# An Extended Payment Model for M-Commerce with Fair Non-Repudiation Protocols

Tran Khanh DANG and Thi Thanh Huyen PHAN

***Abstract*—Non-repudiation in e-commerce has recently gained a lot of interest but its successor brother, non-repudiation in m-commerce, is still at the start. In this paper, we propose an extension of existing mobile payment models to introduce an extended mobile payment service (EMPS) model, which is based on assumptions about the cooperation between mobile network operators and financial institutions to deal with different payment amounts ranging from micro to macro payment. The novel model focuses on enhancement of non-repudiation problem. Fair non-repudiation protocols are developed for not only payment phase but also other phases in a typical m-commerce transaction, including price negotiation and content delivery. Joint signatures method is used in protocols to overcome the limitations in mobile handheld device capability and to reduce the trust dependence totally on the payment service. As with the proposed non-repudiation protocols, EMPS plays the role of a semi-trusted third party and is an indispensable factor for creating the fairness property. Non-repudiation analyses of these protocols are also conducted besides some guidelines for ensuring non-repudiation in m-commerce.**

***Index Terms*—Communication system security, M-commerce security, non-repudiation, semi-trusted 3rd party, payment model.**

## I. Introduction

IN recent years, *m-commerce* with many advantages such as the ubiquity, reachability, localization has emerged as a new potential application and research area. However, its inherently secure weaknesses, resulted from the limited capacity and the mobility of mobile handheld devices, insecure wireless channel, etc are the main obstacles on the path of success. Basically, security in m-commerce also deals with the fundamental issues as authentication and authorization, confidentiality, integrity, availability, and non-repudiation. Among these issues, non-repudiation, one of the services used to cope with internal attack risks, almost has not been studied thoroughly.

Manuscript received June 29, 2009. Manuscript accepted for publication November 17, 2009.

This work was supported in part by Advances in Security & Information Systems (ASIS) Lab, Faculty of Computer Science & Engineering, HCMUT, Vietnam.

T. K. Dang is with the Faculty of Computer Science & Engineering, HCMC University of Technology, VNUHCM, Ho Chi Minh City, Vietnam (phone:+84-8-38647256, ext. 5841, e-mail: khanh@cse.hcmut.edu.vn).

T. T. H. Phan is with the Faculty of Computer Science & Engineering, HCMC University of Technology, VNUHCM, Ho Chi Minh City, Vietnam (phone:+84-8-38647256, ext. 5842, e-mail: huyenttp@cse.hcmut.edu.vn).

Repudiation is the false denial of having been involved in a communication. The goal of the non-repudiation service is to generate, collect, maintain, make available and verify evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action [12]. Currently, most non-repudiation protocols use digital signature in generating non-repudiation evidences. Among the properties of a non-repudiation protocol, fairness may be the most desirable. This feature helps the protocol execute fairly, i.e. at the end of the protocol, either both entities get the expected evidences, or none of them get any valuable information. Using a trusted third party (TTP) is a common approach to resolve this problem.

The power of non-repudiation services creates its importance to the commercial transactions in e-/m-commerce environments where the parties participating in may not trust each other. Non-repudiation in e-commerce has generated a lot of interests recently and built a relatively sound foundation while this issue in m-commerce is still at a start. Although m-commerce can be considered as mobile e-commerce, we can not apply the same non-repudiation protocols in e-commerce to the new environment because of the inherently insecure nature of wireless network and limited capability of mobile devices. Therefore, we need lightweight but sufficiently secure non-repudiation protocols to protect transactions conducted in wireless environment. Non-repudiation protocols in m-commerce should be based on existing non-repudiation protocols in e-commerce and adjusted to suit the resource constraints of mobile devices as well as specific requirements of different transaction types. Nearly all currently existing research mentioning the non-repudiation in m-commerce just pays attention to this problem in mobile payment, one of the most important commercial transactions in m-commerce. Mobile payment or billing is defined as the process of two parties exchanging financial value using a mobile device in return for goods or services [13]. A general mobile payment system, along with a typical transaction, is described in figure 1. It uses a third party which could act at the same time as a payment service provider and a TTP to support the financial transaction between mobile customer and service provider. As with m-commerce, none of the proposed solutions gives a complete analysis of non-repudiation properties such as non-repudiation evidences, the fairness property, the timeliness properties or a formal verification and so on. Moreover, some

forget the limited capability of mobile handheld devices while other solutions are suitable for only some specific cases.

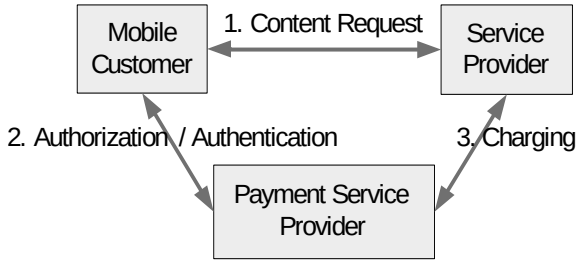


Fig. 1. A general mobile payment system.

In this paper, we propose a new mobile payment system founded on the extension of existing ones to support not only the non-repudiation protocol in the payment stage but also the other phases of a general commercial transaction such as price negotiation, content delivery, placing particular emphasis on the payment phase. In the proposed system, in addition to the traditional role, payment service provider also takes the role of a semi-trusted third party in non-repudiation protocols and supports mobile devices in generating non-repudiation evidences to help them overcome their limitations in computational power. The model and protocols proposed also address a variety of payment methods like credit card/account based payment methods, phone bill charging method and payment amounts like macro/micro payment.

The rest of this paper is organized as follows. Section 2 briefly discusses the related work. Section 3 presents common requirements and properties of non-repudiation protocols in m-commerce. In section 4, we introduce an extension of existing mobile payment systems, the overall architecture and innovations of our approach, and present three non-repudiation protocols for mobile transactions. Next, we carry out theoretical analyses of the proposed protocols in section 5. Finally, section 6 gives concluding remarks and presents future work.

