secondary endorsers to customer *A* (that is endorsers to customer *A's* direct endorsers) may endorse such transaction. With this approach secondary endorsers are not billed for any transaction as they only assist the primary endorsers to complete their endorsement. This approach does not absolutely guarantee that a merchant will get paid as the primary endorsers signatures are not obtained for the transaction endorsed by the secondary endorsers, hence, the primary endorsers may default.

4.1.2 Full Endorsement Delegation

In this type of endorsement delegation, the secondary endorsers serve as a proxy to the primary endorsers and are responsible to pay the merchant in a situation where the customer fails to pay for the transaction. Using the same example as above, the primary and secondary endorsers are billed if they are available to endorse the transaction and customer *A* fails to pay for the transaction, thereby ensuring absolute guarantee that the merchant will get paid for the transaction.

We adopt the full delegation approach in our mobile payment system since our goal is to allow people in the disaster area to shop in a disaster area and also ensures that the merchant is guaranteed payment after every transaction.

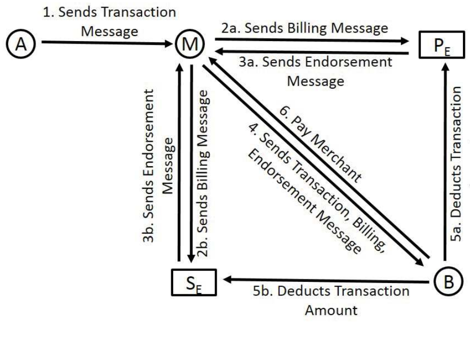
1. Sends Transaction Message
A
M
2a. Sends Billing Message
P_E
3a. Sends Endorsement Message
3b. Sends Endorsement Message
2b. Sends Billing Message
6. Pay Merchant
4. Sends Transaction, Billing, Endorsement Message
5a. Deducts Transaction Amount
S_E
5b. Deducts Transaction Amount
B

Fig. 1 Transaction using endorsement delegation. *B*: bank; *M* : merchant.

Let's consider a scenario in which customer *A* buys an item from merchant *M*, with endorser P_E as the primary endorser and endorser S_E as the secondary endorser to customer *A*. Using endorsement delegation as shown in Figure 1, the merchant sends the billing message to both the primary and the secondary endorsers to obtain their signature on the transaction as a guarantee. Unlike our previous approach in which the merchant only search for the secondary endorsers if the primary endorsers are not available, the endorsement delegation mechanism allows the merchant to send the billing message to the secondary endorsers whether the primary endorser is available or not, thereby avoiding the use of excessive communication needed to search for secondary endorsers when there are insufficient endorsers to endorse a transaction. Hence merchant overhead is reduced. This will ensure that there are more endorsers available to endorse a transaction. In a situation where the customer *A* fails to pay for the item purchased, both the primary endorser and the secondary endorser will pay instead of customer *A*.

Default Scenario 1 : When a customer defaults, the primary endorser and the secondary endorser are billed by the bank for the payment of the item. As illustrated in Figure 2, e-coins are collected from the primary endorser P_E, and the secondary endorser S_E.

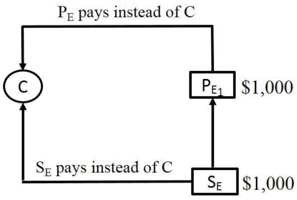

Fig. 2 Customer default scenario using endorsement delegation with sufficient money.

Default Scenario 2 : In a situation when a customer defaults and the primary endorsers do not have sufficient money to cover the payment or not available during transaction, the secondary endorsers will be charged for the transaction. Let us consider the same scenario described above, the primary endorsers (direct endorser to customer *A*) P_{E_1}, P_{E_2} and P_{E_3} do not have enough money. In this case, the secondary endorsers (for example, S_E) are charged. Each secondary endorser is charged according to the endorsement amount they agreed to endorse the primary endorser with.

