Vol.2014-CSEC-66 No.5
Vol.2014-SPT-10 No.5
2014/7/3

Consideration of a Mobile Payment System using Endorsement in MANETs for a Disaster Area

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

Abstract: Payment system in the disaster area is essential for people to buy necessary amenities, like groceries, clothing, medical supplies. However, due to the lack of infrastructures in disaster areas, existing payment systems cannot be applied directly to such scenarios because they either require direct connection to the payment authorities or cannot prevent fraudulent transactions. In this paper, we propose a mobile payment system by adopting infrastructureless mobile ad-hoc networks (MANETs), which can allow users to purchase amenities in disaster areas while providing secure transactions. Specifically, we propose an endorsement-based scheme to verify each transaction and location information based monitoring scheme to achieve transaction validity and reliability. By employing blind signature and one-time session token techniques, our mobile payment system can also prevent double spending and replay attacks.

Keywords: Endorsement, mobile payment system, e-coin, token, reset-and-recovery, hash-function

1. Introduction

One of the major problems in disaster areas is that people there do not have cash on hand to pay for necessary amenities (e.g., groceries, clothing and medical supplies). Moreover, due to the lack of communication infrastructures in disaster areas, people can neither access their bank accounts to make electronic financial transactions. Therefore, an infrastructureless payment system is vital for people in disaster areas to buy life-maintaining goods.

Although wireless mobile ad-hoc network could be used cost effectively to provide a payment system solution that can work in an infrastructureless environment, such technology comes with many security issues [1]. Also, the mobile environment comes with more issues which include limited storage size, limited computational capabilities and limited bandwidth of the mobile network [2]. In addition, the dynamic topology of mobile ad-hoc network makes it difficult to provide a secure payment system where there is no direct connection to the payment source during the transaction. Most of the current studies on payment systems ensure reliability and validity of a transaction in the network by verifying each transaction with the financial institution, thereby avoiding fraud in the network. Researchers have successfully developed many payment systems and security protocols that make payment system more secure and usable to users and merchants alike, but there has been little work done in the area of wireless mobile ad-hoc networks. Furthermore, no mobile payment system has been developed that addresses the needs of people in a disaster area because most of the focus has been on rebuilding the area and relocating people. Hence, this paper proposes a new payment system using endorsement in mobile ad-hoc network.

In this paper, we propose a system that will provide mobile payment for allowing customers to buy items from a merchant after disaster has happened. This will ease the difficulty of doing transaction in case of non-availability of network infrastructure. The proposed system is based on endorsement; that is, each user on the network will select people to endorse them and their digital signature is obtained on every transaction as proof of endorsement. This will ensure that the merchant gets paid after each successful transaction. Thus, in the case where a customer buys an item and did not pay, the money can be deducted from the endorsers. Moreover, since there is no direct connection with the payment source, it is not possible to achieve transaction validity and reliability. Thus, in the proposed method, we introduce monitoring based on location information. This will not only make transaction valid and reliable but also prevent double spending in the network. To prevent impersonation and fraud, identity of the other party by digitally signed picture is introduced. Although the proposed system can work both online and offline, this paper focuses on offline transaction over mobile ad-hoc network.

The rest of this paper is organized as follows. We review related literature on mobile payment systems in Section 2. In Section 3, we present the overview of the proposed mobile payment system and propose in Section 4 various schemes to provide secure transactions. Finally, we show in Section 5 the evaluation of the proposed system and conclude the whole paper in Section 6.

2. Related Work

Electronic commerce and micropayment systems have evolved from one form to another ever since its creation. Such forms range from desktop applications to web applications and, more recently, mobile applications. These systems allow users to carry

[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

out purchases directly using their mobile devices. Mobile payments started with the use of short message service (SMS) but now there are payment systems that use wired and wireless systems but very limited research is carried out in the area of mobile payments using a mobile ad-hoc networks. Also, it is difficult to provide mobile payment system using mobile ad-hoc networks due to the following features of ad-hoc networks [3]:

- `Unreliability wireless link between nodes.` Mobile ad-hoc network is characterized with limited energy, which makes it difficult to maintain a consistent wireless link for communication between participants.
- `Constantly changing topology.` Topology changes very rapidly in mobile ad-hoc network due to movement of nodes in and out of the network. This also results in a decrease in performance as it is hard to route data with an increase in the overhead.
- `Lack of incorporation of security features.` Non-availability of security features in statically configured wireless routing protocol not meant for ad-hoc environments always leads to increase in vulnerability and exposure to attacks.

Many researches have been conducted on mobile payment systems, though those research works alight and address the common features of a good payment system. Most of these research works do not really address the need of mobile payment that can function using mobile ad-hoc networks, which can also be used in a disaster area.