## II. Related Work

There are several mobile payment models, ranging from the concept to universal model [2], and most of them do not refer to non-repudiation problems. Moreover, the other systems mentioning non-repudiation in their solutions either have too simple and inflexible models or give incomplete analysis and unsuitable non-repudiation protocols for m-commerce environment. Some typical previous work is discussed as follows.

- The limited models such as PayBox, Vodafone m-PayBill, iPIN [10] are restricted in payment methods, customer, secure mechanism and none of them provides non-repudiation protocols.
- SEMOPS [9] is a typical example of universal models. The model looks prettily perfect because it is capable of supporting all transactions values, operating in any channels and supporting any transaction type with a domestic and/or international geographic coverage. However, SEMOPS does not give any formal protocols for its transactions and non-repudiation is not handled too. Another limitation of SEMOPS is that the customer and service provider have to trust the payment processor absolutely. Furthermore, using data center increases the number of steps in a transaction and reasonable solutions to traditional problems around data center such as bottleneck, attack risks are not presented.
- The payment model presented in [2] is derived from SEMOPS model with some enhancements for tackling the signature validating and privacy issues. A protocol which is a formal representation of the payment process and some initial non-repudiation analyses are discussed in [2]. This is a very first effort for non-repudiation in m-commerce, but the proposed protocol does not take into account the limited capacity of mobile devices when using traditional signatures to generate non-repudiation evidences and the non-repudiation analysis is just the case of non-repudiation of origin. Moreover, the given protocol skips the differences in nature of different payment methods and payment value.
- Other solutions to non-repudiation in mobile payment concerning evidence generation cost are given in [1, 3]. Both of them use the joint signature instead of traditional digital signature to reduce cost but one is for home network and the other is for foreign network. Although they are better than the aforementioned ones due to low cost, deeper non-repudiation analysis, they are only suitable for small payment which charges mobile customers through their phone bills.

## III. Non-Repudiation Considerations in M-Commerce

An m-commerce transaction taking place between mobile customer (MC) and service provider (SP) usually involves three phases: price negotiation, payment and content delivery. The non-repudiation requirements for this transaction include:

- *Non-repudiation in price negotiation phase:* MC and SP can not falsely deny having involved in the communication and agreed on the given price.
- *Non-repudiation in payment phase:* MC can not falsely deny having agreed to pay her bill and SP can not falsely deny having received the payment for the invoice of MC.
- *Non-repudiation in content delivery phase*: MC can not falsely deny having received goods and SP can not falsely deny having not delivered the goods.

By examining the existing non-repudiation protocols in e-commerce and specific properties of m-commerce like the limited computational capability, inherently insecure wireless network, we identify some requirements for building non-repudiation protocols in m-commerce:

- They should be built on the non-repudiation foundation in e-commerce.
- Number of messages originated from mobile customer should be minimized.

- Cost for non-repudiation evidence generation and verification should be low but the used methods must reach an acceptable level of data security.
- A third party supporting the data delivery and evidence generation should be employed and the candidate for this role will vary according to transaction type and be chosen from the main players in mobile commerce environment such as mobile network operator (MNO), bank. Moreover, we should reduce the trust dependence on these third parties.
- Specific properties of each transaction type should be examined.

### A. Non-Repudiation Evidence

Most of the existing solutions for non-repudiation in mobile commerce are reducing cost in non-repudiation evidence generation resulted from the limited computational capability of mobile devices. They can be divided into two groups: one based on the symmetric key technique and the other founded on the digital signature technique.

- *Symmetric key technique:* The idea is to use the symmetric cryptographic technique to create evidence at a low cost. However, if we use just a secret key k shared between two parties, generated evidence can not be irrefutable. The solution here is different from the rule of secure envelops mechanism in non-repudiation in e-commerce. It combines using 2 secret key $k_1$, shared between MC and SP, $k_2$, shared between MC and TTP, with other techniques such as hash, keyed hash, MAC. Therefore, the evidence containing both $k_1$ and $k_2$ must be generated by MC. A number of proposals like [8] can be counted in this group.
- *Digital signature technique:* Although digital signature can ensure the non-repudiation of origin of evidence, the cost of generating it is too high for limited computational devices to execute. Some schemes have been proposed to address this problem by designing more efficient mathematical algorithm. Other proposals use a third party to sign message on the original signer's behalf such as joint signature, proxy signature or server-supported signature [1].

### B. Trusted Third Party

The particular properties of m-commerce environment influence the choice of candidate for TTP role in a non-repudiation protocol. Besides the traditional TTP which is indispensable for a non-repudiation protocol such as time-stamping authority (TSA), certification authority (CA), TTP assisting in fair exchange of the message and/or non-repudiation evidence can be one or combination of the following players:

- *Mobile Network Operator (MNO):* MNO owns the channels and almost all communications in mobile environment must pass through it. Besides its large customer bases, MNO has a lot of experience in the fields of billing and roaming.
- *Financial Institution/Bank (FI/B):* Its strengths lie in the trust of customers and long-standing customer relationships. Stemming from its expertise to handle transaction and risk, the necessary licenses, large customer and merchant bases, etc, FI/B is a valuable candidate for the role of a TTP, especially in the case of payment services.
- *Independent agent (IA)*: Although IA does not have advantages like MNO or FI/B such as the trust of customers and large customer bases; it can be more flexible and faster to explore new technologies than MNO or FI/B. Moreover, IA can collaborate with different mobile network operators and financial institution to offer its services to a variety of customers.

## IV. EMPS System Model with Non-Repudiation Protocols

This section presents our main contributions, solutions to non-repudiation in m-commerce, by building an extended mobile payment service (EMPS) to support non-repudiation protocols in not only the payment phase but also other phases in a general m-commerce transaction including price negotiation and content delivery.

### A. EMPS System Model

EMPS system model is based on the models introduced in [2, 9] because of their extensibility and universality. Some improvements are suggested to meet our requirements.