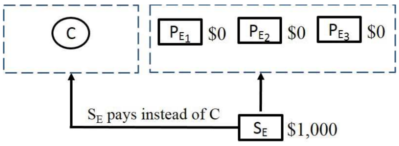

Fig. 3 Customer default scenario using endorsement delegation with insufficient amount from primary endorsers.

4.2 Transaction Process using Endorsement Delegation

The following steps illustrate the transaction process shown in Fig 4. For illustration purpose, we use monitor *D* to monitor primary and secondary endorsers, however, in our system unique neighboring users are randomly selected for monitoring.

STEP 1: Customer *A* creates a transaction order message and blinds the transaction order message using a blind signature; then computes the hash value of the last event chain block and appends it to the message; then broadcasts the message. The transaction order message includes a list of primary and secondary endorsers that customer *A* wants to delegate the transaction to.

STEP 2: Monitor *J* accepts the message and signs a combination of hash values, GPS coordinates, the timestamp and a new event; appends it to the message; then sends it to customer *A*.

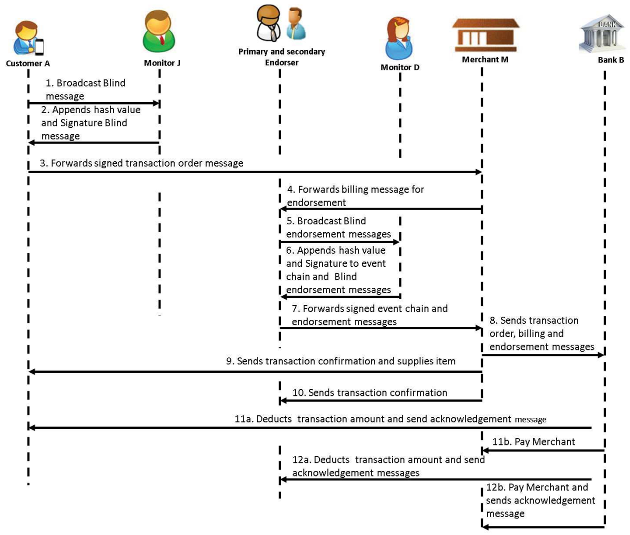
Customer A
Monitor J
Primary and secondary Endorser
Monitor D
Merchant M
Bank B
BANK
1. Broadcast Blind message
2. Appends hash value and Signature Blind message
3. Forwards signed transaction order message
4. Forwards billing message for endorsement
5. Broadcast Blind endorsement messages
6. Appends hash value and Signature to event chain and Blind endorsement messages
7. Forwards signed event chain and endorsement messages
8. Sends transaction order, billing and endorsement messages
9. Sends transaction confirmation and supplies item
10. Sends transaction confirmation
11a. Deducts transaction amount and send acknowledgement message
11b. Pay Merchant
12a. Deducts transaction amount and send acknowledgement messages
12b. Pay Merchant and sends acknowledgement message

Fig. 4 Transaction Flow using Endorsement Delegation.

STEP 3: Customer *A* unblinds the transaction order message and forwards the signed transaction order message to merchant *M*.

STEP 4: Merchant *M* checks the validity of the event chain. If the event chain is valid, merchant *M* proceeds to forward the transaction message and the billing message to primary endorser P_E and secondary endorser S_E. An invalid event chain indicates that the transaction order message is forged or was already used in a previous transaction, and the merchant will reject the transaction.

STEP 5: Primary Endorser P_E and secondary S_E create endorsement messages and blind them using a blind signature scheme; then compute the hash value of the last event chain block and append to the message the hash value and an e-coin equivalent to endorsement amount; then broadcast their messages.

STEP 6: Another monitor *D* accepts the messages and checks if the e-coins are not double spent; checks for the validity of the event chain (and the event chain of the HELLO messages); then signs a combination of hash values, GPS coordinates, the timestamp and a new event, and appends it to both messages; then sends them to both endorsers P_E and S_E.

STEP 7: Both endorsers P_E and S_E unblind their endorsement messages and forward their signed endorsement messages with an e-coin to merchant *M*.

