An Endorsement-based Mobile Payment System for a Disaster Area

Babatunde Ojetunde*, Naoki Shibata*, Juntao Gao*, Minoru Ito*
*Graduate School of Information Science, Nara Institute of Science and Technology, Nara, Japan
Email: {ojetunde.babatunde.nq3, n-sibata, jtgao, ito}@is.naist.jp

***Abstract*—A payment system in a disaster area is essential for people to buy necessities such as groceries, clothing, and medical supplies. However, existing payment systems require the needed communication infrastructures (like wired networks and cellular networks) to enable transactions, so that these systems cannot be relied on in disaster areas, where these communication infrastructures may be destroyed. In this paper, we propose a mobile payment system, adopting infrastructureless mobile ad-hoc networks (MANETs), which allow users to shop in disaster areas while providing secure transactions. Specifically, we propose an endorsement-based scheme to guarantee each transaction and a scheme to provide monitoring based on location information, and thus achieve transaction validity and reliability. Our mobile payment system can also prevent collusion between two parties and reset and recover attacks by any user. Security is ensured by using location-based mutual monitoring by nearby users, avoiding thereby double spending in the system.**

I. Introduction

A major problem in disaster areas is that people there do not have cash on hand to pay for such necessities as groceries, clothing and medical supplies. Moreover, due to the lack of communication infrastructures (like wired networks and cellular networks) in disaster areas, people cannot access their bank accounts to make electronic financial transactions. Therefore, an infrastructureless payment system which functions well without the support of communication infrastructures is vital for people in disaster areas.

To enable carrying out offline financial transactions in disaster areas that lack communication infrastructures, we need an infrastructureless mobile ad-hoc network to be able to design a mobile payment system. Although the proposed system can also work online (e.g. as a digital currency), requesting electronic money from a bank for immediate use is not possible when there is no direct connection to the bank. There are many payment systems providing digital currency services, but none of them have been developed to address the needs of people in a disaster situation where there is no communication infrastructure. This paper therefore focuses on offline transaction over a mobile ad-hoc network. In designing such a system, however, we face the following challenges [1].

· **Unreliability of wireless link between nodes :** A mobile ad-hoc network is characterized by its limited energy, which makes it difficult to maintain a consistent wireless link for communication.
· **Constantly changing topology :** Topology changes very rapidly in a mobile ad-hoc network due to movement of nodes into and out of the network. This also results in a decrease in performance, due to a difficulty in routing data to its destination.
· **Lack of incorporation of security features :** Security features in statically configured wireless networks are not available for ad-hoc environments, which increases exposure and vulnerability to attacks.

In this paper, we propose an endorsement-based mobile payment system to address these issues. Specifically, each customer in the network will select people to endorse their transactions, where the digital signature of an endorser is obtained on every transaction as proof of the endorsement. This will ensure that the merchant gets paid after each successful transaction. Thus, in the case where a customer buys an item and does not pay, the money can be deducted from the endorser's account. Since there is no direct connection with the payment source (bank) and it is therefore not possible to achieve transaction validity and reliability, we introduce monitoring based on location information. This will not only make a transaction valid and reliable, but also prevent reuse of transaction data to carry out attacks in the network. To prevent impersonation and fraud, a digitally signed photograph is introduced to identify users. Our payment system could also prevent cases of collusion and double spending. Furthermore, user privacy protection is secured by ensuring that the user nickname (e.g. a Temporary ID) is used in every transaction. The nickname can be scrambled, and this will give a customer a different nickname per transaction.

The rest of this paper is organized as follows. In Section II, we review related literature on mobile payment systems. In Section III, we present the overview of the proposed mobile payment system, and in Section IV we propose schemes to provide secure transactions. Finally, we give in Section V an evaluation of the proposed system and conclude the whole paper in Section VI.

II. Related Work

In this section, we outline existing mobile payment systems. Although many works have been conducted on payment systems, most of these studies require the help of infrastructures (online services) to enable secure transactions in the payment system, and are therefore not suitable for disaster areas. For example, Hu *et al.* [2] designed an online authentication system (called Anonymous Micropayments Authentication) to allow a customer and a merchant to authenticate each other indirectly, while preventing a merchant from knowing the customer's real identity. Their proposed system also introduces a payment mechanism where a customer sends an order and payment authorization to the merchant to buy an item. The protocol ensures that the computational overhead of the customer's mobile phone is minimized. However, the payment protocol is not optimized for subsequent payments by the customer to the same merchant, and the protocol depends on a trusted third party, which is a performance bottleneck in the system.