- A data center is not used in our model because it increases the complexity of the non-repudiation protocol with many steps, third parties and the trust level to third parties. Moreover, the other problems in a data center such as bottleneck, attack risk, message integrity can arise. In our model, customers of different EMPSs can do business together if their EMPSs have made a deal.
- Our model is also a payment service, so the value of transaction greatly affects the proposed protocols. Payment amounts are usually categorized in micro and macro payment. Micro payment refers to small purchases, usually less than 10 Euro and macro payment is about large purchases over 10 Euro. EMPS assumes that MNO and FI/B will collaborate on payment phase. Micro payment has low requirements for security but cost efficiency, hence it is reasonable to ask MNO to charge customers through their mobile phone bills. Marco payment requires higher security level, thus it should be paid by customer's bank account or card. FI/B with a lot of experience in payment services and risk management will responsible for macro payment.
- An innovation of EMPS is that it not only features mobile payment service but also supports MC and SP in price negotiation and good delivery in order to obtain a fair non-repudiation transaction. This is the reason we name this model *Extended Mobile Payment Service*.
- To reduce computational load on mobile user without affecting the system security, we use the idea of joint signature [1] in generating non-repudiation evidences. MC will have 2 secret keys: $k_{mc,emps\text{-}mc}$ shared between MC and EMPS of MC, $k_{mc,sp}$, shared between MC and SP. This means MC is the originator of messages

containing both $k_{mc,emps-mc}$ and $k_{mc,sp}$. EMPS of MC, which has large computational capability and also involves in the transaction between MC and SP, will sign on these messages to create the irrefutable evidences of non-repudiation protocols.

– A strong point of this model is the ability to reduce the trust dependence of MC to EMPS. In the system, EMPS can be regarded as a semi-trusted third party. This implies that EMPS just helps MC sign evidences and transfer them to other parties but it cannot modify or forge these evidences because of the presence of the secret key $k_{mc,sp}$, which is known only by MC and SP, in these evidences.

The system model of EMPS is shown in figure 2. There are four main parties participating in this model: MC, SP, EMPS-MC, and EMPS-SP. To gain the generality, we assume that MC and SP register to different EMPSs and these EMPSs trust each other. EMPS-MC and EMPS-SP are the payment service providers of MC and SP respectively. In our model, MNO collaborates with FI/B to build EMPS. While FI/B deals with macro payment, MNO is responsible for micro payment and supports MC in generating joint signature besides the traditional role of wireless access provider. In addition to these main parties, TSA and CA which are the essential TTP in most non-repudiation protocols also appear in our model. TSA is used to add trusted time information to evidence; and in the non-repudiation protocols, the step in which evidence is time-stamped is usually omitted for simplicity. CA is another TTP that issues public key certificates to guarantee the authenticity of public verification keys used for non-repudiation purpose.

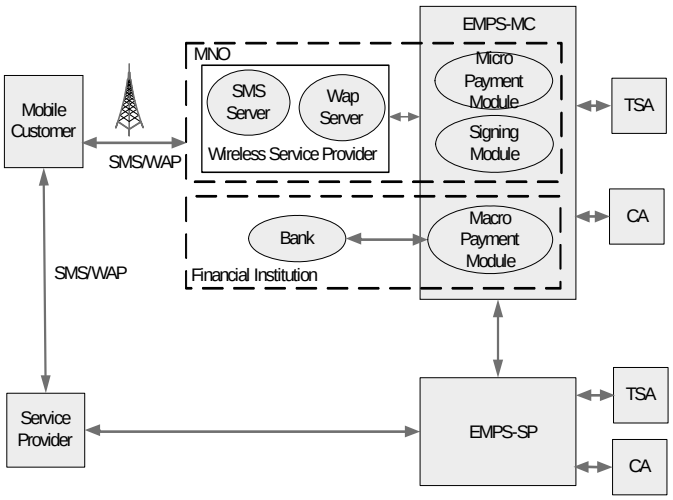


Fig. 2. EMPS System Model

Due to the space limitation, we just summarize main features of crucial modules in EMPS. Micro Payment Module handles micro payment and Macro Payment Module involves in macro payment. Signing Module helps MC generate joint signature on evidences and messages. Price Negotiation Module manages the related message in price negotiation phase and Content Delivery Module deals with managing the related messages in content delivery phase. Another module is User Management Module which manages customers of EMPS. Customers of EMPS can be categorized into MC, SP and other EMPS. Therefore, we need some communication modules serving the interaction between MC and EMPS, SP and EMPS as well as between EMPSs. In order to facilitate customers' easy access to the services, EMPS also supplies the front-end modules to MC and SP, especially MC front-end module which can assist MC to carry out an m-commerce transaction with necessary functions such as price negotiation, payment, personalization, and security.

### *B. Fair Non-Repudiation Protocols of M-Commerce Transactions in EMPS*

TABLE I
NOTATIONS.

| | |
|---|---|
| h(m) | Collision resistant hash function |
| $m_1$, $m_2$ | Concatenation of data item $m_1$ and $m_2$ |
| $k_{A,B}$ | Session key shared between A and B |
| $ID_A$ | Identity of entity A |
| $pk_A=(e_A, n_A)$ | Public key of entity A |
| $sk_A=(d_A, n_A)$ | Private key of entity A |
| $s_A=(h(m))^{d(A)} \bmod n_A$ | Entity A signature over message m |
| Ek | A symmetric key encryption function under key k |
| Dk | A symmetric key decryption function under key k |
| c=Ek(m) | Cipher of message m under the key k |
| $E_A$ | A public key encryption function under A's public key |
| $D_A$ | A public key decryption function under A's private key |
| $cert_A$ | Digital Certificate of entity A |
| L | A label uniquely identifies a protocol run |
| F | A flag indicating the purpose of a message |
| y=HOAC | Hash Origin Authentication Code |
| x=HMAC | Hash Message Authentication Code |
| $ts_A$ | Time stamp of entity A |
| $d_{A-P}$ | A deadline for response which is imposed by A in protocol P |
| $dl=[t_s, t_e]$ | A time interval |
| OI | Order Information |
| $P_A$ | Price suggested by entity A |
| PID | Identity of Product which MC intends to buy |
| N | Quantity of a Product which MC intends to buy |
| $Adr_A$ | Delivery address of A |
| $Account_A$ | Information about account of entity A |
| SC | Shipping cost |

In this section, we present three fair non-repudiation protocols built for three phases of an m-commerce transaction: price negotiation, payment and content delivery. Assume that the communication channels among EMPS, between EMPS and both SP/MC are resilient. The communication between MC and SP may be unreliable.

