NAIST-IS-MT1351116

Master's Thesis

A Mobile Payment System Utilizing MANETs for A Disaster Area

Babatunde Ojetunde

February 3, 2015

Department of Information Science
Graduate School of Information Science
Nara Institute of Science and Technology

A Master's Thesis
submitted to Graduate School of Information Science,
Nara Institute of Science and Technology
in partial fulfillment of the requirements for the degree of
MASTER of ENGINEERING

Babatunde Ojetunde

Thesis Committee:

Professor Minoru Ito	(Supervisor)
Professor Keiichi Yasumoto	(Co-supervisor)
Associate Professor Naoki Shibata	(Co-supervisor)
Assistant Professor Juntao Gao	(Co-supervisor)

A Mobile Payment System Utilizing MANETs for A Disaster Area*

Babatunde Ojetunde

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 communication infrastructures (like wired networks and cellular networks) to enable transactions, which may be destroyed during disasters (like large-scale earthquake and flooding) and thus cannot be relied on in disaster areas. In this thesis, we propose a mobile payment system, adopting infrastructureless mobile ad-hoc networks (MANETs), which allows users to shop in disaster areas while providing secure transactions. Specifically, we propose an endorsement-based scheme to guarantee each transaction and a location-information based scheme to provide transaction monitoring, and thus achieve transaction validity and reliability. Our mobile payment system can also prevent collusion between two participating parties, reset and recover attacks from any user and double spending by using location-based mutual monitoring by nearby users.

Keywords:

Mobile Ad-Hoc Network, Endorsement, Event Chain, Double Spending

*Master's Thesis, Department of Information Science, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-MT1351116, February 3, 2015.

Contents

List of Figures

List of Tables

1. 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, people in disaster areas can neither access payment systems to make online electronic financial transactions due to the lack of communication infrastructures (like wired networks and cellular networks). Therefore, an infrastructureless payment system which functions well without the support of communication infrastructures is vital for people in disaster areas to do transactions. In this thesis, we will propose a mobile payment system, utilizing infrastructureless mobile ad-hoc network, to enable carrying out offline financial transactions in disaster areas [1].

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. Designing a mobile payment system in disaster areas based on MANETs faces the following challenges [1].

- **Unreliability of wireless link between nodes :** Mobile devices in a mobile ad-hoc network usually have limited energy (battery power), 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 users into and out of the network. This also results in a decrease in network performance (increasing delay and decreasing throughput), 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 environments of MANETs, which increases exposure and vulnerability to attacks.

In this thesis, we propose an endorsement-based mobile payment system to address these issues. Specifically, each customer in our system will select people

[1] Although our mobile payment 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 online communication connection to the bank

to endorse their transactions, where the digital signature of an endorser is obtained on every transaction as proof of the endorsement. In this case, when a customer buys an item and does not pay, the money can be deducted from the endorser's account, thus ensuring that each merchant gets paid after each successful transaction. Since there is no direct connection with the payment source (bank) and it is therefore not possible to achieve transaction validity and reliability. To address this issue, we introduce location-information based scheme to provide transaction monitoring from nearby users. 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, 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.

In the following, we first review related literature on mobile payment systems, then present the overview of the proposed mobile payment system, and finally propose various mechanism to provide secure transactions.

2. Related Works

2.1 Electronic Payment

Electronic commerce (referred to as e-commerce hereafter) is the online buying and selling of goods, services, products or software, while electronic payment is the online payment method for the e-commerce, which involves the exchange of money electronically between a buyer and a seller through a bank. In an e-commerce payment system, trust is an essential part of e-commerce transaction unlike traditional means of transaction. For example, in traditional transactions a buyer will see goods before making payment, but in e-commerce the buyer does not necessarily see or examine the physical goods before making payment. Figure 1 shows a comparison between the design of traditional payment and electronic payment.

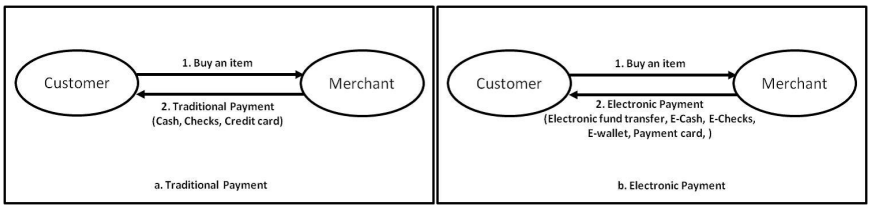

Figure 1. Traditional Payment versus Electronic Payment

There are various electronic payment systems available to online customers for payment, some of which are listed below:

- **Electronic funds transfer (EFT) :** This payment system involves an electronic transfer of money from a customer's bank account to the bank account of another customer/merchant. The money transfer may also involve another bank different from the customer's bank and this is referred to as inter-bank transfer.

- **Credit cards :** This is one of the oldest payment methods. It is also categorized as a buy-now and pay-later payment model. A customer is permitted to buy goods/services up to an agree amount that is granted by the bank or the credit card service provider. The payment for the goods is deducted at the end of the month. This process is known as settlement.

- **Payment cards :** This can be categorized as buy-now and pay-now payment model. The payment cards usually contain the stored value (money) that can be used for payment of goods/services. ATM debit cards that are allowed to carry out online transaction fall in this category. Other cards that can be classified as payment cards are smart cards, gift cards, etc.

- **Electronic money (also known as e-cash) :** This is an electronic equivalent of physical cash that is stored digitally and is used for payment of goods/services in an online e-commerce.

- **Electronic wallets (e-wallets) :** This can be referred to as the electronic form of a physical wallet. E-wallet stores user's payment information and other authentication information. It allows a user to make payment to a merchant using near field communication (NFC). E-wallet, however, can be used to store other information such as health card, driver license etc. Examples of an e-wallet are Osaifu-Keitai, Google wallet, etc.

The emerging of new e-commerce transactions has necessitated the development of new electronic payment as a means of paying for goods that are bought using these new e-commerce systems. Mobile electronic commerce is an example of such e-commerce and it involves the use of wireless mobile devices to buy and sell goods/services, which facilitates the development of mobile payment systems.

2.2 Mobile Payment

Mobile payment is referred to as any transaction that is done using a mobile device. This can be buying of goods or services from a merchant or exchange of electronic cash between two parties. Mobile payments are based on different charging models depending on the way protocols are developed. The followings are the common charging models:

1. **Subscription Model :** A customer is charged based on his/her subscription for a particular service. This is also referred to as billing model. Subscription model can either be a monthly payment where a customer makes the payment personally, or a recurring payment which is charged directly

to the customer account. The subscription model can be implemented on a prepaid or post-paid method.

2. **Credit Model :** In credit model, a customer is allowed to buy goods/services first and make payment later. This is also a form of post-paid method.

3. **Debit Model :** In this model, a customer is charged immediately for a transaction. This is used majorly by most of existing payment systems (especially micro-payment system) and it often involves the use of an electronic currency.

4. **Electronic check Model :** This model adopts the same process as that of a paper check. It is also regulated by the same law as a paper check. It allows a customer to make payment on any transaction where a paper check can be used.

Our proposed mobile payment system adopts the use of both credit and debit model with electronic currency.

Mobile payment can be broadly classified into two categories, depending on the transaction value, namely: micro-payment and macro-payment.

2.2.1 Micro-Payment

Micro-payment can be described as an electronic payment system that is used for transactions that involves a small amount of money (for example, an amount that is less than $1). Micro-payments system is usually used for online transaction such as the purchase of ring tone, music, online games, e-book, etc. Some examples of micro-payment systems are Millicent (available in Japan in 1999), PayPal micro-payment, Mpay. The security mechanism in a micro-payment system is more centered on reducing the payment verification cost among stakeholders. Figure 2 shows the basic design of a micro-payment system.

2.2.2 Macro-Payment

Macro-payment can be described as an electronic payment system that is used for transactions that involves a large amount of money (that is, an amount

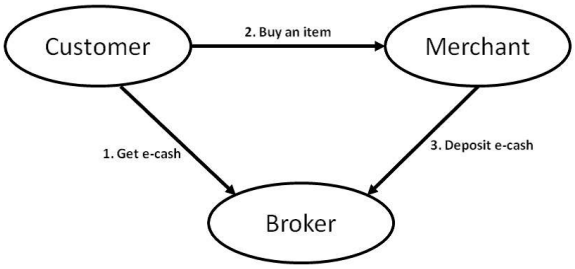

Figure 2. Basic Design of a Micro-Payment System

that is more than $10). The macro-payment system usually involves the payment for paying bills, buying of physical goods, but can also work for digital contents and services. Unlike micro-payment system, the security mechanism in macro-payment is more centered on authorization, privacy of users, and non-repudiation of transactions. The basic design of a micro-payment system is shown in Figure 3.

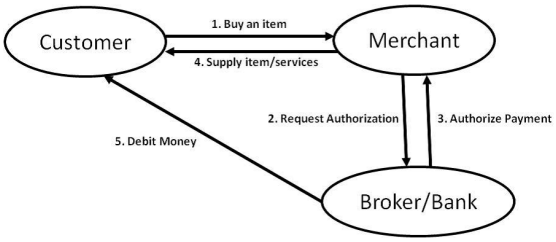

Figure 3. Basic Design of a Macro-Payment System

2.2.3 Differences between Micro-Payment and Macro-Payment

The main differences between micro-payment and macro-payment are stated in Table 1 below:

2.2.4 Security Requirements of Mobile Payment System

The following security requirements should be achieved by a mobile payment system. Our proposed system can achieve these goals after it is run successfully.

- **Authentication :** All users should be able to authenticate each other to avoid impersonation of users.