Wang *et al.* [3] presented a novel e-cash payment system which reduces the online computational cost of transactions. 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 customers account after the merchant supplies the item. Other research focuses on e-payment systems such as electronic cash [4], electronic checks [5], electronic travelers checks [6]. By using oriented architecture in wireless networks, Kiran *et al.* [7] proposed a robust payment system which adopts a public key infrastructure and a hash chain to secure transactions. Different from online payment systems, Dai *et al.* [8] recently developed an offline payment system, which, however, is only for digital goods. Li *et al.* [9] introduces a similar concept, but uses a different approach. Li's electronic payment protocol 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. This protocol uses the prepaid method of payment. Dahlberg *et al.* [10] review various existing mobile payment systems and propose frameworks for analyzing the mobile payment research. In addition, regarding various grey areas, they recommend solutions on which future mobile payment research should be based.

Nakamoto [11] also 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 the nodes try to do a reverse calculation of a hash function, which takes a larger amount of computation, as proof-of-work to validate the transaction for its block. (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 as the previous hash in the next block to form a block chain, and the network can thereby agree on the order in which the transaction occurred. Bitcoin, however, requires a CPU device with a high power and transactions which are computationally irreversible, so that coins whose private key has been forgotten or destroyed can never be replaced.

Our contribution in this paper is the introduction of a secure payment system that adopts infrastructureless mobile ad-hoc networks (MANETs) to allow users to purchase necessities in disaster areas. Also, we propose a mechanism that ensures that double spending is detected before a transaction is completed and instead of when the e-coin is deposited in the bank or deducted from the customer's account. Our proposed system adopts an approach similar to that of Bitcoin by ensuring that transactions are broadcast to neighboring nodes. The proposed system, however, differs in techniques, since users 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.

III. System Overview

In this section, we first introduce the transaction procedures of our payment system in areas of no disaster, and then we explain our endorsement-based mobile payment system for disaster areas.

A. Participants

The parties (customer, endorser, merchant, and bank) involved in a payment system will be referred to as users.

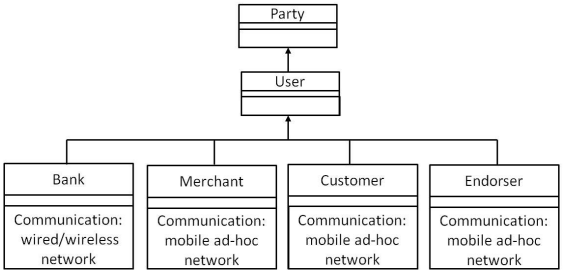

Fig. 1. Users in a payment system.

· **Merchant** - a user that provides goods, services, products or software.
· **Customer** - a user that buys goods, services, products or software from a merchant.
· **Endorser** - a user who pledges to fulfill the customer's obligation should the customer fail to pay for items bought.
· **Monitoring Customer (referred to as a Monitor hereafter)** - a customer that checks every transaction within the radio range to make sure that each is valid and reliable.
· **Bank** - an organization that maintains users' accounts.

B. Payment System in Areas without Disaster

In areas without disasters, there is a direct communication connection to the payment source (e.g., a bank) through communication infrastructures.

The procedure to buy an item in such a payment system is as follows:

· The customer sends a transaction order to buy an item from the merchant, (e.g. a bag of rice worth $50).
· The merchant confirms the customer's identity and forwards the billing information to the bank, (e.g. customer *A* wants to buy a bag of rice worth $50).
· If there is enough money in the customer's account, the bank accepts the transaction and temporarily deducts the amount from the customer and tells the merchant to deliver the item. (If there is not enough money, the bank rejects the transaction, which ends there.).
· The merchant delivers the item to the customer.
· If there is no complaint from the customer, the bank deducts the money permanently from the customer's account, pays the merchant, and then notifies the customer.

Such payment systems fail to function in disaster areas for the following reasons:

· **Unavailability of a network infrastructure**.
· **Non-availability of a bank** — We will assume that a user can access a bank at least every two days.
· **Fraudulent Transactions and Impersonation**.
· **Security/Authentication Issues** — Online authentication is not possible in disaster areas for lack of a network infrastructure.

C. Endorsement-Based Mobile Payment System

In order to enable transactions in disaster areas without network infrastructures and without direct access to a bank, this study aims to achieve mobile transaction in disaster areas by introducing an endorsement-based mobile payment system.