Firstly, there is an initiation process occurring before these three phases for establishing a session key shared between MC and SP. As MC and EMPS-MC share a private key $k_{mc, emps-mc}$ which is issued to MC when she registers for services of EMPS-MC, we can apply the NAETEA protocol [4] in this case. At the end of the initiation process, MC and SP share a session key $k_{mc,sp}$ and SP also receives a hash value of the secret key shared between MC and EMPS-MC: $h(k_{mc,emps-mc})$. Secondly, joint signature method [1] is used in our protocols. To help readers grasp the general idea of the joint signature scheme we briefly explain the used notations in Table I.

***Price Negotiation Phase***

In this phase, MC negotiates with SP for certain goods. First, MC sends the order containing information about product identity (PID), amount (N), bidding price ($P_{mc}$): $OI_{mc}$ = PID1, N1, $P1_{mc}$, PID2, N2, $P2_{mc}$.... along with HOAC, HMAC to EMPS-MC. $y_{pn}$ is the HOAC and includes the secret $k_{mc,sp}$ which is not known to EMPS-MC, thus EMPS-MC can not forge a valid $y_{pn}$ to SP. In addition, EMPS-MC can not get $k_{mc, sp}$ from $y_{pn}$ since it is hashed. HOAC also embeds the hash secret $h(k_{mc,emps-mc})$ to protect the SP against false accusation by MC, or impersonation attacks by the SP or other entities against the MC. $x_{pn}$ is the HMAC and can be used for source authentication because it contains $k_{mc, emps-mc}$ which is shared between MC and EMPS-MC only. Moreover, using the received HMAC, EMPS-MC can verify the integrity of $EK_{mc, sp}$ (OI) and $y_{pn}$. In short, the HOAC $y_{pn}$ indicates to SP that the original of $OI_{mc}$ is from MC and the HMAC $x_{pn}$ indicates to EMPS-MC that the HOAC $y_{pn}$ is from MC. dl is also introduced to check the freshness of the timestamp $ts_{mc}$ and prevent EMPS-MC from deliberately replaying the signature generation so as to gain advantage. $d_{mc-pn}$ is the deadline in which MC wants to receive the response of SP for its bidding prices. If the user is successfully authenticated, then in step 2, EMPS-MC will construct the joint signature from these messages and send to SP. In step 3, SP verifies the authenticity and integration of request. After successful request verification and validation, SP considers the bidding price of MC and replies with an OIResponse before the deadline $d_{mc-pn}$. SP also sets a deadline $d_{sp-pn}$ for MC's feedback and generates a label l used for future communications. If the prices in OIResponse are the same as those in $OI_{mc}$, SP and MC reach an agreement. On the contrary, this phase will be repeated until one agrees with the prices given by the other or decides to give up. l and OIResponse will be used in the other phases of the transaction.

**1. MC → EMPS-MC: $f_{pn}$, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $d_{mc-pn}$, dl, $ts_{mc}$, $Ek_{mc, sp}$ ($OI_{mc}$), $y_{pn}$, $x_{pn}$**
$y_{pn}$ = $h(OI_{mc}$, dl, $k_{mc,sp}$, $d_{mc-pn}$, $h(k_{mc,emps-mc}))$ and $x_{pn}$ = $h(Ek_{mc,sp}(OI_{mc}), f_{pn}, ID_{mc}, ID_{sp}, ID_{emps-mc}, ts_{mc}, k_{mc,emps-mc}, y_{pn})$.

**2. EMPS-MC → SP: $f_{pn}$, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $dl_{pn}$, $d_{mc-pn}$, $ts_{emps-mc}$, $cert_{emps-mc}$, $Ek_{mc, sp}$ ($OI_{mc}$), $y_{pn}$, $x_{pn}$, $signpn_{emps-mc}$**
The joint signature $signpn_{emps-mc}$ = $s_{emps-mc}(f_{pn}$, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $dl_{pn}$, $d_{mc-pn}$, $ts_{emps-mc}$, $Ek_{mc,sp}(OI_{mc})$, $y_{pn}$, $x_{pn})$.

**3. SP → MC: $f_{pn}$, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $d_{sp-pn}$, $Ek_{mc,sp}$($OI_{mc}$, OIResponse, $pk_{sp}$, l), $s_{sp}$($OI_{mc}$, OIResponse, $pk_{sp}$, l)**
OIResponse = $OI_{sp}$, SC, $d_{sp-pn}$ and l = $h(ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, h(OIResponse), $h(k_{mc, emps-mc}))$, $OI_{sp}$ = PID1, N1, $P1_{sp}$, PID2, N2, $P2_{sp}$....

***Payment Phase***

If MC and SP reach an agreement at the end of the negotiation phase, MC will conduct the payment phase. Depending on the payment amount, MC will choose the micro payment protocol or macro payment protocol.

**1. MC → EMPS-MC: $f_{mip}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $dl_{mip}$, $ts_{mc}$, $d_{mc-mip}$, $Ek_{mc, emps-mc}$ (OIResponse), $y_{mip, x_{mip}}$**
$y_{mip}$ = h(OIResponse, l, $dl_{mip}$, $k_{mc, sp}$, $d_{mc-mip}$, $h(k_{mc, emps-mc})$) is a HOAC showing SP that the original of the request for payment is from MC.
$x_{mip}$ = h(OIResponse, $f_{mip}$, $ts_{mc}$, $k_{mc, emps-mc}$, $y_{mip}$) is a HMAC showing EMPS-MC that the HOAC $y_{mip}$ is from MC.