Hu et. al. [2] designed an innovative and practical authentication system called Anonymous Micropayments Authentication (AMA) for micropayments in a mobile data network which allows the customer and merchant to authenticate each other indirectly while preventing merchant from knowing the customer's real identity. Though the system introduces a payment mechanism that can be used both for local and roaming transactions, it also ensures that the computational overhead of the customer's mobile phone is minimized but it can only work online using wireless networks and not suitable for offline using mobile ad-hoc networks. Also, the research work considered only purchase of digital goods transaction, and not physical goods.

Chitra Kiran et. al. [1] proposed a secure and robust system for micropayment system in a wireless adhoc network using oriented architecture to carry out secure and reliable offline transaction. The paper highlights issues associated with wireless adhoc networks and other payment systems. Also the proposed system highlights a secure e-payment application that does not depend on any third party vendor and the security of the system is based on simple public key infrastructure and hash chain, implemented on a newly designed digital agreement of the broker. The system ensures cooperation of nodes by allocating payment to all nodes that permits relaying of packets in the network. The system does not support multiple brokers.

Nakamoto [4] in Bitcon: a peer to peer electronic cash system proposed an electronic cash that allows payments from one party to the other without going through any third party like a financial institution. The system addresses double spending problem using proof of work which is difficult to modify if honest nodes continue to control most of the CPU power. Nodes can leave and rejoin the network anytime but will have to accept the proof of work chain as a proof of activities that has happened when they are gone. Also messages are delivered based on best effort and this ensures privacy in the network as it is impossible to identify any nodes. Like most of the other payment systems, the proposed system work online and also requires a lot of CPU power which makes it difficult to be use for mobile phone.

Dai et. al. [5] work on Off-line Micro-payment Protocol for Multiple Vendors in Mobile Commerce is based on his previous research called NETPAY, it ensures that each mobile user's transaction does not involve any broker and double spending is detected during the redeeming of the transaction. It is used for the purchase of digital goods like in Anonymous Micropayments Authentication (AMA) for micropayments in mobile data network but allow some transaction to be done offline. The offline scenarios only apply to the vendor and not the users.

Wang et. al. [6] in his work A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices, proposed a payment system that allow customers to purchase e-cash with a fixed face value, the amount of every transaction is deducted from the customer's account, thereby reducing online computational cost of the bank. Other research works focus on e-payment systems such as electronic cash [7], electronic check [8], electronic traveler's check [9] and so on.

Most of the existing payment systems currently in use are infrastructure based which can only work online on wired and wireless networks and are not suitable for mobile ad-hoc networks. Therefore, this paper proposed a mobile payment system in mobile ad-hoc networks.

3. System Overview

3.1 Participants

The parties involved in the system will be known as users. Each user communicates using a wireless mobile ad-hoc and wired network. The basic users are a customer, endorser, merchant, and bank.

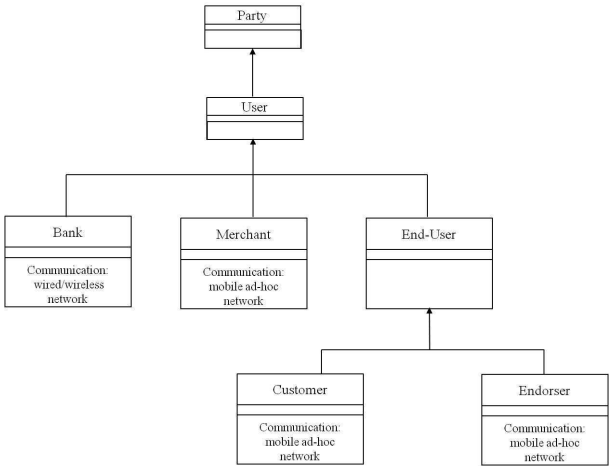

Fig. 1 Users in the System

(1) Customer - a user that buys goods, service, product, or software from a merchant for electronic money.

(2) Endorser - a user who pledges to fulfill customer's obligation should the customer fail to pay for items bought.
(3) Merchant - a user that accepts e-money in exchange for goods, service, product, or software.
(4) Bank - an organization that maintains end-users accounts.

The set of user customer, endorser, merchant and bank are denoted by C, E, M and B respectively.

3.2 Normal Transaction without Disaster

In a normal mobile payment transaction, customer can easily buy an item from the merchant and the payment is directly from the customer account or through an e-money but this is only possible when there is a direct connection to the payment source for example broker or bank as shown in **Fig. 2**.