STEP 8: Merchant *M* receives the endorsement messages from the endorsers P_E and S_E; checks the validity of the event chain and checks whether the e-coins are not double spent; sends the transaction, billing and endorsement forms to bank *B* if the event chain is valid and if the e-coin has not been double spent. If either the event chain is invalid or the e-coin has been double spent, merchant *M* will reject the transaction.

STEP 9: Merchant *M* sends a transaction confirmation to customer *A* and supplies the item to customer *A*.

STEP 10: Merchant *M* sends a transaction confirmation to the endorsers P_E and S_E.

STEP 11(a): Bank *B* authenticates the identities of merchant *M*, primary endorser P_E, secondary endorser S_E and customer *A*;

then checks for the validity of the event chain. If customer A has sufficient funds in his/her account, bank B deducts the transaction amount from customer A and sends an acknowledgment message to customer A.

STEP 11(b): Bank B pays merchant M and sends an acknowledgment message to merchant M.

STEP 12(a): If customer A does not have sufficient money, bank B deducts the transaction amount from the primary endorser P_E and the secondary endorser S_E. Then sends an acknowledgment messages to both endorsers (P_E and S_E).

STEP 12(b): Bank B pays merchant M and sends an acknowledgment message to merchant M.

4.3 Security of Endorsement-Based Mobile Payment System

By adopting various schemes in our endorsement-based mobile payment system, the following security goals are achieved after it is run successfully.

- Anonymity
- Confidentiality
- Integrity
- Double Spending Detection
- Replay Attack Protection
- Non-Repudiation of Transaction
- Reset and Recovery Attack Detection

4.3.1 Security of Endorsement Delegation Mechanism

The proposed endorsement delegation mechanism does not compromise the security of our system. The endorsement delegation mechanism adopts the use of digital signature to prevent the list of primary and secondary endorser from being forged. The endorsers list is signed with the bank signature and timestamp, hence secure from forgery.

5. Performance Evaluation

In this section we evaluate the performance of our endorsement-based mobile payment system in a disaster area using a customized simulator. Our main objectives are to ensure (i) usability of our proposed system in a disaster area, and (ii) reduction of communication cost in order to provide an excellent service for people in a disaster area.

5.1 Simulation Configuration

We conduct our simulation using a customized simulator developed in JAVA. We consider a 5 by 5 grid map with a total size of 1km by 1km. Each node moves according to the random waypoint mobility model [20] and the route is based on Dijkstra's shortest path algorithm. All nodes have the same buffer size and transmission range. We assume 802.11g wireless WiFi is used for communication. The summary of the default values used in our simulation is shown in Table 5.1.

The following metrics will be measured in our simulation.

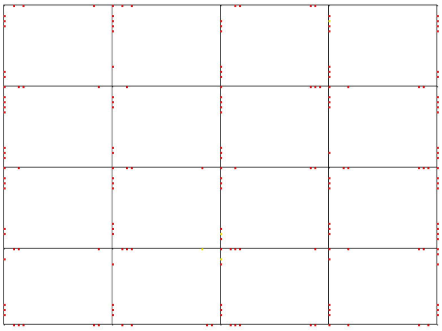

Fig. 5 Map for Simulation

Table 2 Typical simulation parameters value in a disaster area

Parameter	Default Value
Network	
Bandwidth	1 Mbps
Buffer Size	100-500KB
Transmission range	100m
Map	
Grid map size	1km x 1km
Number of mobile nodes	50–200
Node	
Speed	1 - 10m/s
Active interval	1s
Pause time	10s
Mobility Model	Random Way Point
Message	
Size	5 KB
Hello Message Size	5 bytes
Hello message Interval	10s
Bloom filter size	256bits
Transaction Settings	
Proportion of endorser to customer	1 - 12%
Number of monitoring nodes	3
Transaction amount ($)	2
Endorsement amount ($)	2
Total e-coin per endorser ($)	3000