Table 1. Differences between Micro-Payment and Macro-Payment

Category	**Micro-payment**	**Macro-Payment**
Security	Low transaction security	High transaction security
Computational Cost	Require low overhead	Require high overhead
Communication Cost	Require low overhead	Require high overhead
Transaction Amount	Small (less than $1)	Large (more than $10)

- **Anonymity :** Each user's privacy should be protected. A merchant should not be able to associate transaction to the real identity of a customer.
- **Confidentiality :** All messages in the network should be encrypted and digitally signed by users.
- **Integrity :** To ensure that messages are not modified in transit and cannot be repudiated later, the integrity of transaction message should be protected.
- **Double Spending Detection :** A customer should not be able to use the same money (e-coin) twice or more to buy goods/services.
- **Overspending Detection :** A customer should not be able to spend more than the money in his/her account.
- **Replay Attack Protection :** In a situation that an attacker intercepts a message in the system and tries to use the message later to buy an item, the payment system should detect that the message is already used.

2.3 Previous Research

Although many works have been conducted on payment systems, most of these studies require the support of communication 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 Micro-payments 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. In addition, the payment mechanism allows a customer to make a purchase from either his/her local domain or from a remote domain without any additional overheads on the customer. The payment mechanism is based on three different protocols listed below:

1. **Price Negotiation Protocol :** The protocol is used by a customer to get information about price of goods from a merchant before the transaction begins.

2. **Authentication and Micro-payment Protocol :** The protocol is used to buy goods or services from the merchant. During the transaction, the customer sends his/her transaction order and payment authorization to the merchant. The merchant, however, will first send all transaction information and its identity information to a trusted third party for authentication before providing the goods or services to the customer. The protocol adopts the debit model of payment.

3. **Clearing and Settlement Protocol :** The protocol is used to reconcile all transaction amounts that the merchant claimed and the customer spent with the amount of money deducted by a trusted third party.

The payment system ensures that the computational overhead of a customer's mobile phone is minimized. However, the system is not optimized for subsequent payments by the customer to the same merchant, and the system depends on a trusted third party, which is a performance bottleneck.

Wang *et al.* [3] presented a novel e-cash payment system which reduces online computational cost of transactions. The computational cost reduction is achieved by integrating the trapdoor hash function into the system. Wang's payment system requires only integer multiplication and addition operations for computation, similar to [4], [5] and unlike the online computational cost introduced by Krawczyk *et al.* in [6] which requires multiplication and modulo operations and Shamir's schemes in [7] that uses modulo operation for computation. This makes this payment system suitable for application with mobile devices.

The proposed scheme adopts mobile prepaid model of payment, in which a customer buys goods online using an electronic payment certificate issued by a

bank to request payment from the bank as shown in Figure 4. The bank first freezes the transaction amount temporarily, sends the transaction information to the merchant, then waits till there is a confirmation from the customer that the goods are supplied by the merchant, red and finally deducts the money directly from the customer's account and deposits it to the merchant's account. The mobile prepaid system is divided into three phases: the registration phase, the payment phase, and the deposit phase.

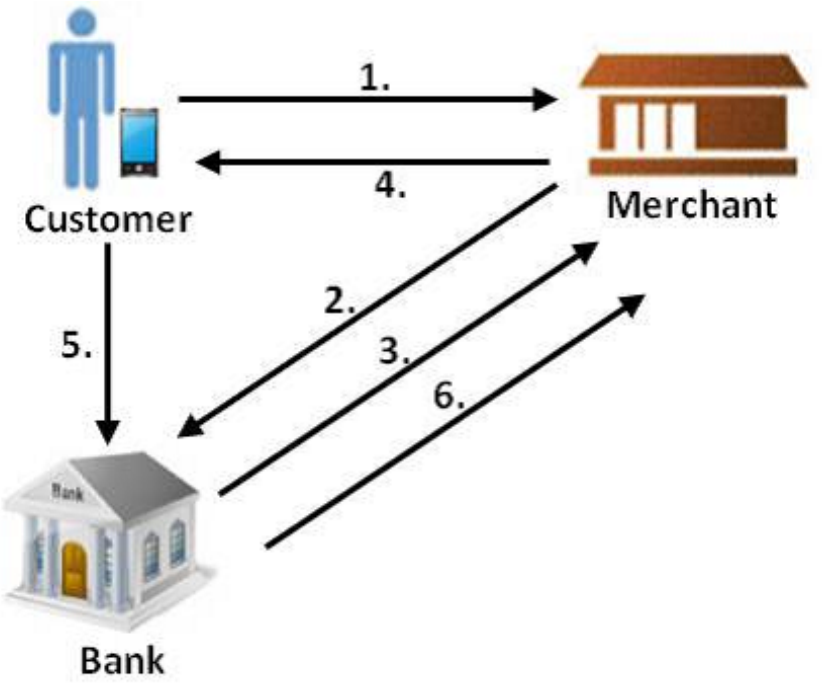

Figure 4. Overview of Wang's Mobile Pre-paid System

The steps for buying an item in Wang's system are summarized below:

1. The customer negotiates price and order item.
2. The merchant verifies the customer and sends billing information to the bank.
3. The bank deducts the transaction amount temporarily and notifies the merchant.

4. The merchant supplies the item to the customer.

5. The customer notifies the bank of receiving the item.

6. The bank deducts the money from the customer's account permanently and pays the merchant.

Chen *et al.* [8] proposed a scheme that focuses on e-payment systems with electronic cash. To reduce merchants' burden of having an account for depositing electronic cash received from customers with multiple banks, Chen's scheme introduced the concept of deposit delegation protocol, which allows a merchant to maintain a single account at its trading bank and delegates all deposits from various banks into the account. The protocol adopts a cryptographic mathematical model that is based on solving discrete logarithm difficult problem or solving factorization difficult problem to secure the system against fraud. The protocol is divided into two schemes, the ElGamal-based deposit delegation scheme shown in Figure 5 and RSA-based deposit delegation scheme shown in Figure 6.

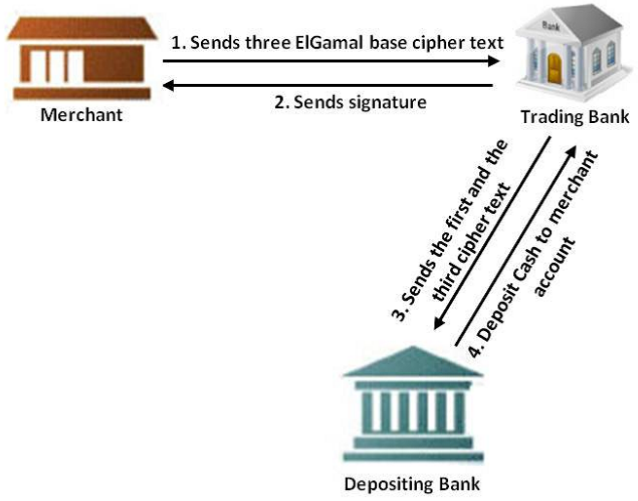

Figure 5. ElGamal Based Deposit Delegation Scheme

The steps in the ElGamal-based deposit delegation scheme are summarized below

1. The merchant blinds the electronic cash and uses his/her merchant ID, trading bank ID, trading bank public key and depositing bank public key

to compute three ElGamal based cipher text (C_{E1}, C_{E2}, C_{E3}). Then the merchant sends the cipher text to his/her trading bank.

2. The trading bank decrypts the second cipher text C_{E2} to obtain the electronic cash. Then the trading bank signs the electronic cash with his/her secret key and forwards the signature to the merchant as proof.

3. The trading bank sends the other two cipher text C_{E1}, and C_{E3} to the depositing bank.

4. The depositing bank decrypts the cipher texts to get the cash, the merchant and the trading, banking information and verifies the electronic cash for double spending. Then the depositing bank transfers the electronic cash in the trading bank for the merchant.

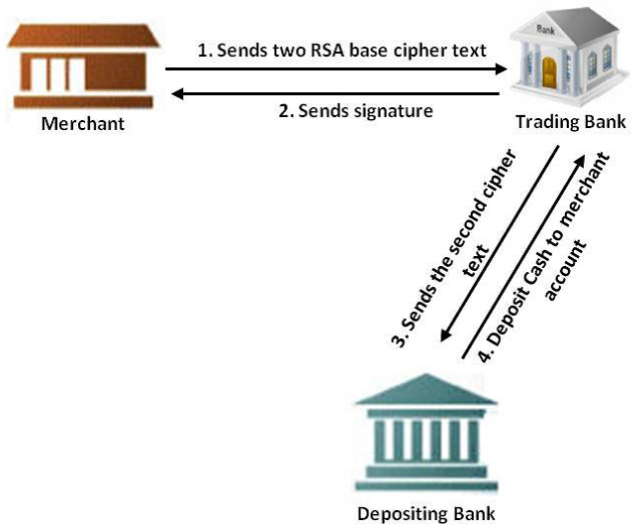

Figure 6. RSA Based Deposit Delegation Scheme

The same transaction process is adopted for RSA based deposit delegation scheme. The major difference between the two schemes is the use of RSA signature and two cipher texts in the RSA based deposit delegation scheme.

Chang *et al.* [9] introduced a novel electronic check scheme to address the inflexibility of the electronic check proposed in [10], [11]. The proposed scheme allows a payer (for example, a customer) to attach the value (i.e., the cost of

goods to be purchased) and the information of a payee (for example, merchant information) to the electronic check during a transaction. The scheme also adopts cryptographic techniques such as one-way hash function, blind signature and RSA cryptosystems to enhance the security of the system. In addition, the electronic check achieved mutual authentication between the payer and the payee, and prevented also various attacks, like replay attack, electronic check book loss, forgery attack and double spending. The proposed scheme is divided into two phases, the registration phase and the paying phase.