**2. EMPS-MC → SP: $f_{mip}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $dl_{mip}$, $ts_{emps-mc}$, $d_{mc-mip}$, $E_{sp}$(OIResponse), $y_{mip, x_{mip}}$, $signmip_{emps-mc}$**
The joint signature $signmip_{emps-mc}$ = $s_{emps-mc}(f_{mip}$, l, $dl_{mip}$, $ts_{emps-mc}$, $d_{mc-mip}$, OIResponse, $y_{mip, x_{mip}})$

**3. SP → EMPS-SP: $f_{mip}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $d_{mc-mip}$, $E_{emps-sp}$ (Bill), $s_{sp}$ ($f_{mip}$, l, Bill, $d_{mc-mip}$)**
Bill = OIResponse, Approval

**4. EMPS-SP → EMPS-MC: $f_{mip}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $E_{emps-mc}$ (Bill, $Account_{emps-sp}$), $s_{emps-sp}$ ($f_{mip}$, l, Bill, $Account_{emps-sp}$)**

**5. EMPS-MC → MC: $f_{mip}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $Ek_{mc, emps-mc}$ (Bill), $s_{emps-mc}$ ($f_{mip}$, l, Bill)**

*Micro Payment Protocol*: MC sends the request for payment to SP through EMPS-MC. EMPS-MC creates the joint signature and encrypts the OIResponse by SP's public key after checking the authentication and integrity of the message as well as the state of customer's account in case of prepaid account. These messages are sent to SP in step 2. In step 3, if SP accepts payment request of MC, he will create a Bill and asks his EMPS EMPS-SP to contact with EMPS-MC. Next, EMPS-SP transfers this Bill along with information about its account to EMPS-MC. EMPS-MC will pay for EMPS-SP through this account. This transaction will depend

on the deal between 2 EMPSs. EMPS-MC charges MC through her phone bill and notifies MC of payment completion in step 5.

*Macro Payment Protocol*: In contrast to micro payment which is charged through phone bill, macro payment is paid by bank account or card. Therefore, this protocol will require some information involving in customer account or card. Some assumptions are made for this case. First, MC shares information about account or his card (AI) with the FI/B which issues the card or account of MC. The second assumption is that MC is also given a PIN shared between MC and FI/B only. When MC registers with EMPS-MC for macro payment service, she must supply information about her FI/B. The macro payment protocol is very similar to the micro payment protocol and the difference between them is slim. The first difference lies in the information sent to EMPS-MC in step 1. Besides the information like in step 1 in micro payment protocol, MC also sends $z_{map}$, a HOAC used to show FI/B that the request for payment is from MC. The other differences are found in the internal processes of EMPS-MC at step 2' and 5'. Prior to transferring the request for payment of MC to SP, EMPS-MC will examine the financial situation of MC by sending the OIResponse and $z_{map}$ to FI/B (step 2'.1). FI/B of EMPS-MC will contact with the FI/B of customer to get information. This process happens under the banking private network. The result will be returned to EMPS-MC in step 2'.2. If the result is positive, EMPS-MC will proceed to the remaining steps like in micro payment. The last difference is in step 5'. EMPS-MC requires its FI/B to link to FI/B of MC to conduct the transaction. The result is returned to EMPS-MC in step 5'.2. The final step of this protocol is the same as step 5 in micro payment protocol.

**1. MC → EMPS-MC: $f_{map}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $ID_{emps\text{-}sp}$, $dl_{map}$, $ts_{mc}$, $d_{mc\text{-}map}$, $EK_{mc,sp}$(OIResponse), $y_{map}$, $x_{map}$, $z_{map}$**
$y_{map}$ = h(OIResponse, l, $dl_{mip}$, $k_{mc,\ sp}$, $d_{mc\text{-}map}$, h($k_{mc,\ emps\text{-}mc}$)) is a HOAC indicating to SP that the original of the request for payment is from MC.
$z_{map}$ = h(OIResponse, AI, $dl_{map}$, PIN) is a HOAC indicating to FI/B that the original of the request for payment is from MC.
$x_{map}$= h(OIResponse, $ts_{mc}$, $k_{mc,emps\text{-}mc}$, $y_{map}$, $z_{map}$) is a HMAC showing EMPS-MC that the HOAC $y_{map}$ and $z_{map}$ are from MC.

**2'. Inside EMPS-MC**
**2'.1. EMPS-MC → FI/B: $f_{map}$, $ID_{mc}$, OIResponse, $z_{map}$, $dl_{map}$, $d_{mc\text{-}map}$, $s_{emps\text{-}mc}$(OIResponse, $z_{map}$, $dl_{map}$, $d_{mc\text{-}map}$)**
**2'.2. FI/B → EMPS-MC: $f_{map}$, $ID_{mc}$, OIResponse, Result, $s_{fi/b}$(OIResponse, $z_{map}$, Result)**
Result = Yes/No

**2. EMPS-MC → SP: $f_{map}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $dl_{map}$, $ts_{emps\text{-}mc}$, $d_{mc\text{-}map}$, $E_{sp}$(OIResponse), $y_{map}$, $x_{map}$, $signmap_{emps\text{-}mc}$**
$signmap_{emps\text{-}mc}$ = $s_{emps\text{-}mc}$($f_{map}$, l, $dl_{map}$, $ts_{emps\text{-}mc}$, $d_{mc\text{-}map}$, OIResponse, $y_{map}$, $x_{map}$)

**3. SP → EMPS-SP: $f_{map}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $ID_{emps\text{-}sp}$, $d_{mc\text{-}map}$, $E_{emps\text{-}sp}$ (Bill), $s_{sp}$($f_{map}$, l, Bill, $d_{mc\text{-}map}$)**
Bill = OIResponse, Approval