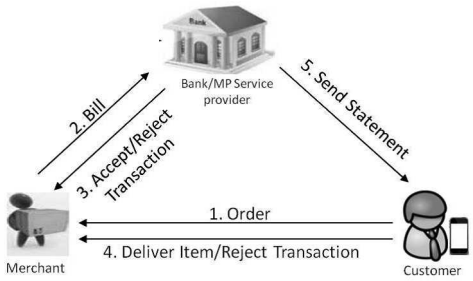

Fig. 2 Normal Transaction

The procedure to buy an item is as follows:
(1) Customer agrees to do transaction with the merchant by registering for the service.
(2) Merchant updates the item list on their platform and using the mobile phone the customer access the platform.
(3) Customer sends transaction order message to buy an item from the merchant.
(4) Merchant confirms customer identity and forwards payment information to the bank.
(5) The Bank temporarily deducts the amount from the customer and notifies the merchant to deliver the item but if there is no money in the customer's account the bank abort the transaction.
(6) Merchant notifies the customer about delivery information.
(7) If there is no complain from the customer, the bank deduct the money permanently from customer's account and pay the merchant. Then send statement to the customer.

However, it is not possible when there is no connection to the payment source which is the case in the disaster area. Some of the problems associated with the existing method, which makes it not suitable for disaster area, are listed below:

- `Non-availability of network infrastructure.` When a large-scale disaster strikes, the communications infrastructure is usually unavailable, making it difficult for any online financial transaction. We will assume that each user has access to the bank once every 2-days.
- `Fraudulent Transaction.` It will be difficult to prevent fraudulent transactions as there will be no direct connection to the payment authority. We will focus on preventing fraud and impersonation.
- `Security/Authentication Issues.` Most payment systems authenticates users and verifies every transaction with financial institution online. This is not possible in disaster area due to non-availability network infrastructure.

3.3 Transaction in Disaster Situation

Consider a disaster scenario. During this phase most of the time, the communication infrastructure is destroyed resulting in the difficulty of doing any online financial transaction. Also, the bank is not available for the people in a disaster area to get access to money in their bank account to buy necessary amenities that is needed. To provide a payment system that can work in a disaster area, our problem is to derive a mechanism that can allow customers to buy an item even when there is no connection to the bank.

In order to solve this problem, this study aims to achieve a mobile transaction in a disaster area by introducing endorsement based mobile payment system.

Endorsement: can be defined as an act of giving one's public approval or support to someone or something. In a payment system, an endorsement is when a person other than the original customer can become part of an agreement. Unlike the traditional credit card scheme, to endorse a customer, an end-user will agree by signing a form which makes him/her to be responsible to pay in a situation where the customer fails to pay for items. Moreover the end-user deposits real money as collateral. This procedure is made before disaster happens.

Using the model in Fig. 2, we can achieve a mobile payment system in a disaster area by introducing an endorser to the model.

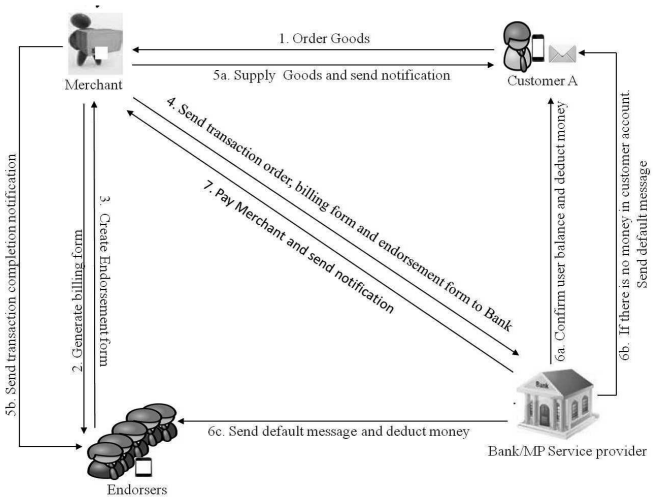

Fig. 3 Transaction in Disaster Situation

Let us say *A* and *D* are customers in a disaster area, and customer *D* agreed to be an endorser to customer *A*. The procedure to buy an item using endorsement based payment is as follows:
(1) Customer *A* sends transaction order message to buy an item from the merchant.
(2) The merchant confirms customer *A's* identity, creates a billing form and then the billing form and a transaction order message are forwarded to the endorser.

(3) The endorser confirms the merchant and customer *A's* identity, creates an endorsement form and signs the endorsement form with his/her signature. The endorser forwards the endorsement form, billing form and transaction order form to the merchant.