Liaw *et al.* [12] introduced an electronic traveler check scheme shown in Figure 7, similar to Chang's electronic check mechanism; however, Liaw's scheme adopts one-way hash function which improves efficiency and reduces cost of the system. A customer and a bank are endorsed by a payee and the endorsement is generated by one one-way hash function. The customer's identity is included in the traveler's check to ensure that only the customer can use a specific electronic traveler's check. It also supports on-line and off-line traveler's check system.

Online transaction in Liaw's scheme is summarized below:

1. The customer registers to use the service.
2. The bank sends a unique identity for the customer.
3. The customer buys electronic check from the bank using his/her identity.
4. The bank registers the electronic check with a clearing house.
5. The bank sends the electronic check to the customer.
6. The customer buys an item from the merchant using the electronic check.
7. The merchant confirms electronic check authenticity with the bank.
8. The bank requests the clearing house to confirm whether the electronic check is not double spent.
9. The bank sends confirmation to the merchant.
10. The merchant deposits the electronic check.
11. The bank confirms if the electronic check is not tampered with.

12. The bank pays the merchant the money equivalent to the electronic check.

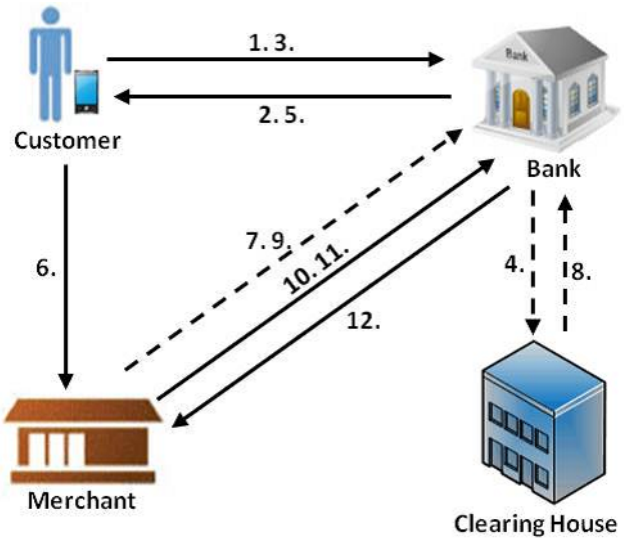

Figure 7. Online Schemes in Liaw's Electronic Traveler Check Scheme

By using oriented architecture in wireless networks, Kiran *et al.* [13] proposed a robust payment system which adopts public key infrastructure and hash chain to secure transactions. The proposed system seeks the cooperation of intermediate nodes to ensure secure and reliable transaction by allocating payment to nodes that permit relaying of packets, thereby providing service. In addition, the proposed payment system uses chains of delegates in which a customer can delegate to other clients (such as a vendor) the authorization to transfer money from the customer's account. The system allows clients to carry out transactions both on-line and off-line. Figure 8 shows the proposed payment system.

Different from online payment systems, Dai *et al.* [14] recently developed an offline payment system, which, however, is only for digital goods. The proposed mobile payment system adopts mechanisms from Dai's previous works in [15], [16], and [17], where they introduced a debit-based payment protocol called NetPay, NetPay-based systems for client-server, vendor and customer networks and e-wallets system to manage e-coins. There are three transaction models in the Mobile-NetPay protocol and these are shown in Figure 9.

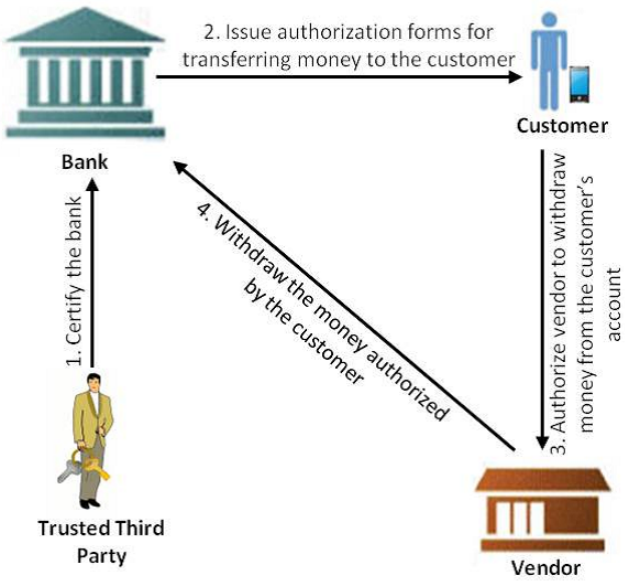

Figure 8. Payment Mechanism in Kiran's Proposed System

The proposed mechanism is designed to handle multiple transactions between vendors and uses the e-coin index to prevent double spending. However, the double spending there is detected only when a vendor tries to redeem all the e-coin received from a mobile user to real money.

Li *et al.* [18] introduced an electronic payment system which allows a vehicle to pay for a transaction in a restricted connectivity scenario, where wireless connection between the merchant and bank during transaction is required. Moreover, the payment system uses the prepaid method of payment. The system adopts self-certified public key agreement to create key sharing between the two parties in the system. The merchant serves as proxy to transmit authentication messages from the vehicle to the bank.

Dahlberg *et al.* [19] reviewed various existing mobile payment systems and proposed frameworks for analyzing mobile payment research as shown in Figure 10. In addition, they recommended solutions to various gray areas in which future mobile payment research should be based on.

Also, their review highlighted the extent of research conducted in each of the factors in the framework as shown in Figure 11. They recommended that researchers should also focus on research that addresses the mobile payment issues

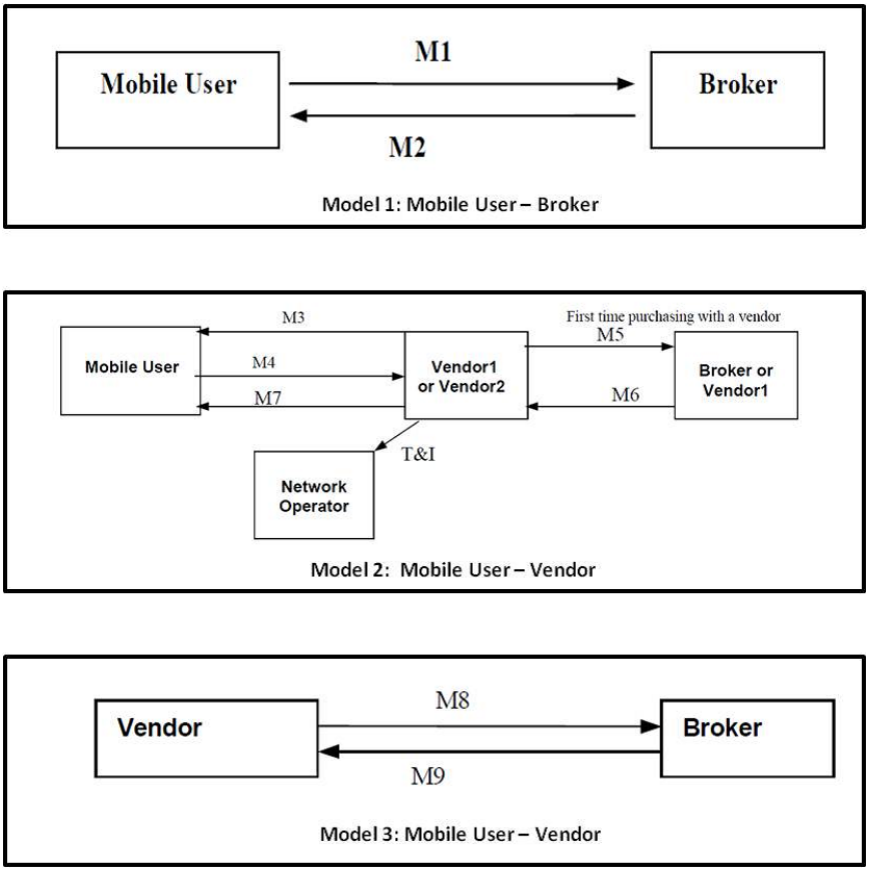

Figure 9. Transaction Model in Dai's Proposed System [14]

in Business-To-Business (B2B) services.

Nakamoto [20] also proposed a decentralized electronic cash system known as Bitcoin that requires no central control. New transactions are broadcasted to all nodes in the system and each node accepts the transaction into a block, then tries to do a reverse calculation of a hash function, which takes a great 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). Figure 12 shows the proof of work in Bitcoin network.