- **Transaction Completion Ratio (TCR)**: The transaction completion ratio is defined as follows:

$$TCR = \frac{\text{Number of successful transactions}}{\text{Number of transaction messages received by merchant}}$$

- **Frequency of breakage of event chain:** The ratio at which the event chain is invalidated in our system, which is computed with the following formula:

$$Frequency = \frac{\text{Number of rejected transaction by merchant}}{\text{Number of received messages by merchant}}$$

- **Communication overhead**: The size of the message needed by the merchant to check the validity of an event chain and to contact secondary endorsers in a successful transaction.
- **Transaction completion time:** The time interval from the time a customer initiates a transaction to the time the merchant accepts the transaction and supplies the items.

We examined other scenarios in our simulation by varying different parameters as below to check how these parameters impact the performance of our system.

(1) Endorser density
(2) Merchant density

(3) Monitoring nodes density
(4) Nodes mobility speed

5.2 Transaction Completion Ratio

We evaluated the transaction completion ratio to determine the usability of our system in a disaster area. Specifically, two scenarios were considered: the first scenario is the normal endorsement where transactions are endorsed by primary endorser only. The second scenario considered is the enhanced endorsement where transactions are endorsed by primary and secondary endorsers. All simulated results in figures below are averaged over 12 simulation runs.

5.2.1 Transaction Completion Ratio of Normal Endorsement

Figure 6 shows the completion ratio against time. The result shows that the normal endorsement achieved an average transaction completion ratio of 42% for 50 mobile nodes, 40% for 100 mobile nodes and 37% for 200 mobiles. The transaction completion ratio decreases as the number of mobile nodes increases this is because as the number of mobile nodes increases the number of transaction message sent also increases while the number of successful transactions does not increase much due to limited endorsers.

5.2.2 Transaction Completion Ratio of Enhanced Endorsement

As shown in Figure 6, the transaction completion ratio increases significantly with 95% for 50 mobile nodes, 77% for 100 mobile nodes and 48% for 200 mobiles. Although the transaction completion ratio decreases as the number of mobile nodes increases, the proposed enhanced endorsement achieves better performance when compared with the normal endorsement with an increase from 11% to 52%. The significant increase is as a result of having more endorsers to guarantee customer transactions. We achieved this with the introduction of the endorsement delegation. We can also observe that the transaction completion ratio increases as time increases, this is because simulations are in a transient stage from 900s to 7000s, and from 7000s to afterwards simulations reach a steady stage.

5.3 Frequency of Breakage of Event Chain

Another metric we measured is the frequency of breakage of an event chain. In our mechanism, we introduced event chains to prevent double spending. However, event chain may be invalidated if dishonest users in the network double spend e-coins, complete a transaction without e-coins, try to complete a transaction without a monitoring node's signature, or too many nodes share similar location history. The simulation results of the frequency of breakage of an event chain is shown in Figure 7. The results indicate that there is a decrease in the frequency of breakage of the event chain for different scenarios with 50, 100 and 200 mobile nodes when the proposed endorsement delegation mechanism is used in our system. Specifically, when the enhanced endorsement is used in our system, there is a decrease ranging from 12% to 52% in event chain breakage when compared with the normal endorsement chain.

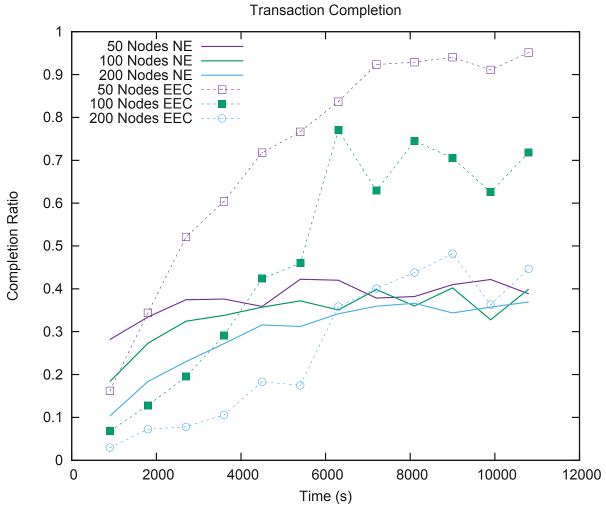

Fig. 6 Transaction completion ratio (NE : Normal Endorsement, EEC : Enhanced Endorsement Chain, endorser = 2, merchant = 1 and monitoring node = 3).