**4. EMPS-SP → EMPS-MC: $f_{map}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $ID_{emps\text{-}sp}$, $E_{emps\text{-}mc}$ (Bill, $Account_{emps\text{-}sp}$), $s_{emps\text{-}sp}$($f_{map}$, l, Bill, $Account_{emps\text{-}sp}$)**

**5'. Inside EMPS-MC**
**5'.1. EMPS-MC → FI/B: $f_{map}$, $ID_{mc}$, OIResponse, $dl_{map}$, $E_{fi/b}$ (Bill, $Account_{emps\text{-}sp}$), $s_{emps\text{-}mc}$ ($f_{map}$, Bill, $Account_{emps\text{-}sp}$)**
**5'.2. FI/B → EMPS-MC: $f_{map}$, $ID_{mc}$, OIResponse, $dl_{map}$, Result, $s_{fi/b}$($f_{map}$, Bill, Result)**
Result = Yes/No

**5. EMPS-MC → MC: $f_{map}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $ID_{emps\text{-}sp}$, $Ek_{mc,\ emps\text{-}mc}$(Bill, Result), $s_{emps\text{-}mc}$($f_{map}$, l, Bill, Result)**

***Content Delivery Protocol***

This protocol is based on the assumption that the content delivered is the electronic goods, for example software, music, films, financial report, and can be considered as a message m in general. If the content is physical goods, we can use the traditional delivery method such as transportation companies and there is no concern of the repudiation problem. The protocol is divided into three sub-protocols, a main, a recovery and an abort protocol. In case of problems, the abort or recovery protocol can be involved.

**1. SP → MC: $f_{cd}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $ID_{emps\text{-}sp}$, c, $E_{emps\text{-}sp}$ ($Ek_{mc,\ sp}$ (k)), $EOO_c$**
$EOO_c$ = $s_{sp}$ ($f_{cd}$, l, c, $E_{emps\text{-}sp}$ ($Ek_{mc,\ sp}$ (k)))

**2. MC → EMPS-MC: $f_{cd}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $ID_{emps\text{-}sp}$, $dl_{cd}$, $ts_{mc}$, $d_{mc\text{-}cd}$, h(c), h($E_{emps\text{-}sp}$ ($Ek_{mc,\ sp}$ (k))), $y_{cd}$, $x_{cd}$**
$y_{cd}$ = h($dl_{cd}$, h(c), h(EK), $dl_{cd}$, $d_{mc\text{-}cd}$, $k_{mc,sp}$, h($k_{mc,emps\text{-}mc}$)) is a HOAC indicating to SP that the response for cipher c is from MC.
$x_{cd}$ = h($f_{cd}$, l, $ts_{mc}$, h(c), h(EK), $k_{mc,emps\text{-}mc}$, $y_{cd}$) is a HMAC indicating to EMPS-MC that the HOAC $y_{cd}$ is from MC.

**3. EMPS-MC → SP: $f_{cd}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $ID_{emps\text{-}sp}$, $dl_{dc}$, $ts_{emps\text{-}mc}$, $d_{mc\text{-}cd}$, h(c), h($E_{emps\text{-}sp}$ ($Ek_{mc,\ sp}$ (k))), $y_{cd}$, $x_{cd}$, $signcd_{emps\text{-}mc}$**
$signcd_{emps\text{-}mc}$ = $s_{emps\text{-}mc}$($f_{cd}$, l, $dl_{dc}$, $ts_{emps\text{-}mc}$, $d_{mc\text{-}cd}$, h(c), h($E_{emps\text{-}sp}$ ($Ek_{mc,\ sp}$ (k))), $y_{cd}$, $x_{cd}$)
**If SP times out then abort**

**4. SP → MC: $f_{cd}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps\text{-}mc}$, $ID_{emps\text{-}sp}$, $Ek_{mc,\ sp}$ (k), $s_{sp}$ ($f_{cd}$, l, k)**
**If MC times out then recovery**

*Main Protocol:* SP sends the cipher of message and the evidence of origin for cipher $EOO_c$ to MC in step 1 and waits for the non-repudiation of receipt evidence NRR. If MC carries out the step 2, the step 3 must be executed because EMPS-MC is a trust party of MC. So we can consider step2

and step 3 as two small steps in a unique step 2-3. After receiving NRR in step 3, SP will give the decryption key k to MC.

*Abort Protocol:* If SP doesn't receive the third message of the main protocol, SP initiates the abort protocol by sending to EMPS-SP an Abort request.

**1. SP → EMPS-SP: $f_{abort}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, Abort**
***Aborted = true***
**2. SP → MC: $f_{abort}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, Abort**

*Recovery Protocol*: MC executes the recovery protocol if she does not receive the message in step 4 of the main protocol. MC asks EMPS-MC to transfer its recovery request to EMPS-SP. EMPS-SP recovers the decryption k and sends it along with evidence back to MC through EMPS-MC.

**1. MC → EMPS-MC: $f_{rec}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $dl_{cd}$, $ts_{mc}$, $d_{mc-cd}$, $E_{emps-sp}$ ($Ek_{mc,\ sp}$ (k)), h(c), $y_{cd}$, $x_{cd}$**
***If aborted or recovered then stop, Else recovered = true***

**2. EMPS-MC → EMPS-SP: $f_{rec}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $E_{emps-sp}$($Ek_{mc,\ sp}$ (k)), $s_{emps-mc}$ ($f_{rec}$, l, $E_{emps-sp}$ ($Ek_{mc,\ sp}$ (k)))**
***If aborted or recovered then stop, Else recovered = true***

**3. EMPS-SP → EMPS-MC: $f_{rec}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $E_{emps-mc}$($Ek_{mc,\ sp}$ (k)), $s_{emps-sp}$ ($f_{rec}$, l, $Ek_{mc,\ sp}$ (k))**

**4. EMPS-SP → SP: $f_{rec}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $s_{emps-sp}$ ($f_{rec}$, l, $Ek_{mc,\ sp}$ (k))**