Nodes only accept the block if the transactions are valid and not already spent. The hash of accepted block is used as the previous hash in the next block to form a block chain (so the network can agree on the order transaction occurred). Bitcoin, however, requires high power of device CPU and transactions

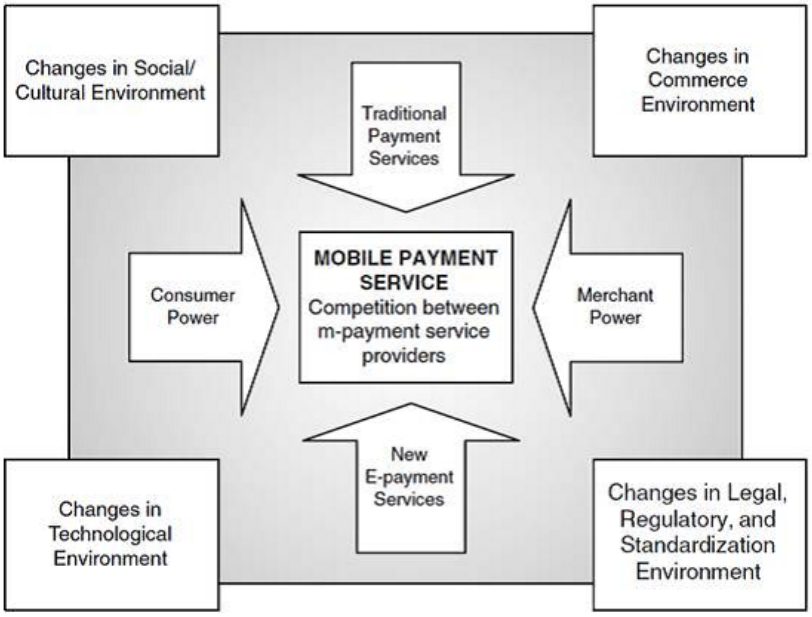

Figure 10. Framework of factors impacting mobile payment (source: [19])

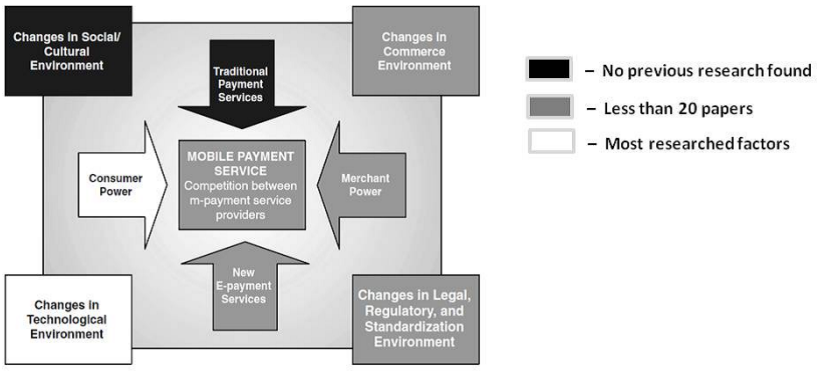

Figure 11. Research in various factors of the framework (source: [19])

are computationally irreversible, hence coins whose private key has been forgotten or destroyed can never be replaced.

The steps of running Bitcoin network are summarized below:

1. A user creates a new transaction and broadcasts the transaction to all nodes.

2. Other users collect the transaction into a block.

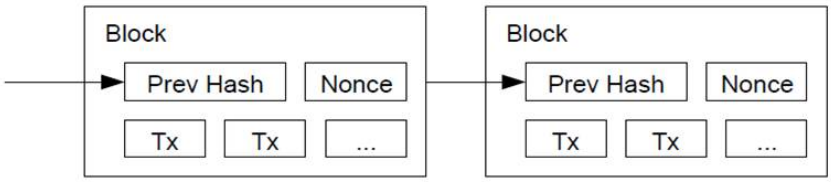

Figure 12. Proof of work in Bitcoin [20]

3. Each user finds reverse calculation of a hash function as proof-of-work for their block.

4. The first user to find the proof-of-work broadcasts the block to all users.

5. Users accept the block if the transactions are valid and not already spent.

6. The hash of the accepted block is used to create the next block in the chain.

Lin *et al.* [21] presented an application-level mobile payment system that can attract a customer's interest to a mobile application with value-added attribute. The proposed system is based on ID-based cryptography and focuses on the reduction of computational cost, memory space of mobile. Lin's scheme uses the network operator as central authority that manages the user and merchant accounts. Double spending and overspending are prevented by adopting the prepaid model (that is, the user account is charged before the user buys the mobile application). The proposed system is based on three-phase transaction process; (1) Withdrawal phase, (2) Payment phase, and (3) Deposit phase. The transaction process is summarized below:

1. To buy a mobile application from a merchant, a user first withdraws an electronic token from the network operator.

2. The electronic token is paid to the merchant in exchange for a mobile application.

3. The merchant confirms the electronic token and if valid, supplies the mobile application.

4. The merchant deposits the electronic token to the network operator in exchange for the monetary value of the token. Both user and merchant maintain an account with the mobile operator.

Tewari *et al.* [22] adopts cryptographic techniques to provide reusable off-line electronic cash. The first scheme, called secret splitting protocol, is used to split the identity of a user to generate identity strings for a customer. The identity string is then used as a transaction item in the system. The second scheme is the encoding protocol, which is a cryptographic technique of binding transaction item to electronic coin that is introduced in the system. Each coin has left and right identity strings. To spend a coin in the system, the left or right of the identity strings of its current owner is randomly blinded and the identity strings of the new owner is encoded and bound to the e-coin. The proposed system depends on a central authority to detect double spending and point of sale device is used for off-line transfer of coins between users in the system.

Chaum [23] introduced the concept of digital blind signature to protect message contents from being viewed by others. According to this technique, a message is first covered (blinded) by xor-ing random bits (a special envelope). The blinded message is then sent to the signer, who will sign the message without knowing the message content. The signed message can be publicly verified against the original message by using regular digital signature. Let us say customer A will like to obtain user J's signature on a message m without user J viewing the message. The following steps will be taken:

1. Customer A blinds the transaction order message by choosing random bits r, raises it to the power of its public key, and multiplies it by the transaction order message ($m^{'} = m \cdot r^{e}$).

2. Customer A sends blinded message $m^{'}$ to user J.

3. After receiving blinded message $m^{'}$, user J will sign the message with his digital signature and sends the message back to customer A

4. Customer A receives a signed message and verifies user J's signature with his public key. Customer A then unblinds transaction order message by

removing r^e from blinded transaction order message $m^{'}$ and finds the user J's signature on the transaction order message.

Huang *et al.* [24] introduced a generic electronic payment system that prevents piracy of electronic contents, thereby protecting intellectual property rights of such electronic contents. The proposed system incorporates digital license, digital receipts and watermark techniques as the solution in the payment model. Merchant verifies the license information before a customer can pay for the item they want to buy.

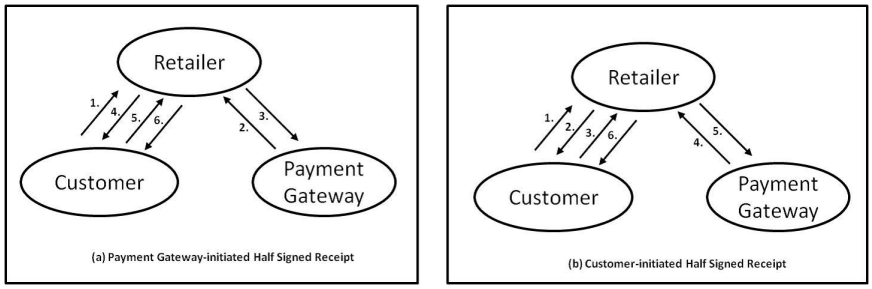

Figure 13. Flows of purchase phase in Huang's scheme [24]

The purchase phase shown in Figure 13 is summarized as follows:
Payment Gateway-initiated

1. The customer sends purchase request to the retailer.
2. The retailer sends his/her seller license to the payment gateway to obtain authorization.
3. The payment gateway authorizes the transaction by sending half signed receipt of the transaction to the retailer.
4. The retailer sends the half signed the receipt and the encrypted key envelope to the customer to obtain the full signed receipt of the transaction.
5. The customer sends the full signed receipt to the retailer.
6. The retailer supplies the encrypted item purchased by the customer.

Customer-initiated

1. The customer sends purchase request to the retailer.

2. The retailer sends his/her seller license and the encrypted item to the customer.

3. The customer sends the half signed receipt to the retailer.

4. The retailer sends the half signed receipt to the payment gateway to obtain authorization.

5. The payment gateway authorizes the transaction by sending full signed receipt of the transaction to the retailer.

6. The retailer sends the full signed receipt and encrypted key envelope to the customer.

Jakobsson *et al.* in [25] introduced a mechanism in which electronic money value and anonymity can be retracted to allow investigation of illegal use (like robberies, money laundering) of such electronic money. Jakobsson's mechanism adopts polynomial-time randomized computation. In addition, a trusted third party is depended on to achieve fairness in the system. The proposed mechanism is divided into five schemes which are public-key probabilistic encryption scheme, the symmetric encryption scheme, the ombudsman signature scheme, bank signature scheme and the coin signature scheme. The five schemes, however, are independent of each other.

Boyd *et al.* [26] proposed a new fair exchange protocol, similar to the one introduced in [27], [28]. In such a system signature sent to another user can only be confirmed by the user, but that user is not allowed to send proof of verification to other parties in the network, except it is made available by the offline third party for others to verify when the need arises. Boyd's protocol, however, introduces a non-interactive verifiable encryption mechanism to improve the limitation (like computational and storage overhead) in the protocols stated above. The schemes also adapt the concept of convertible signature algorithm introduced by Chaum in [29] to a fair exchange protocol, thereby creating two options for the framework in their protocol, namely convertible signature schemes with verifiable encryption and designated converter signatures. The proposed

mechanism ensures that neither the merchant nor the customer is able to take advantage of each other during transaction (for example, the merchant refusing to supply the item to the customer after payment has been made). In addition, the protocol is based on RSA signature, which makes it more efficient than other protocols that also use verifiable encryption.

Sarkar [30] introduced electronic cash that supports multiple usages though it is based on RSA digital signature. By adopting two step encryption schemes in which user information is encrypted into the e-coin, user anonymity is perverse and double spending is prevented. However, like most of payment protocols developed, double spending in Sarkar's protocol can only be detected when the e-coin is deposited in the bank. The protocol uses two unique numbers for the encryption of user information; the first unique number is used during the withdrawal phase and the second for the spending phase of the protocol.