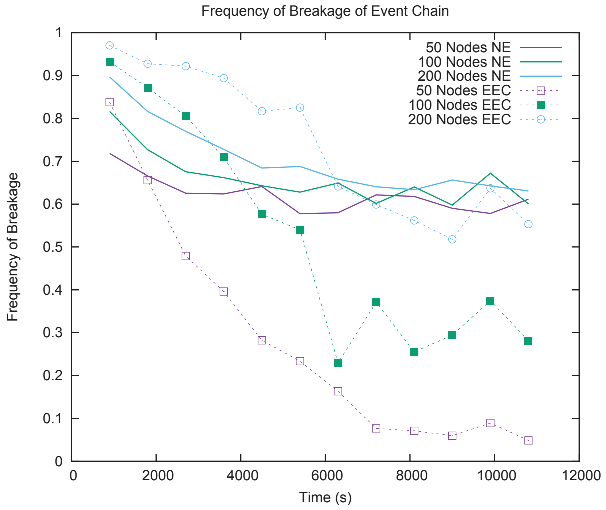

Fig. 7 Frequency of breakage of an event chain (NE : Normal Endorsement, EEC : Enhanced Endorsement Chain, endorser = 2, merchant = 1 and monitoring node = 3)

5.4 Communication Overhead

Our goal of introducing the endorsement delegation is to reduce merchant overhead when enhanced endorsement chain is used, we also evaluated the merchant communication overhead of our previous event chain as against the merchant overhead of our proposed enhanced endorsement chain. As shown in Figure 8, when compared to the merchant overhead in our previous endorsement chain, there is a 10% decrease in merchant overhead in our MPS with enhanced endorsement chain for different scenarios with 50, 100 and 200 mobile nodes. In all scenarios, the simulation result shows that the merchant overhead of our enhanced MPS is 12KB on average, a half of that of our previous MPS, indicating that our enhanced MPS with endorsement delegation is storage-efficient for mobile devices with limited resources in disaster areas.

5.5 Transaction completion time

Another metric evaluated in our simulation is the transaction

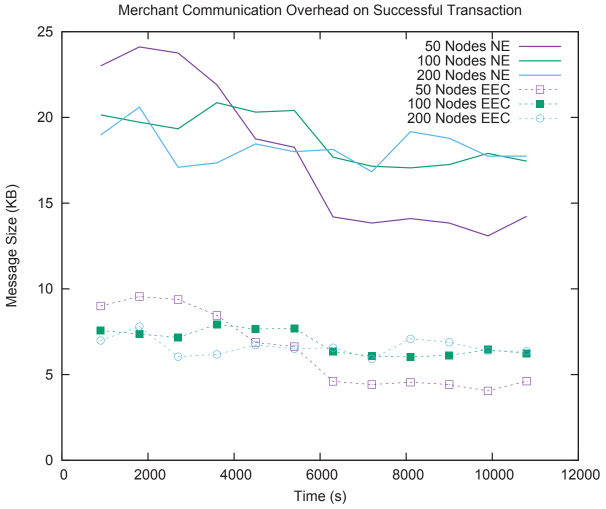

Fig. 8 Merchant communication overhead in successful transactions (NE : Normal Endorsement, EEC : Enhanced Endorsement Chain, endorser = 2, merchant = 1 and monitoring node = 3).

completion time of service. The advantage of our proposed system is that the completion time is less than 1s which makes transactions in our endorsement mobile payment system to have faster execution.