**5. EMPS-MC → MC: $f_{rec}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $Ek_{mc,emps-mc}$($Ek_{mc,\ sp}$ (k)), $s_{emps-mc}$ ($f_{rec}$, l, $Ek_{mc,\ sp}$ (k))**

### C. Non-Repudiation Analysis

***Non-Repudiation Analysis of Price Negotiation Protocol***

*Non-repudiability:* The non-repudiation of origin and receipt evidences for $OI_{mc}$ are $NRO_{pn}$ = $signpn_{emps-mc}$ = $s_{emps-mc}$ ($f_{pn}$, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $dl_{pn}$, $d_{mc-pn}$, $ts_{emps-mc}$, $Ek_{mc,sp}(OI_{mc})$, $y_{pn}$, $x_{pn}$) and $NRR_{pn}$ = $s_{sp}$(OIResponse, $pk_{sp}$, l). If MC denies having sent $OI_{mc}$, SP has to present to the judge $f_{pn}$, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $dl_{pn}$, $d_{mc-pn}$, $ts_{emps-mc}$, $OI_{mc}$, $y_{pn}$, $x_{pn}$, $k_{mc,sp}$, $NRO_{pn}$. The judge verifies that $Ek_{mc,sp}(OI_{mc})$ is the cipher of $OI_{mc}$ under the session key $k_{mc,sp}$, $NRO_{pn}$ is the signature of EMPS-SC on ($f_{pn}$, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $dl_{pn}$, $d_{mc-pn}$, $ts_{emps-mc}$, $Ek_{mc,sp}(OI_{mc})$, $y_{pn}$, $x_{pn}$). As HOAC $y_{pn}$ contains $k_{mc,sp}$, it can be created by only MC and SP. Similarly, HMAC $x_{pn}$ must be generated by only MC and EMPS-MC because of $k_{mc,emps-mc}$. Therefore, it must be MC who produces both of HOAC $y_{pn}$ and HMAC $x_{pn}$. If SP can present all of the items and all the check hold, the adjudicator concludes that MC is at the origin of $OI_{mc}$. If SP denies receipt of $OI_{mc}$ and offered prices of products in $OI_{mc}$, MC gives the judge $NRR_{pn}$, $Ek_{mc,sp}$($OI_{mc}$, OIResponse, $pk_{sp}$, l), OIResponse, l, $OI_{mc}$, $pk_{sp}$. The judge checks that $Ek_{mc,sp}$($OI_{mc}$, OIResponse, $pk_{sp}$, l) is the cipher of ($OI_{mc}$, OIResponse, $pk_{sp}$, l) under the session key $k_{mc,sp}$ and $NRR_{pn}$ is the signature of SP on ($OI_{mc}$, OIResponse, $pk_{sp}$, l). If all checks are valid, the adjudicator claims that SP received the $OI_{mc}$ and replied with OIResponse.

*Fairness:* If SP does not send message in step 3, the protocol will not be strong fairness. However, if step 3 is not executed, SP will lose its customer and gain nothing from that. In other words, SP would harm himself. Consequently, he should carry out step 3 and that means the strong fairness feature of the protocol can be achieved.

***Non-Repudiation Analysis of Payment Protocol***

*Non-repudiability:* Non-repudiation evidences of micro payment protocol are $NRO_{mip}$ = $signmip_{emps-mc}$ = $s_{emps-mc}$ ($f_{mip}$, l, $dl_{mip}$, $ts_{emps-mc}$, $d_{mc-mip}$, OIResponse, $y_{mip,}$ $x_{mip}$) and $NRR_{mip}$ = $s_{emps-mc}$ ($f_{mip}$, l, Bill). In case of non-repudiation of origin, SP has to present to a judge $NRO_{mip}$, $f_{mip}$, l, $dl_{mip}$, $ts_{emps-mc}$, $d_{mc-mip}$, OIResponse, $y_{mip,}$ $x_{mip}$, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, h(OIResponse), $h(k_{mc,\ emps-mc})$. The judge verifies that l = h($ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, h(OIResponse), $h(k_{mc,\ emps-mc})$), and $NRO_{mip}$ is the signature of EMPS-MC on ($f_{mip}$, l, $dl_{mip}$, $ts_{emps-mc}$, $d_{mc-mip}$, OIResponse, $y_{mip,}$ $x_{mip}$). If all the checks hold, the adjudicator concludes that MC is the originator of payment request. On the other hand, MC can prove that SP has received her payment by presenting $NRR_{mip}$, $f_{mip}$, l, $ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, $d_{mc-mip}$, h(OIResponse), $h(k_{mc,\ emps-mc})$, Bill to the judge. EMPS-MC provides $s_{emps-sp}$ ($f_{mip}$, l, Bill, $Account_{emps-sp}$) and EMPS-SP provides $s_{sp}$($f_{mip}$, l, Bill, $d_{mc-mip}$), $Account_{emps-sp}$. The arbitrator checks that l = h($ID_{mc}$, $ID_{sp}$, $ID_{emps-mc}$, $ID_{emps-sp}$, h(OIResponse), $h(k_{mc,\ emps-mc})$), $s_{sp}$($f_{mip}$, l, Bill, $d_{mc-mip}$) is the signature of SP on ($f_{mip}$, l, Bill, $d_{mc-mip}$), $s_{emps-sp}$($f_{mip}$, l, Bill, $Account_{emps-sp}$) is the signature of EMPS-SP on ($f_{mip}$, l, Bill, $Account_{emps-sp}$) and $NRR_{mip}$ is the signature of EMPS-MC on ($f_{mip}$, l, Bill). If all verifications are valid, MC wins. We can have similar verifications in macro payment protocol with $NRO_{map}$ = $signmap_{emps-mc}$ = $s_{emps-mc}$($f_{map}$, l, $dl_{map}$, $ts_{emps-mc}$, $d_{mc-map}$, OIResponse, $y_{map,}$ $x_{map}$) and $NRR_{map}$ = $s_{emps-mc}$($f_{map}$, l, Bill, Result).

