A Proposal of an Endorsement Based Mobile Payment System for A Disaster Area

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

Abstract: Payment system in a disaster area is essential for people to buy necessary amenities, like groceries, clothing, medical supplies. However, existing payment systems require communication infrastructures (like wired networks and cellular networks) to enable transactions, and thus cannot function well in disaster areas where these communication infrastructures may be likely destroyed. Therefore, an infrastructureless payment system is required. 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 guarantee each transaction and a location information based monitoring scheme to achieve transaction validity and reliability. By employing e-coin, blind signature and one-time session token techniques, our mobile payment system can also prevent collusion, reset and recovery attacks. Also, we introduced chains of endorsement to ensure that transactions are not delayed or unsuccessful when endorsers are not present during the transaction.

1. Research Background

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 (like wired networks and cellular networks) in disaster areas, people can neither access their bank accounts to make electronic financial transactions nor through other mobile devices. Therefore, an infrastructureless payment system which can function well without support of communication infrastructures is vital for people in disaster areas to buy life-maintaining goods.

Although many works have been conducted on payment systems, most of these works depend on infrastructures (online services) to enable and secure transactions in the payment system, and thus not suitable for disaster areas. For example, Hu *et al.* [1] designed an online working authentication system (called Anonymous Micropayments Authentication) to allow a customer and a merchant to authenticate each other indirectly while preventing the merchant from knowing the customers real identity. Nakamoto [2] also proposed an online working payment system based on the concept of electronic cash, however, requiring high power of device CPU. Dai *et al.* [3] recently developed an offline payment system, however, they are only for digital goods and only apply to vendors not users.

Since in areas without disaster, there is a direct communication connection through infrastructures (like wireless base station) to the payment source (for example broker or bank), a customer can easily buy an item from a merchant and the payment is deducted directly from the customer's bank account. Such payment system could work well in areas of no disaster, however, fail to function in areas with disaster, due to non-availability of network infrastructure, non-availability of bank, fraudulent transaction and impersonation and security/authentication issues.

2. Proposed System

To enable offline financial transactions in disaster areas without communication infrastructures, we propose an endorsement based mobile payment system by adopting infrastructureless mobile ad hoc network.

With the endorsement mechanism, we can achieve a mobile payment system in a disaster area even if the bank is not available.

Endorsement: In a payment system, endorsement is one mechanism such that a user (referred to as an endorser hereafter) agrees by signing a form to be responsible to pay for a customer in case the customer fails to pay a merchant. The endorser should deposit real money in a bank before disaster happens.

For example, let us say endorser E agrees to endorse customer A. For customer A to buy an item from a merchant using an endorsement based payment system, he/she will:

(1) Customer A sends transaction order message to buy an item from the merchant, (e.g. a bag of rice worth $50).

(2) The merchant creates a billing message and request for the endorser to guarantee the transaction by forwarding the billing and transaction messages to the endorser.

(3) The endorser creates an endorsement message, indicating that he/she accepts to guarantee the transaction and signs the

[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

endorsement message with his/her signature. The endorser forwards the endorsement message to the merchant.

(4) The merchant forwards all messages to the bank and supplies the item to customer *A*.

(5) 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 and pays the merchant. However, if customer *A* does not have enough money to pay for the item, the money is deducted from the endorser *E*.

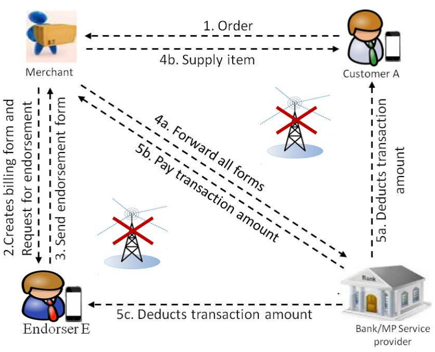

Fig. 1 Transaction process in an endorsement-based payment system without network infrastructure

(1) **Problem (Authentication and Security) :** 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.

Solution (Digitally Signed Picture): We propose using digitally signed picture as an offline mechanism for authenticating each user in the network. (This is the same as checking an individual picture on his/her identity card, though the merchant will also confirm the bank and the customer digital signature on the picture). In addition, users' private keys are used to authenticate users in the system.

(2) **Problem (Customer and Endorser Colluding) :** It is possible for endorsers and a customer to collude to defraud the payment system, since there is no way to confirm the money in their account during the transaction in a disaster area.

Solution (E-coin Balance Checking): We employ the e-coin technique to check bank account balance of endorsers to prevent colluding (The bank creates unique e-coins, similar to tokens and issue it to endorsers). When endorsing a transaction, an endorser attaches an e-coin to an endorsement message equivalent to the endorsed amount of that transaction (the e-coin is part of the an endorsement message and every endorsement message is signed by the endorser). If an endorser sends endorsement message without attaching an e-coin equivalent to the endorsement amount, the endorsement is rejected by the bank.

(3) **Problem (Confirming Transaction Location Source) :** It may happen that an attacker stoles the phone of a customer or endorser and tries to do a transaction with the phone in another location. Also, customers or endorsers may do a transaction in a location other than their usual locations and then deny making such a transaction.

Solution (Location Information Based Monitoring): Under this scheme, each customer and endorser will constantly broadcast HELLO messages and by showing collected HELLO message, each customer or endorsers can prove they are in a particular location at a particular time. The HELLO message contains a tag with the coordinates obtained from the GPS of the customer and endorser's phone. Other users of the system can monitor their transaction by checking their location information from HELLO message. In addition, to monitor the location information of endorsers, each endorser will add their GPS coordinates to the e-coin and sign it with their digital signature. This can be verified by other monitoring nodes by comparing their GPS coordinates on the e-coin with those in the HELLO message that have been previously broadcasted by the endorser. If the GPS coordinates and the HELLO message intervals are not the same with previous ones, a monitor will reject the e-coin usage and thus the endorsement message including that e-coin.