Endorsement: In a payment system, endorsement is a mechanism by which a user (called an endorser hereafter) agrees by signing a form to make payment instead of a customer in the case that the customer fails to pay a merchant. The endorser should have real money deposited in a bank before the disaster occurs.

With the endorsement mechanism, we can achieve a mobile payment system in a disaster area even if the bank is not accessible. For example, let us say that endorser *E* agrees to endorse *A*. The procedure for *A* to buy an item from a merchant using an endorsement-based payment is as follows:

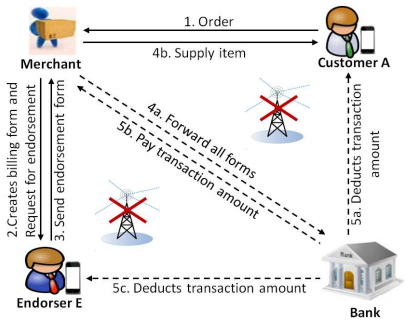

Fig. 2. Transaction process in an endorsement-based payment system without network infrastructure.

· Customer *A* sends a transaction order message to buy an item from the merchant, (e.g. a bag of rice worth $50). The transaction order message includes a transaction order form, customer *A's* temporary identity, the merchant's identity, the endorsers identity, the banks identity, the item number, the item quantity, etc.
· The merchant confirms customer *A's* identity (by a digitally signed photograph, explained later), creates a billing message (which includes billing form, merchant identity, customer temporary identity, endorser identity, bank identity, order number, total transaction value, etc.). However, since there is no direct connection to the bank and there are no means of confirming if Customer *A* has enough money in his/her account, the merchant will request of the endorser, by forwarding the billing and transaction messages to the endorser, that the endorser guarantee the transaction.
· The endorser confirms the merchants identity and customer *A's* identity, creates an endorsement message (which includes an endorsement form, customer A's temporary identity, merchant identity, endorser identity, order number, endorsement amount, etc.), indicating that he/she agrees to guarantee the transaction by signing the endorsement message with his/her signature. The endorser forwards the endorsement message, billing message and transaction order message to the merchant, (stating for example, "I agree to guarantee customer *A's* transaction of $50").
(a) The merchant forwards all messages to the bank.
(b) The merchant then delivers the item to customer *A*. The merchant will get paid since the transaction is endorsed by endorser *E*.
· The bank confirms that the identity of all users and that all the information provided are genuine.
(a) The bank then confirms the account balance of customer *A* and deducts the transaction amount, (e.g. deducts $50).
(b) The bank pays the merchant, (e.g. adds $50 to the merchants account).
(c) However, if customer *A* does not have enough money to pay for the item, the money is deducted from endorser *E*.

With this model, we can achieve a financial transaction in a disaster area even without a direct connection to a bank. However, we still face the problems introduced in Section IV. We will look at the solution for each one in turn.

IV. Schemes Securing an Endorsement-Based Mobile Payment System

In this section, we introduce problems faced by our mobile payment system and the techniques adopted to solve them and thus enable secure transactions in endorsement-based mobile payment systems.

A. Providing Authentication and Security

Problem (Authentication and Security) : When a customer initiates a transaction in a normal payment system, each customer's authentication is checked online through the bank, and access to the payment system is granted only if the authentication is valid. A customer can only be impersonated if a dishonest user is able to get the customer's credentials. In a disaster area, authenticating a customer is impossible since, due to the lack of a network infrastructure, a connection to the bank is not available.

Solution (Digitally Signed Picture) : We propose the following offline mechanism for authenticating each user.

TABLE I. 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}	$S_{K_C^{-1}}$

First, customer and merchant register with the bank and exchange IDs before a disaster occurs. The registration is done off-line beforehand. Second, the bank serves as the certificate authority and issues digital certificates to all users. Users' private keys, as shown in Table I, are used to authenticate users in the system.

In addition, the customer selects a photograph that will be digitally signed by the bank. This serves as an additional authentication means during a transaction; this 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 banks and the customer's digital signatures on the photograph.) The system can also use some other method of biometric authentication.