*Fairness:* These two payment protocols are strong fairness because the transaction are intervened by the trust parties of both MC and SP. EMPS-MC represents MC, EMPS-SP represents SP and the payment actually happens among these EMPSs which trust each other.

***Non-repudiation Analysis of Content Delivery Protocol***

*Non-repudiability:* If the recovery protocol is not invoked, $NRO_{cd}$ = $s_{sp}$ ($f_{cd}$, l, c, $E_{emps-sp}$ ($Ek_{mc,\ sp}$ (k))), $s_{sp}$ ($f_{cd}$, l, k) and $NRR_{cd}$ = $signcd_{emps-mc}$ = $s_{emps-mc}$($f_{cd}$, l, $dl_{dc}$, $ts_{emps-mc}$, $d_{mc-cd}$, h(c), h($E_{emps-sp}$ ($Ek_{mc,\ sp}$ (k))), $y_{cd}$ , $x_{cd}$). On the contrary, $NRO_{cd}$ = $s_{sp}$ ($f_{cd}$, l, c, $E_{emps-sp}$ ($Ek_{mc,\ sp}$ (k))), $s_{emps-mc}$ ($f_{rec}$, l, $Ek_{mc,\ sp}$ (k)) and $NRR_{cd}$ = $s_{emps-mc}$($f_{cd}$, l, $dl_{dc}$, $ts_{emps-mc}$, $d_{mc-cd}$, h(c), h($E_{emps-sp}$ ($Ek_{mc,\ sp}$ (k))), $y_{cd}$ , $x_{cd}$), $s_{emps-sp}$ ($f_{rec}$, l, $Ek_{mc,\ sp}$ (k)). The checking process is similar to the above verifications.

*Fairness:* The protocol is strong fairness. If the step 2-3 of main protocol is not executed, SP can invoke the abort protocol and no party can obtain correct evidence anymore. If MC launches a recovery protocol, both MC and SP will receive all expected evidences, and hence the protocol remains fair.

*Timeliness:* Timeliness is provided by the fact that at each moment in the protocol, both MC and SP can stop the protocol while preserving fairness.

## V. Conclusions and Future Work

In this paper we have identified the most common requirements and properties of concern for dealing with non-repudiation problem in m-commerce. Then, we have introduced an extension of mobile payment model named EMPS for solving the above problem. Based on the EMPS, three non-repudiation protocols for *all fundamental phases* (price negotiation, mobile payment, content delivery) in m-commerce transactions have been built. To the best of our knowledge, this holistic approach to the non-repudiation problem in m-commerce is among the vanguard solutions to address it. Analyses of the non-repudiability, fairness and timeliness of the proposed protocols are also carried out. They are the solid basis for our further improvements in the future.

In the future, we plan to standardize communications among parties in EMPS model, especially between MNO and FI/B and among EMPSs. Web service standard is one of our targets for this purpose. Additional formal analyses along with improvements to achieve the timeliness of the proposed non-repudiation protocols will be of our great interest. Moreover, generating long-term key from session key, combining the initiation process with price negotiation process, etc. are also of our concerns. We also intend to perform empirical evaluations on the proposed protocols' performance to establish their practical value.

## Acknowledgment

We would like to thank all members of ASIS Lab at CSE/HCMUT for their enthusiastic supports during carrying out this research.

## References

[1] L. He and N. Zhang, "A New Signature Scheme: Joint Signature," in *ACM Symposium on Applied Computing*, 2004, pp. 807 – 812.

[2] J. Liu, J. Liao, and X. Zhu, "A System Model and Protocol for Mobile Payment," in *Proc. of IEEE International Conference on e-Business Engineering*, 2005, pp. 638 – 641.

[3] R. K. Tiwari, "Fair Non Repudiation in Mobile Communication using Joint Signatures," in *Proc. of IEEE International Conference on Personal Wireless Communication*, 2005, pp. 438 – 440.

[4] L. He and N. Zhang, "An asymmetric authentication protocol for M-Commerce applications," in *Proc. of IEEE International Symposium on Computers and Communication*, Vol. 1, 2003, pp. 244 – 250.

[5] C. Chen, H. Lin, Y. Chen, and J. Jan, "A Fair Transaction Model in Mobile Commerce," in *Proc. of IEEE International Symposium on Signal Processing and Information Technology*, 2006.

[6] S. Kremer, O. Markowitch, and J. Zhou, "An Intensive Survey of Non-repudiation Protocols," *Computer Communications*, pp. 1606 – 1621, 2002.

[7] Jianying Zhou, "Non-repudiation in Electronic Commerce," Artech House Computer Security Series, 2001.

[8] S. Kungpisdan, B. Srinivasan, and P. D. Le, "A Secure Account-Based Mobile Payment Protocol," in *Proc. of International Conference on Information Technology: Coding and Computing*, 2004, pp. 35 – 39.

[9] A. Vilmos and S. Karnouskos, "SEMOPS: Design of a New Payment Service," in *Proc. of International Workshop on Database and Expert Systems Applications*, 2003, pp. 865 – 869.

[10] S. Nambiar and C.T. Lu, "M-Payment Solutions and M-Commerce Fraud Management," as Chapter IX of Book: Advances in Security and Payment Methods for Mobile Commerce, pp. 192 – 213, Idea Group Inc., 2005.

[11] C. Lee, W. Hu, and J. Yeh, "A System Model for Mobile Commerce", in *Proc. of International Conference on Distributed Computing Systems Workshops*, 2003, pp. 634 – 639.

[12] ISO/IEC 10181-4. Information Technology – Open Systems Interconnection – Security Frameworks in Open System – Part 4: Non-repudiation Framework, ISO/IEC, 1996.

[13] S. Nambiar, C.T. Lu, and L.R. Liang, "Analysis of Payment Transaction Security in Mobile Commerce," in *Proc. of IEEE International Conference on Information Reuse and Integration*, 2004, pp. 475 – 480.