AN EXTENDED PAYMENT MODEL WITH FAIR NON-REPUDIATION PROTOCOLS FOR M-COMMERCE

Thi Thanh Huyen Phan¹), Tran Khanh Dang²)

Abstract
This paper proposes an extended mobile payment service model founded on the existing ones to solve the non-repudiation problems with fair non-repudiation protocols for all phases in a typical m-commerce transaction. The novel model bases on assumptions about the cooperation between mobile network operators and financial institutions to deal with different payment amounts ranging from micro to macro payments. Joint signatures are employed to overcome the limitations of mobile handheld devices and to reduce the trust dependence totally on the payment service.

1. Introduction

Non-repudiation with the ability to resolve disputes about the occurrence or non-occurrence of an event or action has proved its importance to the commercial transactions in e-/m-commerce. Although this issue in e-commerce has built a relatively sound foundation, non-repudiation in m-commerce is still at a start and mainly discussed in mobile payment context. SEMOPS [6] is a prettily perfect example of universal models but without any formal non-repudiation protocols. Most mobile payment models mentioning non-repudiation do not give a complete analysis of non-repudiation properties. Some skip the differences in nature of different payment methods and payment values and the limited capability of mobile handheld devices [2] while others are just suitable for some specific cases, like small payment through phone bill [1, 3].

This paper presents an extended mobile payment model, EMPS model, founded on the existing ones to solve the non-repudiation problem in not only the payment phase but also others of a general commercial transaction, namely price negotiation and content delivery. By using joint signatures, payment service provider is considered as a semi-trusted third party and the load on

¹,² Faculty of Computer Science & Engineering, HCMC University of Technology, National University of Ho Chi Minh City, Vietnam, E-mail: {huyentip, dtkhanh}@cse.hcmut.edu.vn
mobile devices is reduced as well. Our solution also addresses a variety of payment methods like credit card/account based methods, phone bill charging method and payment amounts like macro/micro payments. The rest of this paper is organized as follows. Section 2 presents some non-repudiation considerations in an m-commerce transaction. Next, we introduce our EMPS model with non-repudiation protocols of a general mobile transaction and some theoretical analyses of their characteristics. Some discussions are carried out in section 4. Finally, section 5 gives concluding remarks and presents future work.

2. M-Commerce Non-Repudiation Considerations

An m-commerce transaction usually involves three phases: price negotiation, payment and content delivery. The non-repudiation goals of the first phase are that the parties can not falsely deny having agreed on the given price. Next, mobile customer (MC) can not falsely deny having agreed to pay her bill and service provider (SP) can not falsely deny having received the payment for the invoice of MC. In the third phase, MC can not falsely deny having received goods and SP can not falsely deny having not delivered the goods. Non-repudiation protocols in m-commerce should be based on existing ones in e-commerce [4] and adjusted to suit the resource constraints of mobile devices and specific requirements of different transactions. Evidence generation cost can be reduced by using symmetric key or digital signature. In the first technique, two symmetric keys can be used in combination with other techniques such as hash, keyed hash, MAC [5]. In the other, we need to design more efficient mathematical algorithms or employ a third party to sign message on the original signer’s behalf [1]. A semi-trusted third party assisting in fair exchange of the message and/or non-repudiation evidence should be employed from the main players in m-commerce such as mobile network operator (MNO), financial institution/bank (FI/B) or independent agent.

3. EMPS System Model with Fair Non-Repudiation Protocols

3.1. EMPS System Model

EMPS stands for Extended Mobile Payment Service which represents the system’s innovation in taking full advantage of mobile payment model to build fair non-repudiation protocols for not only the payment phase but also the price negotiation and content delivery phases to obtain a fair non-repudiation m-commerce transaction. EMPS system model is shown in figure 1 with four main parties: 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. The model is based on [2, 6] with
many improvements. The data center is removed because it increases the complexity of the non-repudiation protocol with many steps, third parties and the trust level to third parties. EMPS model makes assumption about the cooperation between MNO and FI/B to process different payment amounts ranging from micro to macro payments. While FI/B deals with macro payment module, MNO is responsible for micro payment module and supports MC in generating joint signature (signing module). Joint signature idea is applied in the system to reduce both computational load on mobile user and the trust dependence totally on the payment service EMPS.

4.2. Fair Non-Repudiation Protocols of M-Commerce Transactions in EMPS

It is supposed that the communication channels among EMPS, between EMPS and both SP/MC are resilient. The communication channels between MC and SP may be unreliable. The notations used in our protocols are briefly explained in Table 1. Details of joint signatures can be found in [1, 3].