In order to ensure the 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 and thereby identify a dishonest user in the network

B. Preventing Customer and Endorser Colluding

Problem (Customer and Endorser Colluding) : In our mobile payment system (in Section III-C), endorsers guarantee to pay a merchant on behalf of their customer. However, it is possible for endorsers and a customer to collude to defraud the payment system. For example, dishonest endorsers may endorse a dishonest customer, both without money in their accounts. There is no way to confirm their account balances during a transaction in a disaster area. Furthermore, due to some delay in receiving messages, it is possible for the customer or the endorsers to withdraw money from their accounts before the bank moves to deduct money for the purchase. Hence, a mechanism is needed to confirm the customer account balance during the transaction.

Remark 1: *There are only three parties that might collude: Customer, Endorser and Merchant. And the maximum number in collusion considered here is two (e.g. customer and endorsers), though there are other conceivable combinations of colluding: customer and monitor, endorsers and monitor etc.).*

Other Combinations of Colluding : The following combinations in colluding are also possible in the system.

· **Two Customers Colluding (A customer and another customer):** one customer pretends to endorse another.
· **Two Endorsers Colluding :** This is possible only if one of the endorsers pretends to be a customer (i.e., is able to forge customer information and collude with another endorser to endorse the transaction).
· **Two Monitors Colluding:** Similar to the case of endorsers, two monitors can collude only if one of the monitors acts as a customer while the other endorses the transaction.
· **Two Merchants Colluding:** Two merchants may want to collude to defraud customer or endorsers; however, this is not possible without knowing both the customers and the endorsers information (i.e., the customers and the endorsers private keys, real IDs, etc.).

Preventing other possible combinations of colluding is described in Section IV-G.

Solution (E-coin Balance Checking): To prevent colluding, we employ the e-coin technique to check the bank balance of endorsers. In order to buy an e-coin, some money has to be deposited. The e-coin not only prevents colluding, it also prevents a customer from carrying out multiple transactions after turning off their phone, when there is no way to confirm their account balance. (We assume that most users will not turn off their phone after they have contacted the bank).

E-coin : The bank creates for an endorser unique e-coins, similar to tokens, as in [12], [13]: 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. As shown in Figure 3, the e-coin contains the endorser's identity, e-coin identifier (signed with the bank digital signature), e-coin value, GPS coordinates (with GPS coordinates of the bank as default values) and two blank fields (for function extension). An example of an e - coin is given in Figure 4.

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.)

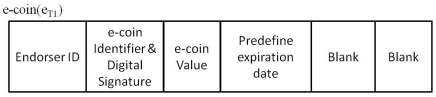

Fig. 3. Format of an e-coin created by the bank.

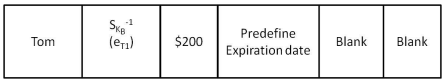

Fig. 4. An example of an e-coin used on a transaction.

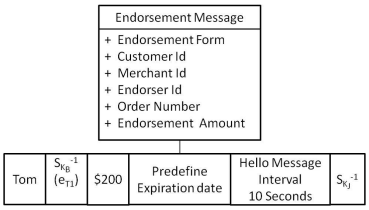

Fig. 5. An example of an endorsement message.

If the endorsed customer does not default in payment, the bank can reissue the e-coin. Otherwise, the corresponding amount of deposited money will be paid. Therefore, colluding by the customer and the endorser can be prevented by checking whether there is an e-coin attached to the endorsement message.

In a situation where an e-coin is lost or corrupted while being transmitted to an endorser, the endorser will have less e-coin than the money in their account. To avoid this, the bank sets a pre-determined expiration date on the e-coin. The e-coin will be invalidated after the predetermined date, if the bank has not received a report from the endorser that the e-coin was received. The bank can then issue a new e-coin to replace the one that was lost or corrupted. When an e-coin is not used and the expiration date passes, the e-coin becomes invalid and cannot be accepted by a merchant. A monitor can confirm whether or not the e-coin has expired by checking the expiration date on the e-coin before the transaction begins. To replace an expired e-coin, the bank issues a new e-coin for the user.

C. Preventing Double Spending

Problem (Preventing Double Spending of an E-coin) : An endorser could possibly try to spend the same e-coin twice for two different transactions, (double spending is using e-currency more than once to pay the same or different people).

Solution (Event Chains) : To prevent double spending in the system and also ensure that the e-coin is secure, the proposed method allows the merchant to check the log for all events in the past associated with the endorser. To do this, an endorser requests other monitoring nodes to sign (with their digital signature) their transaction logs each time a new event occurs. This will, however, require a lot of communication overhead, since the monitoring node will need to go through the customer's entire transaction log before signing.