5.6 Effect of Various Parameters on Transaction Completion Ratio

We also examined the effect of endorsers density, monitoring node density, mobile node's mobility speed and merchant density on transaction completion ratio. First, we set the number of endorsers to be proportional to the number of mobile nodes. We varied endorsers proportion from 2% to 12%.

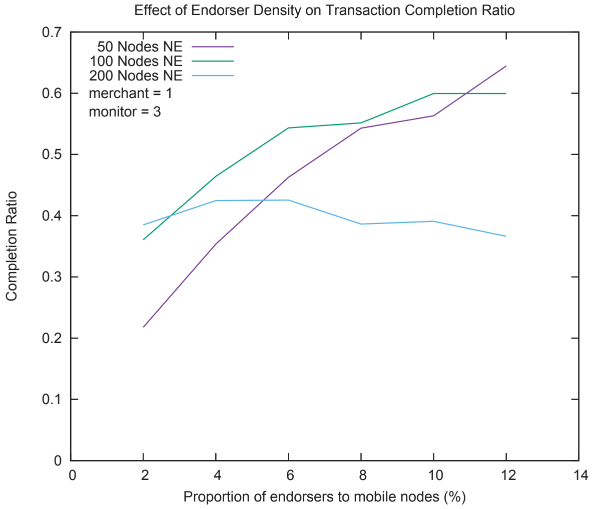

Fig. 9 Effect of endorser density on transaction completion ratio.

5.6.1 Endorser Density

Figure 9 shows that the endorser's density has an impact on the transaction completion ratio. The transaction completion ratio increases as the number of endorsers increases, confirming the effectiveness of our enhanced endorsement mechanism. We also observe that there is a slight decrease in transaction completion ratio for for 200 nodes. This decrease is as a result of insufficient monitoring nodes with more endorsers in the system, e.g., 20 endorsers for endorser proportion being 8%.

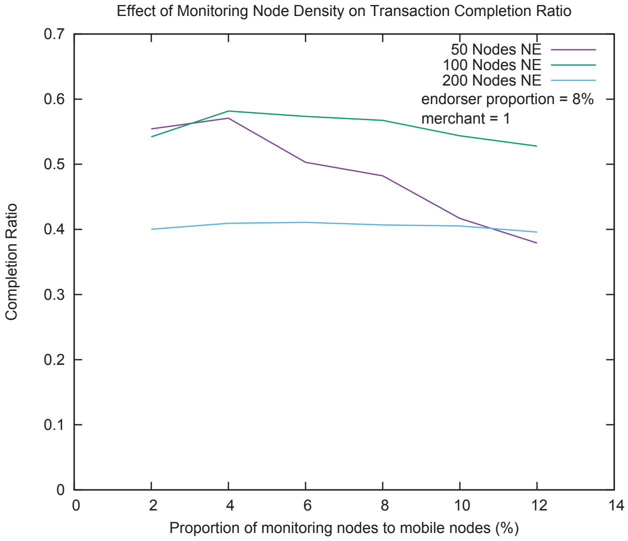

Fig. 10 Effect of monitoring node density on transaction completion ratio.

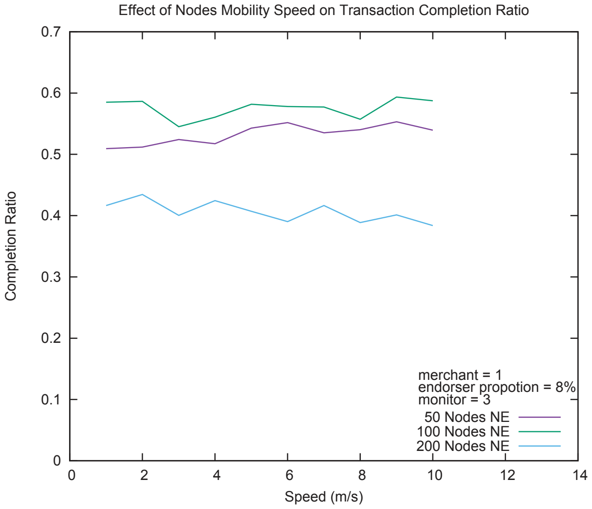

Fig. 11 Effect of nodes mobility speed on transaction completion ratio.