(4) The merchant forwards all forms to the bank and at the same time supplies the item to customer A. It may take a few days for the message to get to the bank since there is no direct connection to the bank during transaction, but the merchant will get paid since the transaction is endorsed by the endorser.

(5) After receiving the messages from the merchant, the bank confirms all user's identity and that all the information provided are genuine. Then it confirms the account balance of customer A and deducts the transaction amount to pay the merchant. However, if customer A does not have enough money to pay for the item, the money is deducted from the endorser.

With this model, we can achieve financial transaction in disaster area even though there is no direct connection to the bank. However, we still face the following problems, which will be solved in Section 4 one by one.

- `Availability of Endorsers.` Given a situation where an endorser is not available as a result of link breakage, the transaction will be delayed and the merchant will not accept the transaction order as valid.
- `Authentication and Security.` When a customer initiates a transaction in a normal payment system, each customer's credentials are checked online and access is only granted if the credentials are valid. A customer can only be impersonated, if a dishonest user is able to get the customer credentials. In a disaster area, authenticating a customer is impossible since the connection to the bank is not available as a result of non-availability of network infrastructure.
- `Reset and Recovery Attack.` Reset and recovery attack is a form of attack in which a user backups all his/her data and resets his/her phone to the default state. Then he/she recovers all valid data already used and maliciously or fraudulently use the same data to buy items. This is also a form of replay attack, where an adversary intercepts the data and retransmits it later. Consider a scenario where a dishonest user buys an item from a merchant M_1 and M_2, then backups the information used and resets the phone to the default settings. Then he/she recovers the backup message and uses the same message to buy an item from another merchant other than the merchant M_1 and M_2. We can say the user has successfully carried out a reset and recovery attack or a replay attack. Although it is possible to detect this if the user is spending money in his/her account when there is a direct connection to the bank, in an infrastructureless environment like a disaster area, this is not possible.
- `Customer and Endorser Colluding.` It is also possible for a customer and endorsers to collude to defraud the system. A dishonest customer can buy an item without having money while dishonest endorsers will endorse without having money, too. It is not possible to detect this in a disaster situation since there is no way to confirm the money in their account during the transaction.

4. Schemes Securing Mobile Payment System

In this section, we introduce techniques adopted to solve the above mentioned problems to secure transactions in mobile payment systems.

4.1 Ensuring Availability of Endorsers

To avoid the lack of endorsers, we propose chains of endorsers, where each customer can have as many endorsers as possible. In a situation where an endorser is not available to endorse a transaction, other endorsers can endorse. The more the number of endorsers of a transaction the more secure the transaction and it also ensures that the merchant will get paid. Aside from providing more than one endorser for a transaction, it ensures that the liability of endorsers on the transaction is reduced. When a customer buys an item but he/she defaults afterwards, instead of one endorser bearing the liability which may reduce the money for endorsing another customer, by introducing many endorsers, the liability for that item is equally shared between all the endorsers, thereby reducing the liability of the endorsers.

To encourage endorsers to stay honest and support the system, some part of the transaction amount (for example, 3%) is given to endorsers as a reward. When an endorser signs an endorsement form, an incentive identifier is created and attached to the endorsement form. The identifier serves as a proof for rewarding an endorser. If the money is deducted from the customer account, the endorser gets incentive, however, if a customer defaults in paying for an item, the endorser will lose the reward on that transaction.

4.2 Providing Authentication and Security

We propose the following mechanism for authenticating each user in the network.

Table 1 Proposed System Keys

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

Customer and Merchant register with the bank and exchange IDs beforehand. The bank serves as the certificate authority and issues digital certificates to all users. The registration is done offline beforehand and private key K_u^{-1} (user's private key) is used to authenticate users in the system. In addition, the customer selects a picture that will be digitally signed by the bank $S_{K_B^{-1}}$ and this is an additional authentication means during the transaction, so that this will protect the other party in case of stolen phones. The system can use another kind of biometric authentication method.

If a dishonest user tries to impersonate another user in the network, he/she will need to get the pre-signed picture of the user and the digital certificate issued by the bank to the user. Moreover, to ensure security of the transactions in the system, all messages are digitally signed and encrypted. This will prevent repudiation of transactions. Also, other users can monitor each transaction; thereby identify a dishonest user in the network. **Table 1** shows the keys which each user in the system possesses.

4.3 Preventing Reset, Recovery Attack and Colluding

We employ the following techniques to achieve the prevention of reset and recovery attack, customer and endorser colluding.

4.3.1 Technique Preliminaries

- `e-coin:` To confirm the amount in each user account.
- `The Blind Signature Scheme:` To ensure anonymity of message that is monitored by other users.
- `One-Time Session Token:` To prevent the user from using the same message again.