2.4 Differences between our Proposed Method and Previous Research

Most of existing payment systems require communication infrastructures therefore cannot be used to provide the needed services for people in a disaster area. Our proposed mobile payment system, however, adopts infrastructures 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 instead of when the e-coin is deposited in a bank or deducted from a customer's account. Unlike most existing payment systems, our proposed mechanism does not depend on a central authority or mint to detect double spending.

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.

3. Problem Definition

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.

3.1 Participants

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

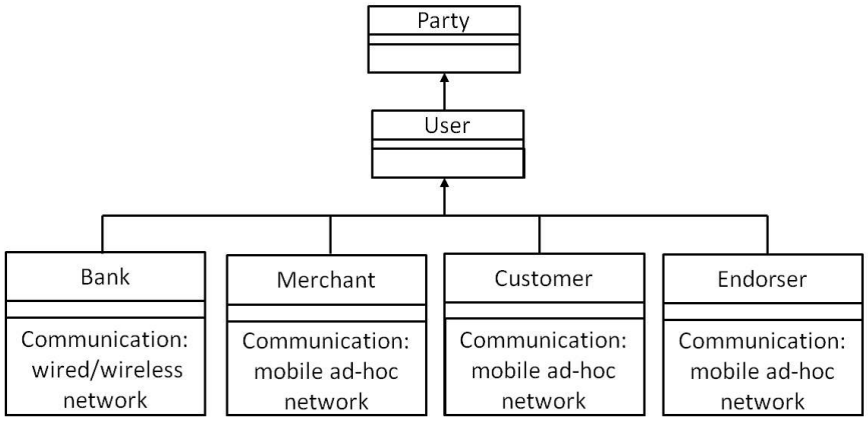

Figure 14. Users in a payment system

- **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.

3.2 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:

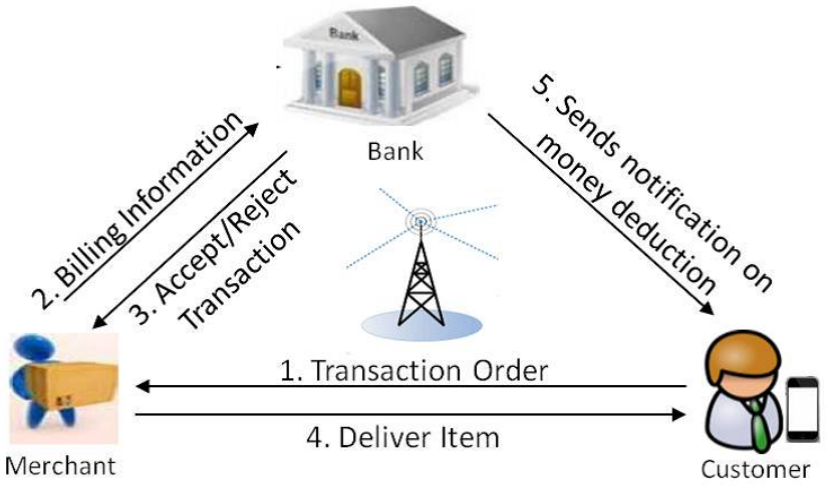

Figure 15. Transactions in areas of no disaster through network infrastructure

1. The customer sends a transaction order to buy an item from the merchant, (e.g. a bag of rice worth \$50).
2. 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).
3. 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.).
4. The merchant delivers the item to the customer.
5. 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.

3.3 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 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:

1. 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 endorser's identity, the bank's identity, the item number, the item quantity, etc.
2. The merchant confirms customer *A's* identity (by a digitally signed photograph, explained later), creates a billing message (which includes billing

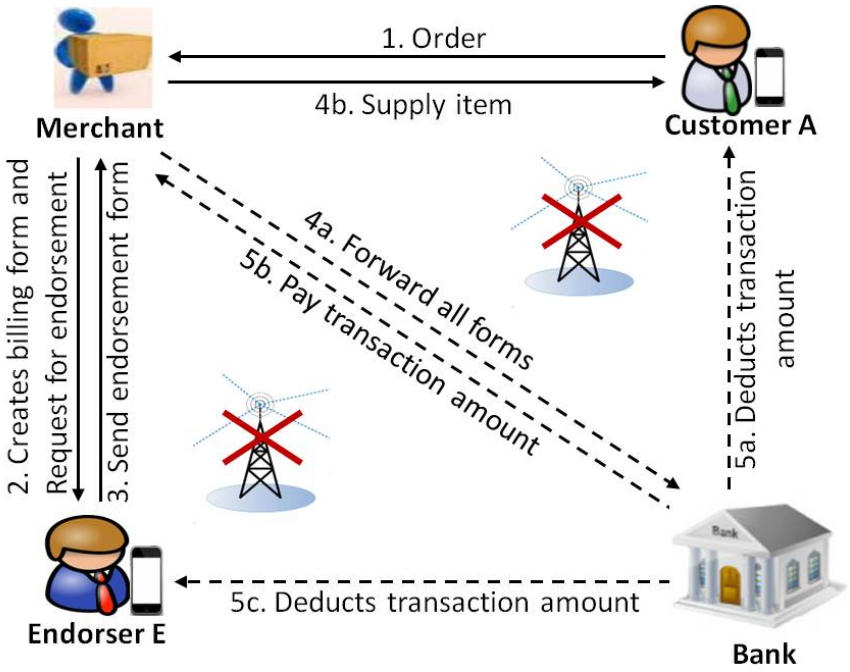

Figure 16. Transaction process in an endorsement-based payment system without network infrastructure

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.

3. The endorser confirms the merchant's 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.

4. 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) b) The bank pays the merchant, (e.g. adds \$50 to the merchant's 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 4. We will look at the solution for each one in turn.

4. Proposed Mobile Payment System

4.1 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.

4.1.1 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 2. 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 2, 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 bank's 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

4.1.2 Preventing Customer and Endorser Colluding

Problem (Customer and Endorser Colluding) : In our mobile payment system (in Section 3.3), 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.

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 customer's and the endorsers' information (i.e., the customer's and the endorser's private keys, real IDs, etc.).

Preventing other possible combinations of colluding is described in Section 4.1.7.

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 [21], [22]: 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 17, 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 18.

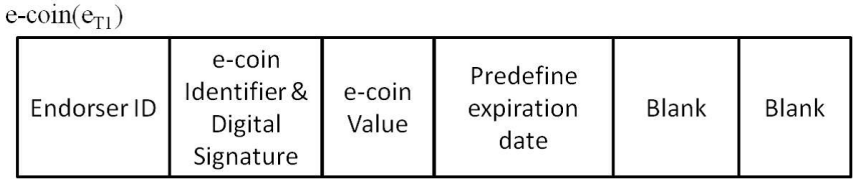

Figure 17. Format of an e-coin created by the bank

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

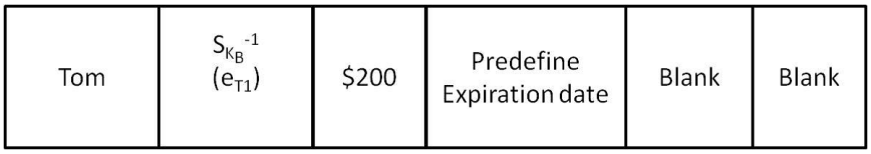

Figure 18. An example of an e-coin used on a transaction

is part of the endorsement message and every endorsement message is signed by the endorser.). An example of an endorsement message is shown in Figure 19.

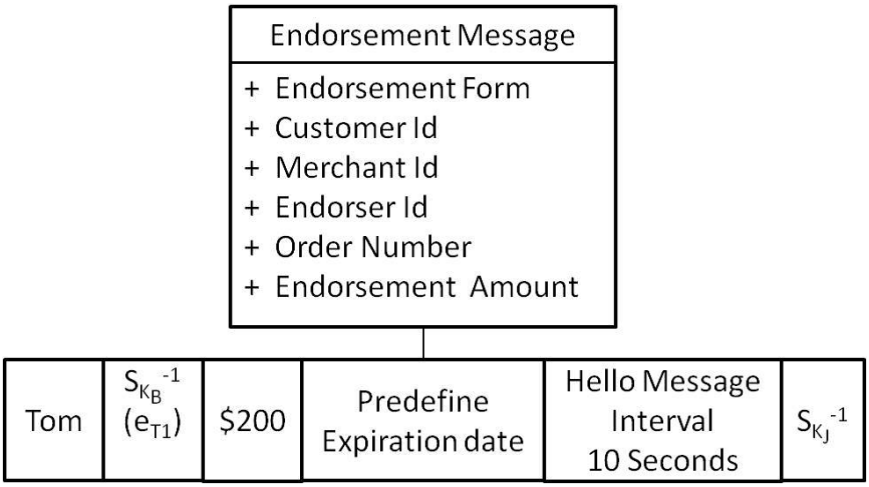

Figure 19. An example of an endorsement message

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.

The e-coin has a predetermined expiration date that is set by the bank. 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. In a situation where an e-coin is lost or corrupted while being transmitted to an endorser, the e-coin will be invalidated after a predetermined date set by the bank, 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.

4.1.3 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 20. 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.