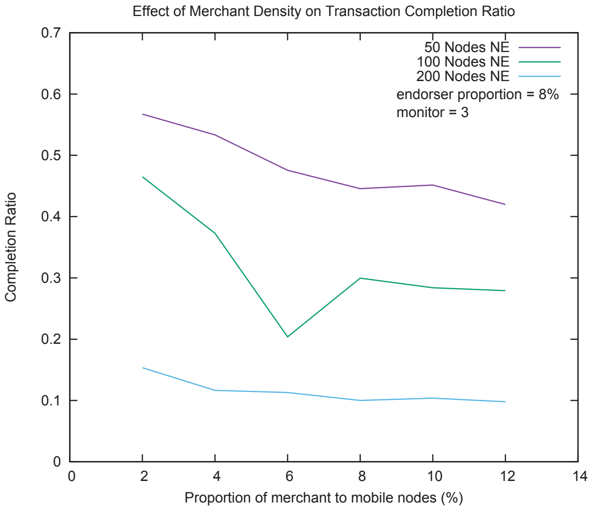

Fig. 12 Effect of merchant density on transaction completion ratio.

5.6.2 Monitoring Nodes Density

As shown in Figure 10, the transaction completion ratio decrease as the number of monitoring nodes needed to complete a transaction successfully increases. The highest transaction completion ratio achieved is when the monitoring node proportion is set to 4%. This affirmed our proposed system setting, i.e., 3 monitoring nodes for validating each message to avoid collusion.

5.6.3 Nodes Mobility Speed

Since the contact times of nodes are essential for a transaction to be successful, we evaluate the impact of node's mobility speed on transaction completion ratio. The result is shown in Figure 11 with almost constant transaction completion ratios. According to the result, node's mobility speed has no significant effect on the transaction completion ratio as the mobility speed increases.

5.6.4 Merchant Density

We also check the effect of merchant density on transaction completion ratio in our system. Figure 12 shows the transaction completion ratio when the proportion of merchant density is varied from 2% to 10%, with an endorser density of 8%. Based on the result, the transaction completion ratio decreases as the number of merchant increases. Although the transaction messages received by the merchant increases, the transaction completion ratio increases only if there are enough endorsers and monitoring nodes to endorse and monitor transactions. Thus an increase in merchant density will only improve transaction completion ratio when the endorser density has also increased and the number of monitoring nodes available is sufficient to monitor transactions.

6. Conclusion

In this paper, we proposed an enhanced mobile payment system with endorsement delegation reduce merchant overhead and transaction completion time. We adopt the full endorsement delegation to ensure an absolute guarantee that a merchant will get paid after every transaction. Through simulation, we showed that our endorsement based mobile payment system is useful in disaster areas. Specifically, we evaluated the transaction completion ratio, frequency of breakage of an event chain, merchant communication overhead and transaction completion time of our system. The new introduced endorsement delegation achieved better transaction completion ratio with an increase of 11% to 52% when compared with normal endorsement without endorsement chain. Also, our results showed that endorser and monitoring node density have significant impact in ensuring customer transaction are completed successfully. We expect better performance if the density of endorsers is made to be directly proportional to the number of uses in the system. In addition, merchant and monitoring density need to be taken into consideration to achieve better performance. For future work, we will evaluate our enhanced mobile payment system through extensive simulations on a real map within the vicinity of the Takayama Science Town, NAIST, Japan.

References

[1] Ojetunde, B., Shibata, N., Gao, J., and Ito, M.: An Endorsement Based Mobile Payment System for A Disaster Area, *in Proc. of The 29th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015)*, pp. 482-489, March. 2015.