Therefore, we propose an event chain as a solution to double spending. An event chain is a successive application of a cryptographic hash function on a piece of an event log (called a block). Instead of sending and signing on the entire log, the

endorser calculates the hash value in the last block, which is effectively the hash value of the entire log, and sends it to the monitor. The monitor signs on the combination of hash value, GPS coordinates, timestamp, and a new event (e.g. spending an e-coin); the monitor then sends the block back to the endorser. In this way, all past events of the endorser are recorded to form an event chain, which can be verified by any user. An endorser exchanges a hello message with neighboring monitor nodes periodically to add a new event to the event chain. If a predetermined length of time passes since the last event before a new event is added to the event chain, the event chain is invalidated and can no longer be used. In order to ensure that the e-coin has not been double-spent, the user receives and checks the event log which is the entire event chain, from the point at which the e-coin was received by the endorser.

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 as shown in Figure 6. The preceding block and the entire log of the present transaction event are signed and sent to the monitor. To verify other information in a block, a user requests the entire log.

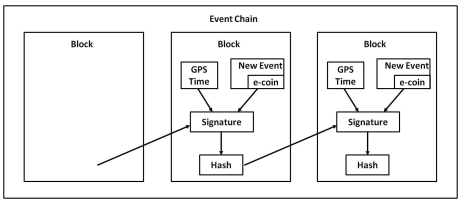

Fig. 6. Event Chain.

When an endorser receives a new e-coin from the bank, the e-coin is received either directly from the bank or relayed to the endorser through the users available within the radio range, as shown in Figure 7. We assume that the bank can be trusted. In the case that an e-coin is delivered through the MANET, the last two users to relay the e-coin to the endorser will compute the hash value of the e-coin identifier and the timestamp combined, and then add this value to the e-coin before signing it with his/her digital signature.

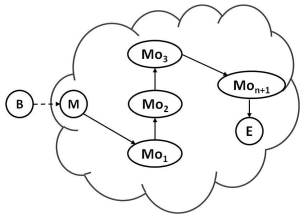

Fig. 7. Receiving a new E-coin.

Remark 2: *The reason we use e-coins only for endorsement is to allow customers to make new transactions immediately after turning off the phone: turning off the phone invalidates the event chain. Our system allows the user to make a new transaction after turning on the phone before he/she communicates with the bank, since the transaction is guaranteed by his/her endorsers. The endorser cannot endorse a transaction immediately after turning the phone off and on. But since we assume that there are many endorsers available, the transaction can be guaranteed by other endorsers.*

D. Preventing Collusion among stolen Phones

Problem (Confirming Transaction Location Source) : It may happen that an attacker steals the phone of a customer or endorser and tries to do a transaction with the phone in another location. If many phones are stolen by an attacker, collusion among those phones is possible. Also, customers or endorsers may do a transaction in a location other than their usual locations and then deny having made such a transaction. Thus, to ensure transaction integrity, the transaction location needs to be confirmed.

Solution (Location Information Based Monitoring) : We propose a location information-based monitoring scheme to achieve confirmation of transaction location. According to this scheme, each endorser will constantly exchange HELLO messages with monitor 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. Other users of the system can monitor the endorser's transaction location by checking an endorser's entire 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. Also, the interval between the HELLO messages is added to one of the blank fields of the e-coin, as shown in Figure 8. The HELLO message intervals in the e-coin can also be compared with the interval in the HELLO message. 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 there is connectivity loss.

Phones that share similar location histories cannot be used in a transaction.

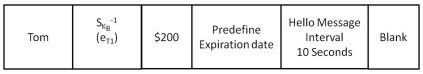

Fig. 8. Example of location information based monitoring.

E. Preventing Reset and Recovery Attack

Problem (Reset and Recovery Attack) : In a reset and recovery attack, a user backs up all transaction data (a transaction order message or an endorsement message) already used to buy an item and then 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 [1]. Consider a scenario where a dishonest customer buys an item from merchants M_1 and M_2, then resets the phone to the default settings. Then the customer recovers the backup data and uses the same data to buy an item from some merchant other than merchants M_1 and M_2. We can say that the user has successfully carried out a reset and recovery 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. Therefore, we need to prevent **already endorsed transactions to be used twice** by a user (customer or endorser) while maintaining his/her anonymity.

[1]This is also a form of replay attack, where an adversary intercepts the data and retransmits it later.