E-coin: The bank creates unique tokens as in [10], [11], which will be known as e-coin and will be equivalent to a user account balance, for example, e_{T_1}, e_{T_2}, e_{T_3},⋯. e_{T_n}. Each e-coin is divided into equal amount based on the money in each user account. The e-coin is encoded with the user's identity, e-coin identifier signed with bank digital signature, bank GPS coordinates as the initial GPS coordinates and two blank fields for transaction monitoring.

e-coin(e_{T1})

Customer ID	e-token Identifier & Bank Digital Signature	Bank GPS(x,y, z)	Blank	Blank

Fig. 4 Example of an initial e-token content

Although the customer can use this pre-issued e-coin to buy an item in a disaster area as a form of prepaid cash but there is no means of preventing the customer for using the same e-coin more than once. Hence, the use of an e - coin will be limited to endorsing.

An endorser attaches an e-coin to an endorsement message based on the endorsed amount of each transaction. If customers do not default in payment, the bank can reissue the e-coin with a new identifier; otherwise, the bank will permanently delete the e-coin information from the endorsers account. If an endorser sends endorsement message without attaching an e-coin equivalent to the endorsement amount, the endorsement is rejected. Only the bank can encode the e-coin identifier on the coin, therefore to avoid other users that monitor each transaction from editing the identifier, the bank signs the identifier with his digital signature. Furthermore, if an attacker tries to use a stolen phone and e-coins later, the transactions are rejected by checking of the picture.

Monitoring Based on Location Information: Each user will constantly broadcast HELLO messages to show they are in a particular place at a particular time. The HELLO message contains a tag with the coordinates obtained from the GPS of the user's phone and by showing collected HELLO messages, so that each customer can prove their location. If a customer stays in a location for a long time, other users of the system can monitor their transaction. If a user fails to broadcast HELLO messages for several time intervals to other users, it indicates that the user is no longer within the range or there is connectivity lost. When a user loses the collected HELLO messages or switches off his/her phone temporarily and cannot provide the collected HELLO messages, such a user will need to find his/her endorsers and provide endorser's confirmation to be able to do transactions afterwards.

Furthermore, the tagged GPS coordinates broadcast in the HELLO message will constantly replace the GPS coordinates of the e-coin. Therefore, an e-coin will always have the GPS coordinates of the last broadcast HELLO message and this can be verified by other users that monitor transactions. Also, the interval between the broadcast HELLO messages is added to one of the blank fields of the e-coin. The last blank field will contain the coordinates of the user that signs the transaction.

e-coin(e_{T1})

Customer ID	e-token Identifier & Bank Digital Signature	Customer Last HELLO GPS(x,y, z)	Interval between HELLO Message	Blank

Fig. 5 Example of an e-token content after GPS coordinates change

Blind signature schemes: Blind signature allows a person to get a message signed by another party without revealing any information about the message to other party. In traditional transactions, people have been using blind signatures by enclosing a message in a special envelope that is lined with a carbon paper. The outside of the envelope is signed and the carbon allows the signature to show on the message. It is used in applications where user's privacy is important and it involves two parties. However, to get a digital blind signature, the message is first covered (blinded) by xor-ing a random bits (a special envelope). The blind message is then sent to the signer, who will then sign the message without knowing the message content. The signed message can be publicly verified against the original message by using regular digital signature, as proposed in [12]. Let us say customer *A* will like to obtain customer *J* signature on a message *m* without customer *J* viewing the message. The following steps will be taken:

(1) Customer *A* creates message m and blind m by choosing a random bit *r*, raise it to the power of the public key, and multiply it by the message ($m' = m, r^e$).
(2) Customer *A* will need to send blinded message m' to customer *J*.
(3) When customer *J* received blinded message m', without opening the message, customer *J* will sign the message with his digital signature and sends the message back to customer *A*. The signed message is ($s' = (m', s)$). Customer *A* receives a signed message s', customer *A* verifies customer *J* signature with his public key to get signed message ($s = m', s$).
(4) Customer *A* remove blind factor r^e from blinded message m' and finds the customer *J* signature on message (m, s).

One-Time Session Token: One way to avoid a replay attack is by using a session token. For example, assume that user *A* and *D* want to send messages to each other and user *A* needs to identify user *D*. User *D* sends the proof of identity (e.g. password), it is possible for user *J* to eavesdrop on the message and copy the password or the means of identification. User *J* can later pose as user *D* by sending a message to the user *A* using user *D* proof of identity as a means of authentication, thereby having access to information of the user *A*. One-time session token is used to prevent user *J* from posing as user *D* as follows:

(1) User *A* will sends a one-time token to user *D*.
(2) User *D* will then find the hash function of the session token and append it to the password or a means of authentication. User *D* then sends the transformed password to user *A*.