[2] Ojetunde, B., Shibata, N., Gao, J., and Ito, M.: Simulation-Based Evaluation of a Mobile Payment System Utilizing MANETs for a Disaster Area, *DICOMO 2015*, pp.757-766, July 2015.

[3] Mishra, A. and Nadkarni, K. M.: *Security in Wireless Ad Hoc Networks*, The Handbook of Ad Hoc Wireless Networks, chapter 30, pp. 479, CRC Press LLC, (2003).

[4] Nakamoto, S.: Bitcoin: A peer-to-peer electronic system, available from ⟨http://bitcoin.org/bitcoin.pdf⟩ (2008) (Online).

[5] Patil, V. and Shyamasundar, R. K.: An efficient, secure and delegable micro-payment system, *Proceeding of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, (EEE '04)* pp. 394 - 404 March 2004.

[6] Chen, Y. Y., Jan, J. K., and Chen, C. L.: A Novel Proxy Deposit Protocol for E-cash Systems, *Applied Mathematics and Computation*, Vol. 163, Issue 2, pp. 869-877, 2005.

[7] Kiran, N. C., and Kumar, G. N.: Implication of secure micropayment system using process oriented structural design by hash chain in mobile network, *IJCSI International Journal of Computer Science Issues*, vol. 9, no. 2, January 2012.

[8] Dai, X., Ayoade, O., and Grundy J.: Offline micro-payment protocol for multiple vendors in mobile commerce, *in PDCAT '06 Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE Computer Society*, 2006.

[9] Hu, Z., Liu, Y., Hu, X., and Li J.: Anonymous micropayments authentication (AMA) in mobile data network, *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, Vol 1, pp. 53, March 2004.

[10] Wang, J. S., Yang F. Y., and Paik I.: A novel E-cash payment protocol using trapdoor hash function on smart mobile devices, *IJCSNS International Journal of Computer Science and Network Security*, Vol. 11, No. 6, pp. 12-19, June 2011.

[11] Yang F. Y.: Efficient Trapdoor Hash Function for Digital Signatures, *Chaoyang Journal*, Vol. 12, pp. 351-357, 2007.

[12] Yang F. Y.: Improvement on a Trapdoor Hash Function, *International Journal of Network Security*, Vol. 9, No. 1, pp. 17-21, July 2009.

[13] Chang C. C., Chang S. C., and Lee J. S.: An on-line electronic check system with mutual authentication, *Computers and Electrical Engineering*, Vol. 35, No. 5, pp. 757-763, 2009.

[14] Chaum D., Den Boer, B., Van Heyst, E., Mjlsnes, S., and Steenbeek, A.: Efficient offline electronic checks, *EUROCRYPT '89 Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pp. 294-301, Springer-Verlag New York, Inc., New York, NY, USA, 1990.

[15] Chen, W.: Efficient on-line electronic checks, *Appl. Math. Comput.* , Vol. 162, No. 3, pp. 1259-1263, Elsevier Science Inc., New York, NY, USA, March 2005.

[16] Liaw, H. T., Lin J. F., and Wu, W. C.: A new electronic traveler's check scheme based on one-way hash function, *Electronic Commerce Research and Applications* , Vol. 6, No. 4, pp. 499-508, 2007.

[17] Li W., Wen, Q., Su, Q., and Jin, Z.: An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network, *Comput. Commun.* , Vol. 35, no. 2, pp. 188-195, Jan. 2012.

[18] P. Lin, H. Chen, Y. Fang, J. Jeng, and F. Lu: A secure mobile electronic payment architecture platform for wireless mobile networks, *IEEE Trans. Wireless Commun.* , Vol. 7, no. 7, pp. 2705-2713, July 2008.

[19] Tewari H., O'Mahony D., and Peirce, M.: Reusable off-line electronic cash using secret splitting, *Trinity College, Computer Science Department, Tech. Rep.* , 1998.

[20] Camp, T., Boleng, J., and Davies, V.: A survey of mobility models for ad hoc network research, *Wireless Communications and Mobile Computing*, vol.2, pp.483-502, 2002.