Solution (Blind Signature and Event Chain): To prevent a user (customer or endorser) from carrying out many transactions with the same transaction order message (already endorsed) for reset and recovery attacks, we propose the schemes described below that employ techniques of an event chain (to prevent users from reusing the same message) and techniques of the blind signature (to ensure anonymity).

Blind signature : The blind signature technique allows a person to get a message signed by another party without revealing any information about the message to that party. In traditional transactions, people have used blind signatures by enclosing a message in a special envelope lined with carbon paper. The outside of the envelope is signed and the carbon allows the signature to show on the message without exposing the content in the envelope. In [14], a method is proposed to do this using cryptography. We use this method in our system.

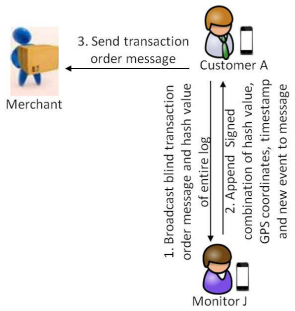

Fig. 9. Preventing reset and recovery attack from a customer.

Preventing attack from a customer : The scheme is illustrated in Figure 9.
· Customer *A* creates a transaction order message and blinds the transaction message using a blind signature, then computes the hash value of the last event chain block, and appends it to the message. Customer *A* then broadcasts the message.
· Monitor *J* accepts the message and signs a combination of hash values, GPS coordinates, the timestamp and a new event, and appends these to the message. Monitor *J* then sends them to customer *A*.
· Customer *A* unblinds the transaction order message, and forwards the signed transaction order message to the merchant.
· The merchant checks the validity of the event chain. If the event chain is valid, the merchant proceeds by forwarding the messages (transaction message and billing message) to the endorsers. If the event chain is invalid, the transaction order message is seen to be forged or already used in the previous transaction, and the merchant will reject the transaction.

Thus, if a user (e.g., customer or endorser) attempts to use the same transaction order message or endorsement message with another merchant, after resetting his/her phone, the user will have to change the event chain of all previous transactions to modify the hash values, GPS coordinates and the timestamp in the previous transaction. The user cannot modify the previous transaction message without changing the hash values. (Monitor *J* also signed the message with his/her digital signature.). By checking the entire event chain to see if the predefined time had passed before a new event was added, the merchant will detect that the message has already been used.

Preventing attack from an endorser: We adopt the scheme illustrated in Figure 9 and the transaction process described above to prevent reset attack from an endorser.

The monitor checks if the e-coin has been double spent before signing a combination of hash values, GPS coordinates, the timestamp and a new event. Also, the monitor checks for the validity of the event chain of the HELLO message.

F. Transaction based on Chains of Endorsement

Problem (Availability of Endorsers) : Given a situation where an endorser is not available, 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 has as many endorsers as possible. When an endorser is not available to endorse a transaction, others will be able to. The more endorsers a transaction has, the more secure it is. When a customer buys an item but defaults afterwards, instead of one endorser bearing the liability, which may reduce the money for endorsing another customer, the liability for that item is shared among all the endorsers by introducing many endorsers. 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.

If 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 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 avoid 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. According to this method, endorsers have their own endorsers that can inherit transactions to be endorsed.

During registration, after the customer has selected endorsers, the bank creates an endorsement-chains tree, in which all the direct endorsers of a customer form the first level of the endorsement chain. The tree is updated as endorsers select their own endorsers. Each customer will have levels of endorsers, as shown in Figure 10, depending on the number of endorsers they have as their primary endorsers.

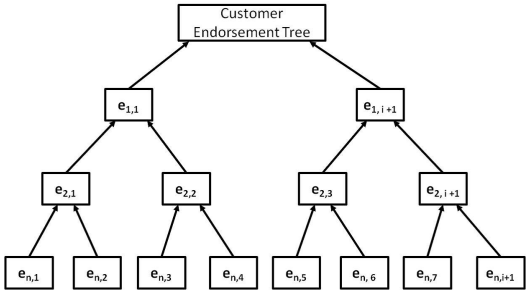

Fig. 10. Customer endorsement tree.

Consider a scenario, in which a customer sends a transaction order to a merchant to buy an item for $4,000. The merchant will create a billing message and forward it to the endorsers. The endorsers create an endorsement message and attach e-coins equivalent to the registered endorsement amount. However, due to disruption of the network, one of the endorsers is not available, as shown in Figure 11.