(3) User *A* calculates the hash function of the session token he sent to user *D*; if both values match, then user *A* can accept connections from user *D*.

(4) Let us say user *J* captured this value and *J* tries to use it on another session; user *A* sends a different session token, and when user *J* replies with the captured value it will be different from user *A's* computation.

The session token is chosen by a random process to prevent user *J* from predicting future token.

4.3.2 Schemes to Prevent Attacks

To prevent users from doing many transactions with the same transaction order message, colluding between parties to do fraud or carrying out reset and recovering attacks. We will use a combination of the schemes described above. Let's look into the following scenario:

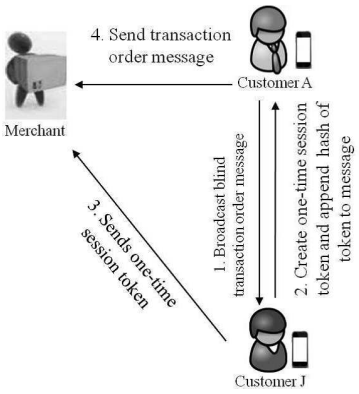

Fig. 6 Preventing replay attack with one-time session token

(1) Customer *A* creates a message and apply a blind factor to the transaction order message, this is to achieve some level of privacy.

(2) Customer *A* broadcast the message.

(3) Customer *J* will accept the message, customer *J* without knowing the information about what customer *A* want to buy, will create a one-time session token, find the hash of the one-time token and append to the transaction order message.

(4) Customer *J* then sign the message with his/her digital signature, send it to customer *A* and then customer *J* will send the one-time session token to the merchant.

(5) Customer *A* will remove the blind factor and forwards the message to the merchant.

(6) When the merchant receives the transaction order message from customer *A*, the merchant will compute the hash of the one-time session token append with the message and compare with the one-time session token received from customer *J*. if the session token does not match, it shows that the transaction message is already used and the merchant will reject the transaction.

However, if the session token matches, the merchant proceeds by forwarding the message to the endorsers. The same steps apply to the endorsement process.

Preventing Reset Attack

(1) Customer *A* reseting his/her phone.

(2) Endorser *D* reseting his/her phone.

Using the same transaction process described above, if a user attempts to use the same message with another merchant after resetting his/her phone, the merchant will request for a new one time session token from customer *J*. The merchant will detect that the message is already used if the new one time session token from customer *J* and the one in the transaction is not the same.

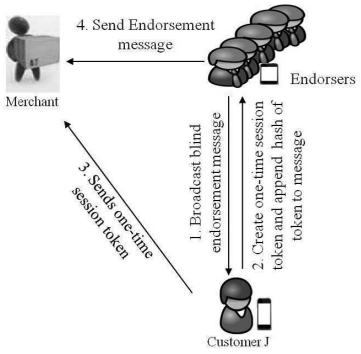

Fig. 7 Preventing reset attack

Preventing Reset Attack with e-coin

From the scenario above, we can only detect if an endorser uses the same message, which means we cannot know if there is enough money in his/her account. Hence, the e-coin scheme is added to the process of reset-and-recovery attacks for the endorsers. So, if an endorser *D* resets his/her phone to default and get all the e-coin already used and attach it to a new transaction order message. Customer *J* will first compare the HELLO message GPS and e-coin GPS coordinates' as shown in **Fig. 8**. Customer *J* will only create a one-time session token, sign the endorsement message and add his/her GPS coordinates to the e-coin, if the HELLO message GPS and e-coin GPS coordinates' are the same. However, endorser *D* can wait for the HELLO message GPS on the e-coin to update, before using it, therefore, customer *J* will also check the interval between the last two HELLO message of endorser *D*.

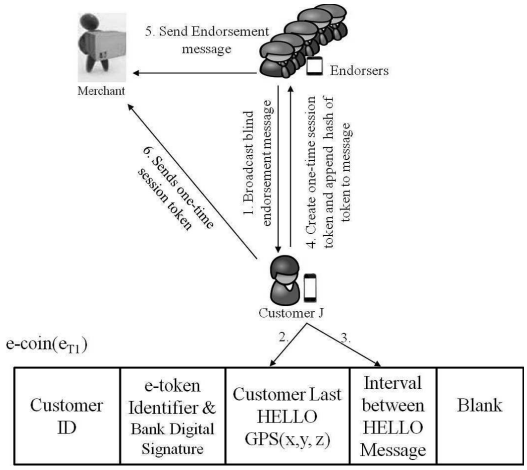

Fig. 8 Preventing reset attack with location based information

Assumption

Most of the users in the system are assumed to be trustable users that do not change location often which will make it easy to avoid fraudulent transactions. Also, it is assumed that if a user

moved to a new location and tries to buy an item from the merchant, such a user cannot be trusted and their transactions are limited according to their movement and the available endorsers at the new location.