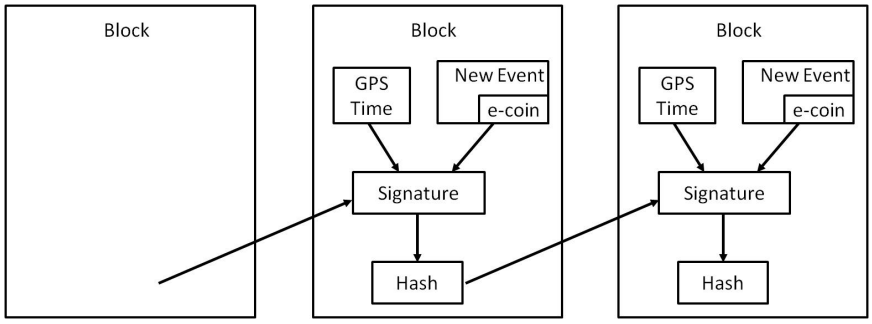

Figure 20. Event Chain

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 21. 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.

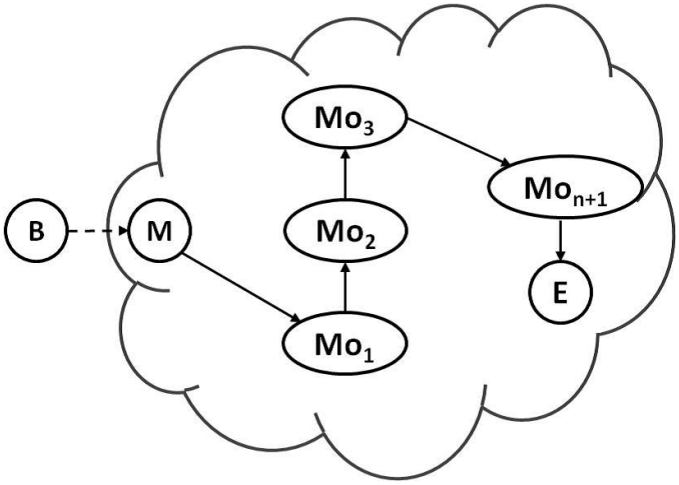

Figure 21. Receiving a new E-coin

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.

4.1.4 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 . 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.

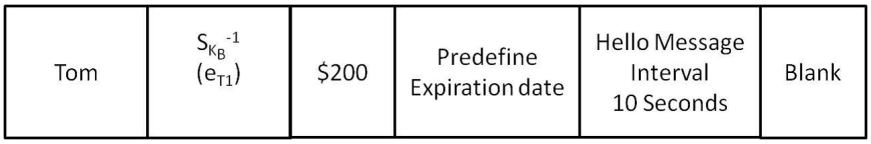

Figure 22. Example of location information based monitoring

4.1.5 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 [2]. 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.

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

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

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 [23], a method is proposed to do this using cryptography. We use this method in our system.

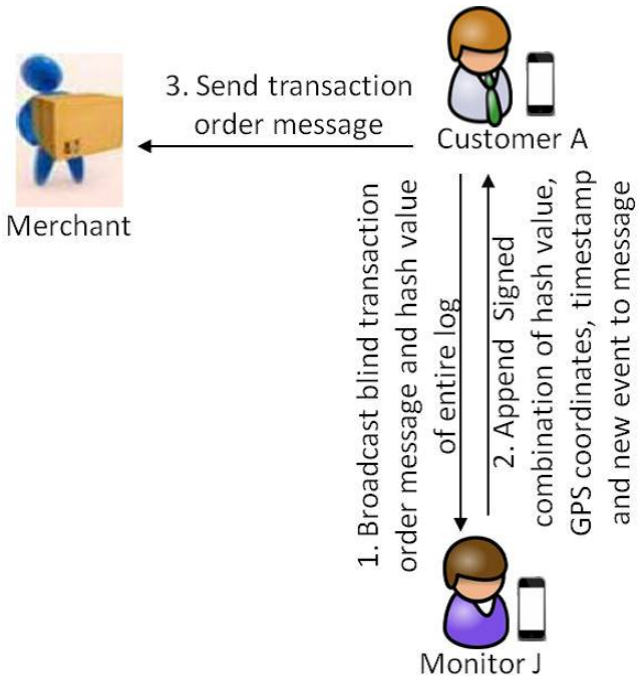

Figure 23. Preventing reset and recovery attack from a customer

Preventing attack from a customer : The scheme is illustrated in Figure 23.

- 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 23 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.

4.1.6 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 24, depending on the number of endorsers they have as their primary endorsers.

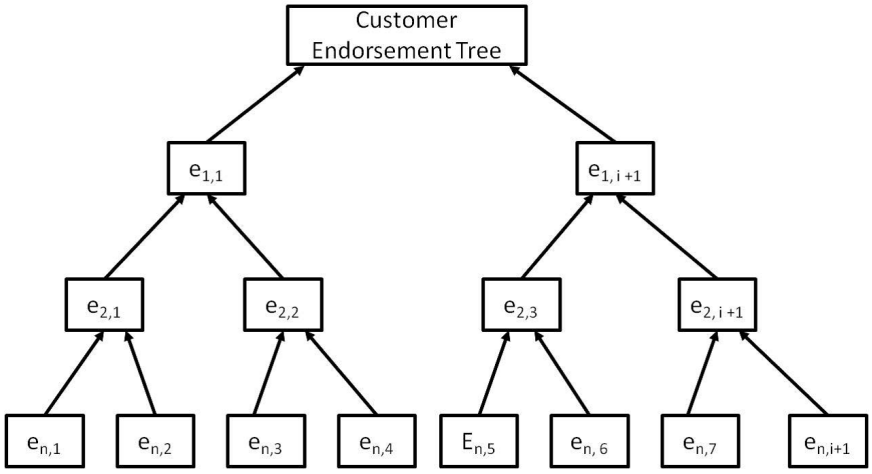

Figure 24. Customer endorsement tree

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 25.

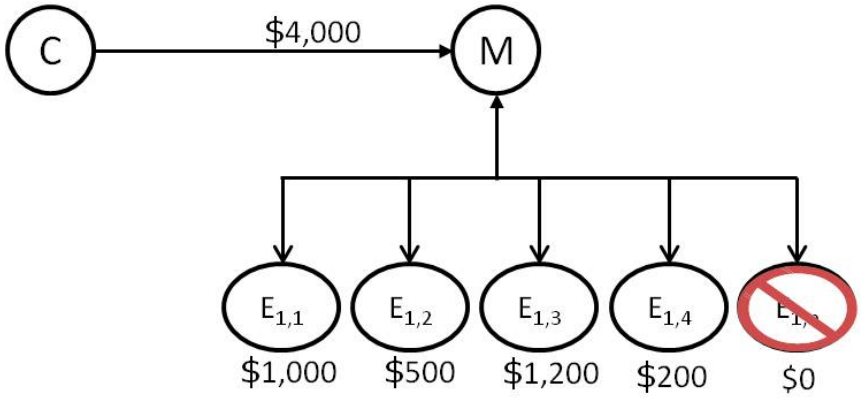

Figure 25. Chains of Endorsement during Transaction

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 customer's 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 26. 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.

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

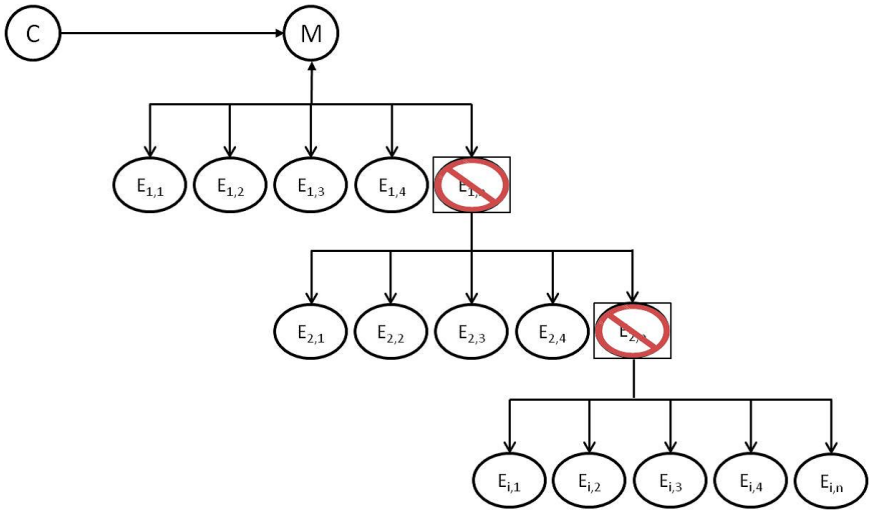

Figure 26. Chains of Endorsement during Transaction with unavailable Endorsers

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.

4.1.7 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.

4.2 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.

4.3 Procedures of Endorsement-based Mobile Payment System

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

1. Customer A creates a transaction order message and blinds the transaction order message using a blind signature; then computes the hash value of the last event chain block and appends it to the message; then broadcasts the message.

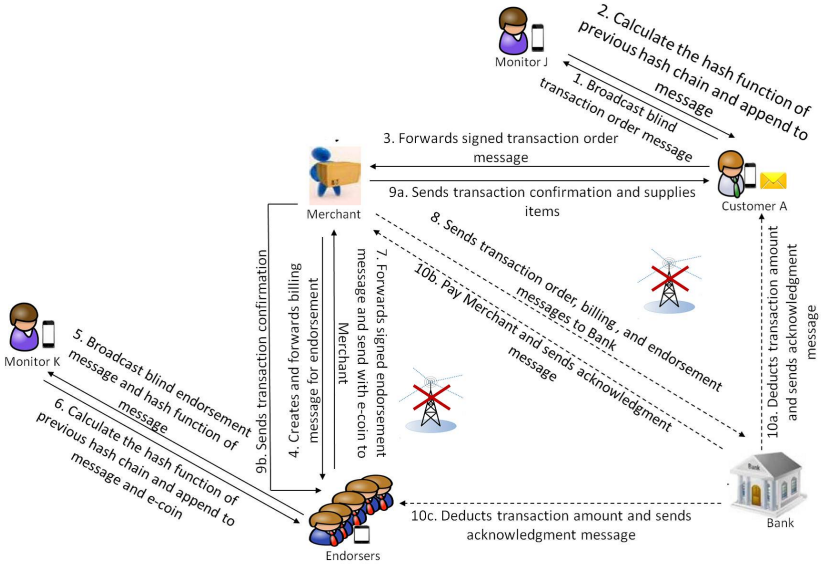

Figure 27. Overview of the proposed mobile payment system

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

3. Customer A unblinds the transaction order message and forwards the signed transaction order message to the merchant.

4. 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.