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>h(m)</td>
<td>collision resistant hash function</td>
</tr>
<tr>
<td>m&lt;sub&gt;1&lt;/sub&gt;, m&lt;sub&gt;2&lt;/sub&gt;</td>
<td>concatenation of data item m&lt;sub&gt;1&lt;/sub&gt; and m&lt;sub&gt;2&lt;/sub&gt;</td>
</tr>
<tr>
<td>k&lt;sub&gt;A,B&lt;/sub&gt;</td>
<td>session key shared between A and B</td>
</tr>
<tr>
<td>ID&lt;sub&gt;A&lt;/sub&gt;</td>
<td>identity of entity A</td>
</tr>
<tr>
<td>pk&lt;sub&gt;A&lt;/sub&gt;</td>
<td>(e&lt;sub&gt;A&lt;/sub&gt;, n&lt;sub&gt;A&lt;/sub&gt;) public key of entity A</td>
</tr>
<tr>
<td>sk&lt;sub&gt;A&lt;/sub&gt;</td>
<td>(d&lt;sub&gt;A&lt;/sub&gt;, n&lt;sub&gt;A&lt;/sub&gt;) private key of entity A</td>
</tr>
<tr>
<td>s&lt;sub&gt;A&lt;/sub&gt; = (h(m))&lt;sup&gt;d(A)&lt;/sup&gt; mod n&lt;sub&gt;A&lt;/sub&gt;</td>
<td>entity A signature over message m</td>
</tr>
<tr>
<td>Ek</td>
<td>a symmetric key encryption function under key k</td>
</tr>
<tr>
<td>c = Ek(m)</td>
<td>cipher of message m under the key k</td>
</tr>
<tr>
<td>E&lt;sub&gt;A&lt;/sub&gt;</td>
<td>a public key encryption function under A’s public key</td>
</tr>
<tr>
<td>cert&lt;sub&gt;A&lt;/sub&gt;</td>
<td>a digital Certificate of entity A</td>
</tr>
<tr>
<td>l</td>
<td>a label uniquely identifies a protocol run</td>
</tr>
<tr>
<td>f</td>
<td>a flag indicating the purpose of a message</td>
</tr>
<tr>
<td>y = HOAC</td>
<td>Hash Origin Authentication Code</td>
</tr>
<tr>
<td>x = HMAC</td>
<td>Hash Message Authentication Code</td>
</tr>
<tr>
<td>d&lt;sub&gt;A,P&lt;/sub&gt;</td>
<td>a deadline for response which is imposed by A in protocol P</td>
</tr>
<tr>
<td>dl = [t&lt;sub&gt;s&lt;/sub&gt;, t&lt;sub&gt;e&lt;/sub&gt;]</td>
<td>a time interval</td>
</tr>
<tr>
<td>OI&lt;sub&gt;A&lt;/sub&gt; = P&lt;sub&gt;A&lt;/sub&gt;, PID, N</td>
<td>Order Information constructed by A</td>
</tr>
<tr>
<td>P&lt;sub&gt;A&lt;/sub&gt;</td>
<td>Price suggested by entity A</td>
</tr>
<tr>
<td>PID</td>
<td>Identity of Product which MC intends to buy</td>
</tr>
<tr>
<td>N</td>
<td>Quantity of a Product which MC intends to buy</td>
</tr>
<tr>
<td>Account&lt;sub&gt;A&lt;/sub&gt;</td>
<td>Information about account of entity A</td>
</tr>
<tr>
<td>SC</td>
<td>Shipping cost</td>
</tr>
</tbody>
</table>

Table 1. Notations

4.2.1. Price Negotiation Phase

If MC accepts the OIResponse of SP, the payment phase will be conducted. On the contrary, this phase will be repeated until one agrees with the prices given by the other or decides to give up.

Protocol:

1. MC → EMPS-MC: f<sub>pn</sub>, ID<sub>mc</sub>, ID<sub>sp</sub>, ID<sub>ems-p-mc</sub>, d<sub>mc-pn</sub>, dl, l<sub>mc</sub>, Ek<sub>mc</sub>, sp (OI<sub>mc</sub>), y<sub>pn</sub>, x<sub>pn</sub>

\[
y_{pn} = h(OI_{mc}, dl, k_{mc,sp}, d_{mc-pn}, h(k_{mc,ems-mc})) \text{ and } x_{pn} = h(Ek_{mc,sp}(OI_{mc}), f_{pn}, ID_{mc}, ID_{sp}, ID_{ems-mc}, l_{mc}, k_{mc,ems-mc}, y_{pn}).
\]
2. EMPS-MC $\rightarrow$ 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 $signpn_{emps-mc} = signpn_{emps-mc}(f_{pn}, ID_{mc}, ID_{sp}, ID_{emps-mc}, dl_{pn}, d_{mc-pn}, ts_{emps-mc}, Ek_{mc, sp}(OI_{mc}), y_{pn}, x_{pn})$.