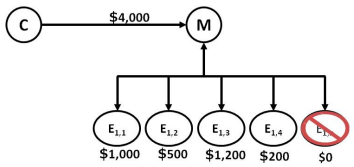

Fig. 11. Chains of Endorsement during Transaction

The merchant, after receiving the endorsement message from endorsers, checks whether the value of the e-coins is less than the transaction amount. If the value of the e-coins exceeds the transaction amount, the merchant proceeds to forward all the information to the bank. However, if the e-coins value is less than the transaction amount, the merchant obtains the information of level-two endorsers from the endorsement tree header. The endorsement tree header is the one who provides information on how the merchant can access the secondary endorsers. The endorsement tree header is included in the customer transaction message and contains the information of the customers secondary endorsers up to level 5.

Then the merchant can search for level-two endorsers of the customer (who are the endorsers of the unavailable level 1 endorsers). The merchant forwards the billing information to the level-two endorsers, as shown in Figure 12. The process is repeated until the e-coin value equals or exceeds the transaction amount. If no secondary endorser is available in these cases, the merchant can reject the transaction.

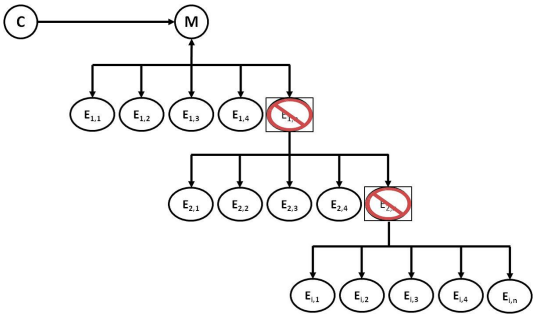

Fig. 12. Chains of endorsement during transaction.

Problem (Forged Endorsement Tree Header) : The endorsement tree header can be forged by an attacker or a dishonest user to deceive secondary endorsers into endorsing transactions that do not originate directly from the legitimate customer (in this example, the customer of the first level endorser).

Solution (Preventing Forged Endorsement Tree Header) : As a proof that the endorsement tree header is not forged, each endorser, each time they endorse a customer, updates their information on the endorsement tree header by calculating the hash value of the customer ID of the last customer they endorsed.

Before endorsing a customer, each secondary endorser, by calculating the hash value of the customer ID, confirms if this hash value in the endorsement header matches the one received from the merchant.

If the hash value is the same, the secondary endorser can then endorse the customer; otherwise the endorsement request from the merchant is rejected.

G. Preventing Other Combinations of Colluding

Other combinations of colluding are also prevented in the system.

Colluding with the Monitor : Customer, endorsers or Merchant may want to collude with the monitor, but this is difficult without knowing the monitor before the transaction is carried out. Colluding with the monitor is possible only given a small number of users in the system. To prevent customer, endorsers or merchant from colluding with the monitor, the proposed protocol will ensure that customer, endorsers and merchant will be unable to predict the monitor that will check their transaction for validity before signing the transaction.

Colluding with the Merchant : Endorsers cannot collude with the merchant without a customer. And it is impossible for an endorser or for other users to forge the digital signature of a customer, which is used on every transaction.

H. Assumptions

We make the following assumptions about the mobile payment system.

Assumption 1 : Most of the users in the system are trustworthy users who do not change location often; this will make it easy to prevent fraudulent transactions. Most of the users do not power off the phone very often.

Assumption 2 : All users are in the disaster area except the bank. Users in a disaster area communicate using a mobile ad-hoc network while the bank uses a wireless or wired network to communicate. Also, it takes at least two days for a message to get to the bank.

Assumption 3 : No more than two parties will collude to commit fraud in the system.

Assumption 4 : A sufficient number of monitoring nodes is available most of the time.

The overall procedures of our proposed endorsement-based mobile payment system are summarized as follows.