Also, it is assumed that each endorser in the system is available during the transaction, so if a certain number of endorsers are collected, large part of them will not default in payment. Furthermore, we assume that all users are in the disaster area except the bank. Users in a disaster area communicate using mobile adhoc network while bank uses wireless or wired network to communicate. Moreover, it takes at least two days for the message to get to the bank.

We assumed that attackers are not very quick enough to carry out an attack in the same location as the user. Also, an attacker cannot get all the necessary keys and information needed before that user flag an alert. Furthermore, more than two parties will not collude to do fraud in the system.

Preventing Collusion

Other users that monitor transactions can detect if two parties colluded by checking if there is an e-coin attached to the endorsement message, since this confirms if an endorser have money in his/her account. If customer *A* buys an item without having money and colludes with some dishonest endorsers to endorse the transaction without having money, customer *J* will detect this when the endorsement message is broadcast as there will be no e-coin attached to the endorsement message. Customer *J* will reject the endorsement message.

4.4 Summary of Our Mobile Payment Protocol

The overall procedures of our proposed endorsement based mobile payment system, as shown in **Fig. 9**, are summarized as follows.

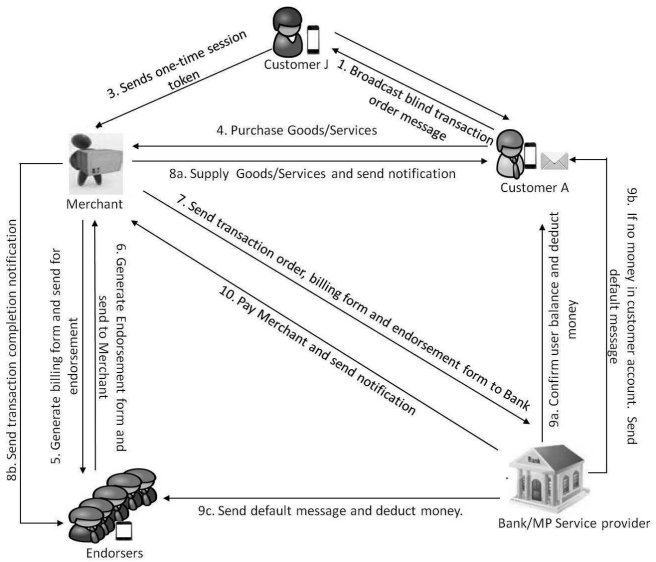

Fig. 9 Proposed System

(1) Customer *A* creates a message and apply a blind factor to the transaction order message, this is to achieve some level of privacy.

(2) Customer *A* broadcast the message.

(3) Customer *J* will accept the message, customer *J* without knowing the information about what customer *A* want to buy, will create a one-time session token, find the hash of the one-time token and append to the transaction order message.

(4) Customer *J* then sign the message with his digital signature and send it to customer *A*. Then customer *J* will send the one-time session token to the merchant.

(5) Customer *A* will remove the blind factor and forwards the message to the merchant.

(6) When the merchant receives the transaction order message from customer *A*, the merchant will compute the hash of the one-time session token appended to the message and compare it with the one-time session token received from customer *J*. if the session token does not match, it shows that the transaction message is already used and the merchant will reject the transaction. Otherwise merchant *M* proceeds to creating billing form.

(7) Merchant *M* creates a billing form and forward the billing form and transaction order form to the endorser.

(8) Endorser *D* creates an endorsement message and attach an e-coin equivalent to the endorsement amount.

(9) Endorser *D* applies a blind factor to the endorsement message alone.

(10) Endorser *D* broadcasts the message with the attached e-coin.

(11) Customer *J* will accept the message and compare the GPS coordinates of endorser *D* on the e-coin with the last broadcast GPS coordinates of the HELLO message.

(12) If the GPS coordinates are the same, customer *J* without knowing the information about what customer *A* want to buy, customer *J* will create a one-time session token, find the hash of the one-time token and append to the message. Customer *J* GPS coordinate is also added to the e-coin as proof that the transaction is monitored.

(13) Customer *J* then sign the message with his digital signature, send it to endorser *D* and then customer *J* will send the one-time session token to the merchant.

(14) Endorser *D* will remove the blind factor and forwards the message to the merchant.