3. SP $\rightarrow$ MC: $f_{pn}, ID_{mc}, ID_{sp}, ID_{emps-mc}, ID_{emps-sp}, d_{sp-pn}, Ek_{mc,sp}(OI_{mc}, OIResponse, pk_{sp}, l), s_{sp}(OI_{mc}, OIResponse, pk_{sp}, l)$

$OI_{Response} = OI_{sp}, SC, d_{sp-pn}$ and $l = h(ID_{mc}, ID_{sp}, ID_{emps-mc}, ID_{emps-sp}, h(OI_{Response}), h(k_{mc, emps-mc}))$

Analysis:

− Non-repudiability: $NRO_{pn} = signpn_{emps-mc}$ and $NRR_{pn} = s_{sp}(OI_{Response}, pk_{sp}, l)$.

− Fairness: If SP does not send message in step 3, he will lose his customer and gain nothing from that. Consequently, he should carry out step 3 and the strong fairness feature can be achieved.

− Timeliness: By making use of deadline $d_{mc-pn}$ and $d_{sp-pn}$, MC and SP will be able to decide, within a finite amount of time, whether the protocol is ended.

4.2.2. Payment Phase

In contrast to micro payment which is charged through phone bill, macro payment is paid by bank account or card. Therefore, macro payment protocol will require some extra information involving in a PIN and information about her account/card (AI) shared with her FI/B.

Micro Payment Protocol:

1. MC $\rightarrow$ EMPS-MC: $f_{mip}, l, ID_{mc}, ID_{sp}, ID_{emps-mc}, ID_{emps-sp}, dl_{mip}, ts_{mc}, d_{mc-mip}, Ek_{mc, emps-mc}(OI_{Response}), y_{mip}, x_{mip}$

$y_{mip} = h(OI_{Response}, l, dl_{mip}, ts_{mc}, d_{mc-mip}, h(k_{mc, emps-mc}))$, $x_{mip} = h(OI_{Response}, f_{mip}, ts_{mc}, d_{mc-mip}, y_{mip})$

2. EMPS-MC $\rightarrow$ SP: $f_{mip}, l, ID_{mc}, ID_{sp}, ID_{emps-mc}, ID_{emps-sp}, dl_{mip}, ts_{emps-mc}, d_{mc-mip}, Ek_{sp}(OI_{Response}), y_{mip}, x_{mip}, signmip_{emps-mc}$

The joint signature $signmip_{emps-mc} = signmip_{emps-mc}(f_{mip}, l, dl_{mip}, ts_{emps-mc}, d_{mc-mip}, OI_{Response}, y_{mip}, x_{mip})$.

3. SP $\rightarrow$ EMPS-SP: $f_{mip}, l, ID_{mc}, ID_{sp}, ID_{emps-mc}, ID_{emps-sp}, dl_{mip}, ts_{mip}, d_{mc-mip}, E_{emps-sp}(Bill), s_{sp}(f_{mip}, l, Bill, d_{mc-mip})$

$Bill = OI_{Response}, Approval$

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

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

Macro Payment Protocol:

1. MC $\rightarrow$ EMPS-MC: $f_{map}, l, ID_{mc}, ID_{sp}, ID_{emps-mc}, ID_{emps-sp}, dl_{map}, ts_{mc}, d_{mc-map}, Ek_{mc,emps-mc}(OI_{Response}), y_{map}, x_{map}$

$y_{map} = h(OI_{Response}, l, dl_{map}, ts_{mc}, d_{mc-map}, h(k_{mc, emps-mc}))$, $x_{map} = h(OI_{Response}, AI, dl_{map}, PIN)$ is a HOAC.

2’. Inside EMPS-MC

2’.1. EMPS-MC $\rightarrow$ FI/B: $f_{map}, l, ID_{mc}, OI_{Response}, z_{map}, dl_{map}, s_{emps-mc}(OI_{Response}, z_{map}, dl_{map}, d_{mc-map})$

2’.2. FI/B $\rightarrow$ EMPS-MC: $f_{map}, l, ID_{mc}, OI_{Response}, Result, s_{fi/b}(OI_{Response}, z_{map}, Result)$

Result = Yes/No

3. EMPS-MC $\rightarrow$ SP: $f_{map}, l, ID_{mc}, ID_{sp}, ID_{emps-mc}, ID_{emps-sp}, dl_{map}, ts_{emps-mc}, d_{mc-map}, Ek_{sp}(OI_{Response}), y_{map}, x_{map}, signmap_{emps-mc}$

$signmap_{emps-mc} = signmap_{emps-mc}(f_{map}, l, dl_{map}, ts_{emps-mc}, d_{mc-map}, OI_{Response}, y_{map}, x_{map})$