5. 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.

6. 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.

7. Endorser E unblinds the endorsement message and forwards the signed endorsement message with an e-coin to the merchant.

8. 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.

9. Merchant M sends a transaction confirmation to customer A and to endorser E and supplies the item to customer A.

10. 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.

5. Evaluation Plan

In order to evaluate the performance of our proposed payment system, we are going to develop a simulator to check the effectiveness of our method in a disaster area. Our main objectives are to ensure (i) reduction of communication overhead cost, (ii) reduction of storage overhead cost, and (iii) reduction of computation in order to provide that an excellent service for people in a disaster area. Our simulation will avail us the opportunity to test various low computational cryptography algorithms, thereby allowing us to select the most optimized cryptography algorithm best suited for reducing overheads in a disaster area. Table 3 shows values of network parameters in a disaster area.

Simulation Description : We will conduct our simulation using a customized simulator developed by using JAVA programming language. The simulated scenario will consist of mobile nodes that are first randomly placed in an area and then move according to some mobility models. We assume 802.11g wireless WiFi is used for communication in our simulation.

Table 3. Typical simulation parameters value in a disaster area

Parameter	**Default Value**
Network	
Bandwidth	1 Mbps
Transmission range	100 m
Map	
Disaster area size	5 km x 5 km
Number of mobile nodes	200–500
Node	
Speed	1 - 3 m/s
Mobility Model	Random Waypoint
Message	
Size	3 KB
Hello Message Size	5 bytes
Hello message Interval	10secs

The following metrics will be measured in our simulation.

- **Message delivery ratio**: The message delivery ratio is computed with the following formula:

$$Delivery\ ratio = \frac{Number\ of\ messages\ delivered}{Number\ of\ messages\ sent}$$

- **Frequency of breakage of event chain :** In our mechanism, we introduced event chains to prevent double spending. However, dishonest users in the network will cause transactions rejected and thus breaking event chain. We will check the frequency of event chain breakage, which is computed with the following formula:

$$Frequency = \frac{Number\ of\ rejected\ transactions}{Number\ of\ delivered\ messages}$$

- **Response time of service :** The time it takes to complete a transaction successfully will also be measured. We will introduce different mobility models to measure transaction completion time and its impact on our payment system.

Overheads

- **Storage overhead :** In our proposed mechanism, each user needs to store the event chain, Hello message and endorsement tree header. The impact of storing the information on a mobile device with limited resources will be measured.

- **Computational overhead :** Due to limited resource of mobile devices in a disaster area, cryptographic algorithms requiring high computation power cannot be used. Therefore, to reduce computational overhead in our system, the computing time of our schemes will be measured for the encryption algorithm, decryption algorithm; blind signature and hash function operations a user needs to perform in the system. We will use an RSA cryptosystem and compare its computational overhead to some other cryptographic systems, thereby selecting the optimal cryptographic algorithm of low overhead cost without compromising the security of our system.

6. Conclusions

In this thesis, 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.

Appendix

A. Discussion

In this thesis, we proposed a new mobile payment system which allows users to shop in a disaster area. Specially, we proposed 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. However, there are some comments regarding the payment system proposed in this thesis listed below.

- Question: Why is the proposed system restricted to a disaster area?
- There are many payment systems, providing online digital currency services, but such online services rely on communication infrastructure to enable transactions, which make it unreliable for people in a disaster area or places without network connection. Therefore, we restrict our proposed system to a disaster area to allow users to shop there. Our proposed system can also work online as a digital currency.

- Question: How does the proposed system realize privacy protection?
- Answer: The user privacy protection is secured in our system by using user nicknames a Temporary ID in every transaction. The temporary ID is also scrambled to give a user different ID per transaction. In addition, all messages in the network are encrypted and digitally signed by users. Using digitally signed photographs for authentication does not degrade the privacy protection of the system as the process is the same as checking an individual photograph on an identity card.

- Question: What is the mechanism to prevent collusion?
- Answer: The e-coin technique is introduced to check the bank balance of endorsers to prevent collusion between a user and an endorser. In order to

buy an e-coin, some money has to be deposited and this will be used for endorsement alone. In addition, we introduced an event chain mechanism to prevent endorsers from double spending their e-coins and from overspending more than the available balance in their endorsement account such that any transaction that does not have an e-coin attached is rejected.

- Question: What are the incentives for endorsers?
- Answer: To encourage users to endorse others and stay honest in the system, we introduce an incentive mechanism in which an endorser is awarded some part of the transaction amount (for example, 3% of the transaction cost).

- Question: How to prevent a customer from endorsing himself/herself?
- Answer: Our proposed mechanism uses endorsement tree to prevent endorsers from endorsing him/herself. The endorsement tree is created by a bank during registration and updated when a customer have new endorsers. Each endorser ID is mapped to a customer in the endorsement tree, thereby preventing an endorser to be able to endorse him/herself during a transaction.

- Question: What is the relationship between the proposed system and Bitcoin?
- Answer: Our proposed system adopts an approach similar to that of Bitcoin by broadcasting transactions to neighboring nodes. However, the proposed system differs in techniques, since users in our system do not need proof of work, a mechanism requiring great computation power. Rather, users in our system only compute the hash value of a transaction log which requires little computation power and neighboring nodes then append their signatures to the log to form an event chain (similar to a block chain in Bitcoin networks). Our payment system is suitable for mobile devices of limited

computational power in a disaster area.

- Question: What is the benefit of endorsing?
- Answer: Endorsement guarantees that a merchant gets paid after each successful transaction. This will encourage merchant participation in the payment system. In addition, users contribute to helping each other in a disaster situation. Also, endorsing allows each user to make new transactions right after turning the phone off and on.

- Question: What is the difference between escrow services of some online auction and the proposed endorsement?
- Answer: Online escrow services depend on independent trusted third party while our proposed endorsement scheme is just between users. Also, the online escrow services require communication infrastructures and cannot detect double spending; therefore, it cannot be relied on in disaster areas.

- Question: Is finding the endorsers manual or automatic?
- Answer: The merchant can find the endorsers of a customer automatically.

- Question: How can merchant access the endorsers?
- Answer: The merchant obtains the information of the endorsers and secondary endorsers from the endorsement tree header. The endorsement tree header is used to provide information on how the merchant can access the endorsers.

- Question: How can the merchant get the endorsement tree?

- Answer: The customer includes in his transaction message the endorsement tree header which contains the information of the customer's secondary endorsers up to a predefined level (e.g. Level 5).

- Question: Does the merchant need to find the monitoring users?
- Answer: No. The customer or endorsers find the monitoring users to monitor their transaction. The merchant can validate the monitoring user's signature.

- Question: What happen if there is missing information in the previous block of an event chain?
- Answer: A missing information in the previous block means the event chain is broken and cannot be used again in any transaction.

- Question: How frequently is an event chain broken?
- Answer: The frequency of an event chain breakage will be tested in our simulation by checking the number of rejected transactions over the number of total messages delivered. However, there are some transactions that will be rejected when an endorser failed to attach an e-coin to his/her endorsement message. This will be separated to know the actual frequency of event chain breakage.

- Question: What is the relationship between the customer balance account and endorsement account balance?
- Answer: We separate the customer account balance from the endorsement account balance. The customer account balance is used to pay for item purchased by the customer while the endorsement account balance is used by the endorser to guarantee the customer's transaction. The endorsers deposit some money into an endorsement account, in a situation that the

customer does not have enough money to pay for the item purchased, the endorsement amount is deducted from the endorsement account balance of the endorser.

- Question: Is there control on the number of users an endorser can endorse?
- Answer: The number of users an endorser can endorse is not limited. However, each endorser decides the endorsement amount and the number of users they want to endorse on their own. For example, if an endorser has $10,000 in his endorsement accounts and decides during registration to endorse 10 users with $1,000 each. The endorser can only endorse more than 10 users if he/she decides to reduce the endorsement amount of each user to be less than $1,000. The endorser however, needs to contact the bank to add a new user they want to endorse and change the endorsement amount of each user before he/she can endorse a new user.

- Question: What happen if a user tries to use already spent e-coin outside a disaster area?
- Answer: An endorser cannot pay for an item from the endorsement account because the endorsement account is locked and can only be used for endorsing other user's transaction.

B. Definition of Terms

Anonymity: is a situation where a user's real identity cannot be connected with his/her assumed name (temporary identity) used in a transaction.

Bank: is an organization that maintains users' accounts.

Blind signature: is a method in which a person gets a message signed by another party without revealing any information about the message to that party.

Central authority: is a trusted party that is in-charge of issuing an electronic currency, and setting the regulations on the use and misuse of the electronic currency. A central authority also manages user account (such as deducting money from a customer's account and paying a merchant).

Clearing and settlement: a process carried out by a trusted party to compare the transaction made by a customer with the monetary value a merchant claimed the customer spent.

Collusion: is a secret agreement between two or more parties to defraud another user of his/her money or goods.

Credential: is digital information that is unique to a user and is used to access or authenticate a user in a payment system.