(4) **Problem (Reset and Recovery Attack):** Reset and recovery attack is a form of attack in which a user (either a customer or an endorser) backups all transaction data already used to buy an item (transaction order message or endorsement message), and resets his/her phone to the default state. Then he/she recovers all valid transaction data and maliciously or fraudulently uses the same data to buy items. It is not possible to detect in an infrastructureless environment like a disaster area.

Solution (One-Time Session Token and Blind Signature): To prevent a user (customer or endorser) from doing many transactions with the same transaction order message (already endorsed) to carry out reset and recovery attacks, we propose the following schemes by employing techniques of one-time session token (to prevent a user from reusing the same message) and blind signature (to ensure anonymity of the message).

Blind signature: It allows a person to get a message signed by another party without revealing any information about the message to that party.

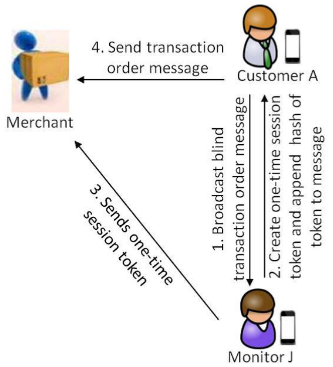
4. Send transaction order message
Customer A
Merchant
1. Broadcast blind transaction order message
2. Create one-time session token and append hash of token to message
3. Sends one-time session token
Monitor J

Fig. 2 Preventing reset and recovery attack from a customer

Preventing attack from a customer: The scheme is illustrated in Figure 2.

(a) Customer *A* creates a transaction order message and blinds the transaction order message using blind signature. Customer *A* then broadcasts the message.

(b) Monitor *J* accepts the message, and creates a one-time session token, finds the hash function of the one-time token and appends it to the transaction order message. Monitor *J* then signs the message (including the token) with his/her digital signature and sends it to customer *A*.

(c) Monitor *J* then sends the one-time session token to the merchant.

(d) Customer *A* unblinds the transaction order message, and forwards the signed transaction order message to the merchant.

(e) The merchant then compute the hash function of the one-time session token received from monitor *J* and compare it with the one-time session token in the transaction order message received from customer *A*. If the one-time session token matches, the merchant proceeds by forwarding the message to the endorsers. Otherwise, the merchant will reject the transaction.

Preventing attack from an endorser: The same transaction process described above is adopted except that a monitor creates a one-time session token, signs the last blank field of the e-coin and endorsement message with his/her digital signature, only if the GPS coordinates and HELLO message interval are the same with previously broadcasted ones. Otherwise, the monitor will reject the endorsement message.

(5) Problem (Availability of Endorsers) : Given a situation where an endorser is not available as a result of communication breakage (i.e., the endorser is not available for service), the transaction will be delayed and the merchant will not accept the transaction order as valid.

Solution (Chains 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. To encourage endorsers to stay honest and support the mobile payment system, some part of the transaction amount (e.g., 3%) is given to endorsers as a reward.

Moreover, in a situation where the number of endorsers available to endorse a transaction is not enough to cover the transaction amount or the customer does not know enough people to endorse him to use the system, this will lead to shortage of money to pay the merchant. To avoid this and ensure that customer can still buy an item, we introduce chains of endorsement in which endorsers to a customer can allow their own endorsers to inherit transactions they endorse.

The merchant, after receiving the endorsement message from endorsers, confirms if the e-coins are less than transaction amount. If the e-coins value are more than the transaction amount, the merchant proceeds to forward all the information to the bank. However, if the e-coin values are less than the transaction amount, the merchant obtains the level two endorsers information from the endorsement tree header, (The endorsement tree header provides information about how the merchant can get access to the secondary endorsers), that is created in the customer transaction message (each endorser has the information of their secondary endorsers up to level 5 in the endorsement tree header. Then merchant can search for level two endorsers of the customer (that is endorsers to the unavailable level 1 endorser) and forwards the billing information to them.

3. Evaluation

The following goals can be achieved for mobile payment system in a disaster area after our proposed system is run successfully.

- Feasibility: Our proposed mobile payment system suits the limitations of mobile transaction in a disaster area such as non-availability of the network, account balance verification, prevention of reset and recovery attacks, etc.
- Authentication: In our system, the bank serves as certificate authority and issues digital certificates to all users and users can authenticate each other without a network connection with a third party. A Customer authenticates a merchant using the digital certificates issued by the bank while a merchant can use both digital certificates and the digitally signed picture to authenticate a customer.
- Anonymity: When broadcasting transaction messages, users do not reveal the content of the message because the blind signature scheme is used. Furthermore, a customer nickname is used instead of real name in each transaction.
- Confidentiality: All messages in the network are encrypted and digitally signed by users.
- Integrity: To ensure that messages are not modified while in transit or cannot be repudiated later, blind digital signature and one time session token scheme are used.
- Reliability: In order to ensure consistency in transaction information and also avoid impersonation of users in a situation where their phones are stolen, location information based monitoring is used. Each user GPS coordinates are attached to the transaction message to prove that the users are in locations they claim they are.

4. Future Work

To ensure the proposed Payment System protocol is able to function adequately in the real world, there is need to evaluate the payment system protocol method using simulation. Also, there is a need to extend the protocol to ensure that the merchant is able to spend money received from customers without depositing to the bank.

References

[1] 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).

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

[3] 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).