· 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.
· 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* unblinds the transaction order message and forwards the signed transaction order message to the merchant.
· Merchant *M* checks the validity of the event chain. If the event chain is valid, the merchant proceeds to forward the transaction message and the billing message to the endorsers. 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.
· Endorser *E* creates an endorsement message and blinds it using a blind signature scheme; then computes the hash value of the last event chain block and appends to the message the hash value and an e-coin equivalent to endorsement amount; then broadcasts the message.
· Monitor *D* accepts the message and checks if the e-coin is not double spent; checks for the validity of the event chain (and the event chain of the HELLO message); then signs a

combination of hash values, GPS coordinates, the timestamp and a new event, and appends it to the message; then sends it to Endorser *E*.
· Endorser *E* unblinds the endorsement message and forwards the signed endorsement message with an e-coin to the merchant.
· Merchant *M* receives the endorsement message from endorser *E*; checks the validity of the event chain and checks whether the e-coin is 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.
· Merchant *M* sends a transaction confirmation to customer *A* and to endorser *E* and supplies the item to customer *A*.
· Bank *B* authenticates the identities of merchant *M*, endorser *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 pays merchant *M*. Bank *B* sends an acknowledgment message to merchant *M*, endorser *E* and customer *A*. If customer *A* does not have sufficient money, bank *B* deducts the transaction amount from endorser *E*.

V. Evaluation

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

· **Feasibility:** Our proposed mobile payment system overcomes such limitations of mobile transaction in a disaster area as unavailability of a network, need of account balance verification, danger of reset and recovery attacks, etc.

· **Authentication:** In our system, the bank serves as a 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 the digital certificates and the digitally-signed photograph to authenticate a customer.

· **Anonymity:** When broadcasting transaction messages, users do not reveal the content of a message because the blind signature scheme is used. Furthermore, a customer can use a nickname instead of a real name in each transaction. Since customer and merchant physically meet and agree to do a transaction, it is always possible to take a photograph. Using a digitally signed photograph, therefore, does not compromise anonymity. In addition, our proposed system can use biometric methods of authentication .

· **Confidentiality:** All messages in the network are encrypted and digitally signed by users. If customer *A* sends a message to merchant *M*, the message will be encrypted with merchant *M's* public key and digitally signed with customer *A's* private key. Any other user in the system will not be able to decrypt a message unless they have merchant *M's* private key.

· **Integrity:** To ensure that messages are not modified while in transit or cannot be repudiated later, a blind digital signature scheme and an event chain scheme are used. Forms such as a transaction order form, a billing form and an endorsement form are also digitally signed.

· **Reliability:** To ensure consistency in transaction information and to avoid user impersonation in a situation where phones may be stolen, location information-based monitoring is used. Each user's GPS coordinates are attached to the transaction message to prove that the users are in their claimed location.

VI. Conclusion

In this paper, we proposed a new mobile payment system which adopts infrastructureless mobile ad-hoc networks (MANETs) to allow users to purchase necessities in a disaster area. Based on the endorsement mechanism, endorsers provide payment guarantees for each transaction between customers and merchants, thereby enabling mobile transactions in disaster areas even without immediate access to a bank. Moreover, by employing techniques of blind signature, event chain and location information-based monitoring, the proposed mobile payment system promises also to provide secure transactions, preventing, for example, fraud, collusion, reset and recovery attacks, impersonation of users and double spending.

There is at present no reason to suppose that our proposed method is not scalable, and, as a future work, its scalability will be evaluated using simulation.

References

[1] A. Mishra and K. M. Nadkarni, *Security in Wireless Ad Hoc Networks*. CRC Press LLC, 2003.

[2] Z. Hu, Y. Liu, X. Hu, and J. Li, "Anonymous micropayments authentication (ama) in mobile data network," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 1, March 2004, p. 53.

[3] J. Wang, F. Yang, and I. Paik, "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.

[4] Y. Y. Chen, J. K. Jan, and C. L. Chen, "A novel proxy deposit protocol for e-cash systems," *Applied Mathematics and Computation*, vol. 163, no. 2, pp. 869–877, 2005.

[5] C. C. Chang, S. C. Chang, and J. S. Lee, "An on-line electronic check system with mutual authentication," *Computers and Electrical Engineering*, vol. 35, no. 5, pp. 757–763, 2009.

[6] H. T. Liaw, J. F. Lin, and W. C. Wu, "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.

[7] N. C. Kiran and G. N. Kumar, "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] X. Dai, O. Ayoade, and J. Grundy, "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] W. Li, Q. Wen, Q. Su, and Z. Jin, "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.

[10] T. Dahlberg, N. Mallat, J. Ondrus, and A. Zmijewska, "Past, present and future of mobile payments research: A literature review," *Electron. Commer. Rec. Appl.*, vol. 7, no. 2, pp. 165–181, Jul. 2008.

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic system," 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[12] 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.

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

[14] D. Chaum, "Blind signatures for untraceable payments," in *Crypto '82 Proceedings of Advances in Cryptology*, 1983, pp. 199–203.