Cryptographic: is the art of coding and decoding a message to make it secure.

Cryptosystem: is a collection of cryptographic algorithms used for encoding and decoding of a message.

Business-to-business service (B2B): is an electronic transaction or service between companies in a payment system.

Customer: is a user that buys goods, services, products or software from a merchant.

Merchant: is a user that provides goods, services, products or software.

Monitoring customer: is a customer that checks every transaction within the radio range to make sure that each is valid and reliable.

Decrypt: is the process of changing a data from a form that is difficult-to-

understand to the original form using a mathematical algorithm.

Digital currency: an electronic equivalent of physical cash that is stored digitally.

Digital signature: is a mathematical procedure used to confirm the reliability of a message or document.

Double spending: is using an e-currency more than once to pay the same or different people.

Encrypt: is the process of changing a data from its original form to a form that is difficult-to-understand using a mathematical algorithm.

Endorser: is a user who pledges to fulfill the customer's obligation should the customer fail to pay for items bought.

Endorsement: is a mechanism by which a user agrees to endorse a customer by signing a form to guarantee paying the customer's merchant even the customer fails to pay his/her merchant.

Endorsement account: an account chosen to guarantee a customer's transaction in a situation where the customer fails to pay.

Endorsement-chains tree: is a tree like structure used to connect a customer to an endorser and to determine the level of endorsers.

Escrow service: is when a third party agrees to receive money on behalf of the two parties and the money is released if the condition of the transaction is meant.

Event chain: is a successive application of a cryptographic hash function on a piece of data.

E-coin: is electronic money that is used for payment of goods/services in an online e-commerce.

Fraudulent transaction: is an illegal transaction carried out by a dishonest user with another person's payment information.

Hash function: is a mathematically derive function used to compress data of an arbitrary length to a fixed length of data.

Mobile ad-hoc network (MANET): is a self-configuring network that consists of independent nodes that are connected by wireless communication.

Mobile payment system: is a method that allows a customer to pay for a transaction using a mobile device (such as a Smartphone).

Modulo operation: is a mathematical equation used to get the remainder of a number after its division by another number.

Near field communication (NFC): is a wireless technology that allows smart phones and other devices to establish radio communication with each other by bringing them together.

Ombudsman: is an independent, trusted party that facilitates resolution of complaints between parties in a payment system.

Overspending: is when a user spends more than the money in his/her bank or digital currency account.

Point of sale: is an electronic device configured to read and verify user payment information.

Public key: is a cryptography key that is used to encode a message that is intended for a particular user.

Private key: is a cryptography key that is used to decode a secret message that is received from a particular user.

Replay attack: is an attack where an adversary intercepts some data and retransmits it later.

Repudiation: is when a customer denies making a transaction after the goods/services have been provided for him/her.

Reset and recover attack: is an attack, in which a user backed up all transaction data already used to buy an item and then rests 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.

Rivest, Shamir, and Adelman (RSA) algorithm: is a cryptosystem that is based on public key encryption used for both encryption and authentication.

Symmetric encryption: is a cryptography algorithm in which the same key is used for both encoding and decoding of the message.

Transaction: is a process in which goods, services, or money are exchanged between one person or company and another person or a company.

Transaction billing form: is a form containing the details of the number of items a customer bought and the amount supposed to be paid to the merchant.

Transaction endorsement form: is an form signed as proof of agreeing to pay by an endorser should the customer fail to pay for items purchased.

Transaction order: is a form containing the details of the items to be purchased from the merchant.

Trusted third party: is an entity that is trusted by two parties to facilitate

interactions between both parties. An example of a trusted third party in a transaction between a customer and a merchant is a bank.

Acknowledgements

My sincere appreciation goes to Almighty God for keeping me alive to complete my Master degree in good health.

I would like to express my profound gratitude to Professor Minoru Ito for his support and for giving me the opportunity to do my Master program in Foundations of Software Laboratory. His invaluable comments and suggestions have been a great contribution to the success of my research.

My gratitude also goes to Professor Keiichi Yasumoto for his vital and helpful comments and discussion which has contributed greatly to the success of my research.

I am sincerely grateful to Associate Professor Naoki Shibata, for his support, suggestions, advices and teachings without which this research would be impossible. I learned a lot from discussions during research meetings, which has helped my research and my personal life.

I also appreciate Assistant Professor Juntao Gao for his support, comments and contribution to my research. I am grateful for the assistant during my research.

My deep appreciation goes to Mrs. Miki Ikeda, past and current students of Foundations of Software Laboratory, all African students in NAIST and other international students that have made staying in Japan enjoyable.

Finally, I would like to say a big thank you to my lovely wife - Adebola Ojetunde for her encouragement and support during my Master degree. Also, I'm grateful to my family and my in-laws for their prayers and support.

References

[1] A. Mishra and K. M. Nadkarni: "Security in Wireless Ad Hoc Networks (Chapter 30)", CRC Press LLC, 2003

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

[3] J. S. Wang, F. Y. 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] F. Y. Yang: "Efficient Trapdoor Hash Function for Digital Signatures", Chaoyang Journal, Vol. 12, pp. 351-357, 2007.

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

[6] H. Krawczyk, and T. Rabin: "Chamelon Signatures", (NDSS'00), Symposium on Network and Distributed Systems Security, pp. 143-154, 2000.

[7] A. Shamir, and Y. Tauman: "Improved Online/Offline Signature Schemes", Advances in Cryptology-CRYPTO'01, LNCS 2139, PP. 355-367, 2001.

[8] 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, Issue 2, pp. 869-877, 2005.

[9] 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.

[10] D. Chaum, B. Den Boer, E. Van Heyst, S. Mjlsnes, and A. Steenbeek: "Efficient offline electronic checks", EUROCRYPT '89 Proceedings of the workshop on the theory and application of cryptographic techniques on Advances

in cryptology, pp. 294-301, Springer-Verlag New York, Inc., New York, NY, USA, 1990.

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

[12] 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.

[13] 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.

[14] 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.

[15] X. Dai, and B. Lo: "NetPay An Efficient Protocol for Micropayments on the WWW", Fifth Australian World Wide Web Conference, Australia (1999).

[16] X. Dai, and J. Grundy: "Architecture for a Component- based, Plug-in Micro-payment System", In Proceedings of the Fifth Asia Pacific Web Conference, LNCS 2642, Springer, pp. 251-262, April 2003.

[17] X. Dai, and J. Grundy: "Three Kinds of E-wallets for a NetPay Micropayment System", The Fifth International Conference on Web Information Systems Engineering, pp. 66 - 77, Brisbane, Australia. LNCS 3306, November 22-24, 2004.

[18] 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.

[19] 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. [Online]. Available: http://dx.doi.org/10.1016/j.elerap.2007.02.001

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

[21] 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.

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

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

[24] Y. Huang, S. Shieh, and F. Ho: "A Generic Electronic Payment Model Supporting Multiple Merchant Transactions", Comput. Secur., Vol. 19, pp. 453-465, 5 July 2000.

[25] M. Jakobsson, and M. Yung: "Revokable and versatile electronic money (extended abstract)", In Proceedings of the 3rd ACM conference on Computer and communications security (CCS '96), pp. 76-87, ACM, New York, NY, USA, 1996.

[26] C. Boyd, and E. Foo: "Off-Line Fair Payment Protocols Using Convertible Signatures", In Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '98), pp. 271-285, Springer-Verlag, London, UK. 1998.

[27] N. Asokan, V. Shoup, and M. Waidner: "Optimistic Fair Exchange of Digital Signatures", In Advances in Cryptology, Proceedings of EUROCRYPT '98, pp. 591-606, Springer-Verlag, Espoo Finland, May 1998.

[28] F. Bao, R. H. Deng, and W. Mao: "Efficient and Practical Fair Exchange Protocols with Off-line TTP", In Proceedings of CRYPTO '90, pp. 189-205, Springer-Verlag, 1991.

[29] D. Chaum: "Designated Confirmer Signatures", In Advances in Cryptology, Proceedings of EUROCRYPT '94, pp. 86-91, Springer-Verlag, Perugia Italy, May 1994.

[30] P. Sarkar: "Multiple-Use Transferable E-Cash", International Journal of Computer Applications, Vol. 77, pp. 35-38, September 2013.

[31] X. Dai, and J. Grundy: "Off-Line Micro-payment System for Content Sharing in P2P Networks", Distributed Computing and Internet Technology, Vol. 3816, pp. 297-307, Springer Berlin Heidelberg, 2005.

[32] A. Tiwari, S. Sanyal, A. Abraham, and S. Sanyal: "A Multi-Factor Security Protocol for Wireless Payment - Secure Web Authentication using Mobile Devices", CoRR, 2011. http://arxiv.org/abs/1111.3010.

List of Publications

Domestic Conference

1. Babatunde Ojetunde, Naoki Shibata, Juntao Gao, Minoru Ito, "Consideration of a Mobile Payment System using Endorsement in MANETs for a Disaster Area," *Proc. Information Processing Society of Japan, IPSJ*, CSEC-66 No.5, pp. 1-8, June 26, 2014.

2. Babatunde Ojetunde, Naoki Shibata, Juntao Gao, Minoru Ito, "A Proposal of an Endorsement Based Mobile Payment System for A Disaster Area (Poster)," *22nd multimedia communication and Distributed Processing workshop(DPSWS2014)*, pp.98-100, Dec 2014.

International Conference

1. Babatunde Ojetunde, Naoki Shibata, Juntao Gao, Minoru Ito, "An Endorsement Based Mobile Payment System for A Disaster Area," *to appear in Proc. of The 29th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015)*, March 2015.