(15) When the merchant receives the endorsement message from endorser *D*, the merchant will compute the hash of the one-time session token append with the message and compare with the one-time session token received from customer *J*. If the session token does not match, it shows that the message is already used and the merchant will reject the transaction, otherwise, the merchant check the e-coin details to confirm if the endorser have money and prove that the transaction is monitored.

(16) The Merchant *M* sends the item order form, bill form, and endorsement form to bank *B*. Then, merchant *M* sends transaction confirmation to the customer *A* and endorser *D*.

(17) Bank *B* authenticates merchant *M*, endorser *D* and customer *A* identities respectively. Check if the contents of item order form, endorsement form and bill form are consistent. Checks if customer *A* has enough funds in his account and deduct the transaction amount from customer *A* and pay merchant *M*.

(18) Bank *B* sends acknowledgment message to merchant *M*, en-

dorser D and customer A.

5. Evaluation

A. Security

The following goals are to be achieved for mobile payment system in a disaster area after the protocols is run successfully.

- `Goal 1:` Users can authenticate each other without a network connection with a third party.
  The users of the proposed system register with the bank. The bank serves as certificate authority and issue digital certificates to all users. Customer C authenticates each other using the digital certificates and the digitally signed picture issued by the bank. However, authentication of merchant M by customer C is with the digital certificates issued by the bank while merchant M can use both digital certificates and the digitally signed picture to authenticate customer C.
- `Goal 2:` Anonymity
  The merchant cannot identify a customer by their real name as customer's nickname TID_C is used in every transaction. The nickname TID_C can be scrambled, and this will give a customer different nickname per transaction. Users do not reveal their name to another party in the system. When transactions are broadcast to other users for monitoring, each user cannot see the content of the message because the blind signature scheme is used. However, the GPS coordinates of the e-coin attached to the message is visible for monitoring purpose.
- `Goal 3:` Confidentiality
  All messages in the network are encrypted and digitally signed by the users. If customer A send a message to merchant M, the message will be encrypted with merchant M public key and digitally sign with customer A private key. Any other user in the system will not be able to decrypt the message unless they posses merchant M private key.
- `Goal 4:` Integrity
  To ensure that messages are not modified while in transit or cannot be repudiate later, blind digital signature and one time session token scheme are used. Forms such as transaction order form, billing form and endorsement form are also digitally signed.
- `Goal 5:` Reliability
  In order to ensure consistency in transaction information and also avoid impersonation of users in a situation where their phones are stolen, monitoring based on location information is used. Each user GPS coordinates are attached to the transaction message to prove that the users are in locations they claim they are.

B. Feasibility

The payment system protocol should suit the limitations of mobile transaction in a disaster area such as non-availability of network, account balance verification, prevention of reset and recovery attacks etc. The proposed system allows mobile transaction in disaster areas as shown in **Fig. 3**, **Fig. 4**, **Fig. 7** and Fig. 8.

6. Conclusion and Future Works

In this paper, we proposed a new mobile payment system by adopting infrastructureless mobile ad-hoc networks (MANETs), which allows users to purchase amenities in disaster areas. Through the description of transaction phases of the mobile payment system, we also demonstrated that our proposed system could provide secure transactions, including preventing fraud, impersonation of users, double spending and replay attacks.

One interesting future work is to address colluding between more than two parties (e.g. merchant, endorsers and customer), as well as chains of endorsements, in which endorsers to a customer can allow their own endorsers to inherit transactions they endorse. Another interesting research direction is to further improve the anonymity of the proposed system without using a digital picture.

References

[1] Chitra Kiran, N., 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, Issue 1, No 2, January (2012).

[2] Hu, Z., Liu, Y., Hu, X., and Li, J.: *Anonymous Micropayments Authentication (AMA) in Mobile Data Network*, IEEE INFOCOM 2004 Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies Issue: 7 March (2004).

[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] Dai, X., Ayoade, O., and Grundy, J.: Offline Micro-payment Protocol for Multiple Vendors in Mobile Commerce, *(PDCAT '06 Proceedings)* Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE Computer Society Washington (2006).

[6] Wang, J., Yang, F., 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, (online), June (2011).

[7] 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, No. 2, pp. 869-877, (2005).

[8] 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).

[9] 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).

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

[11] Tewari H., O'Mahony D., and Peirce, M.: Reusable Off-line Electronic Cash Using Secret Splitting, Technical Report TCD-CS-1998-27, Trinity College, Computer Science Department, Dublin (1998).

[12] Chaum, D.: Blind Signatures for Untraceable Payments, *(Crypto '82 Proceedings)* Proceedings of Advances in Cryptology, pp. 199-203, New York, (1983).