3. SP $\rightarrow$ EMPS-SP: $f_{map}, l, ID_{mc}, ID_{sp}, ID_{emps-mc}, ID_{emps-sp}, dl_{map}, E_{emps-sp}(Bill), s_{sp}(f_{map}, l, Bill, d_{mc-map})$

$Bill = OI_{Response}, Approval$

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

5’. Inside EMPS-MC

5’.1. EMPS-MC $\rightarrow$ FI/B: $f_{map}, l, ID_{mc}, OI_{Response}, dl_{map}, F_{fb}(Bill, Account_{emps-sp}), s_{emps-mc}(f_{map}, Bill, Account_{emps-sp})$
5.2. FI/B → EMPS-MC: fmap, IDmc, OIResponse, dlmap, Result, s\_gb(fmap, Bill, Result)
5. EMPS-MC → MC: fmap, l, IDmc, IDsp, IDemps-mc, IDemps-sp, Ek\_mc, emps-mc(Bill, Result), s\_emps-mc(fmap, l, Bill, Result)

### Analysis:

- **Non-repudiability:**
  
  \[
  NRO_{\text{mip}} = \text{signmip}_{\text{emps-mc}} \text{ and } NRR_{\text{mip}} = s_{\text{emps-mc}}(f_{\text{mip}}, l, \text{Bill}) ; NRO_{\text{map}} = \text{signmap}_{\text{emps-mc}} \text{ and } NRR_{\text{map}} = s_{\text{emps-mc}}(f_{\text{map}}, l, \text{Bill, Result}) .
  \]

- **Fairness:** Strong fairness is achieved because the transaction is intervened by the trusted EMPSs of MC and SP, EMPS-MC and EMPS-SP, which trust each other.

- **Timeliness:** By making use of deadline d\_A\_P, MC and SP will be able to decide, within a finite amount of time, whether the protocol is ended.

### 4.2.3. Content Delivery Protocol

#### Main Protocol:

**Initiated in normal cases.** The abort or recovery protocol will be involved.

1. SP → MC: f\_cd, l, IDmc, IDsp, IDemps-mc, IDemps-sp, c, E\_emps-sp(Ek\_mc, sp(k)), s\_sp(f\_cd, l, k)
2. MC → EMPS-MC: f\_cd, l, IDmc, IDsp, IDemps-mc, IDemps-sp, dl\_cd, ts\_mc, d\_mc-cd, h(c), h(E\_emps-sp(Ek\_mc, sp(k))), y\_cd, x\_cd
   
   \[\begin{align*}
   y_{\text{cd}} &= h(\text{dl}_{\text{cd}}, h(c), h(\text{EK}), \text{dl}_{\text{cd}}, \text{d}_{\text{mc-cd}}, k_{\text{sp}}, h(k_{\text{mc-emps-mc}})), \\
   x_{\text{cd}} &= h(f_{\text{cd}}, l, t_{\text{mc}}, h(c), h(\text{EK}), k_{\text{mc-emps-mc}}, y_{\text{cd}})
   \end{align*}\]
3. EMPS-MC → SP: f\_cd, l, IDmc, IDsp, IDemps-mc, IDemps-sp, dl\_cd, ts\_mc, d\_mc-cd, h(c), h(E\_emps-sp(Ek\_mc, sp(k))), y\_cd, x\_cd
   
   \[\begin{align*}
   s_{\text{emps-mc}}(f_{\text{cd}}, l, d_{\text{mc-cd}}, t_{\text{mc}}, h(c), h(E_{\text{emps-sp}}(E_{\text{mc-emps-sp}}(k))), y_{\text{cd}}, x_{\text{cd}})
   \end{align*}\]

**If SP times out then abort protocol**

4. SP → MC: f\_cd, l, IDmc, IDsp, IDemps-mc, IDemps-sp, Ek\_mc, sp(k), s\_sp(f\_cd, l, k)

**If MC times out then recovery protocol**

#### Abort Protocol:

**Used to cancel the transaction.**

1. SP → EMPS-SP: f\_abort, l, IDmc, IDsp, IDemps-mc, IDemps-sp, Abort
   
   Aborted = true

2. SP → MC: f\_abort, l, IDmc, IDsp, IDemps-mc, IDemps-sp, Abort
   
   Aborted = true

#### Recovery Protocol:

**Invoked to recover non-repudiation evidences.**

1. MC → EMPS-MC: f\_recv, l, IDmc, IDsp, IDemps-mc, IDemps-sp, dl\_cd, ts\_recv, 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\_recv, l, IDmc, IDsp, IDemps-mc, IDemps-sp, E\_emps-sp(Ek\_mc, sp(k)), s\_emps-mc(f\_recv, l, E\_emps-sp(Ek\_mc, sp(k)))
   
   If aborted or recovered then stop, Else recovered = true

3. EMPS-SP → EMPS-MC: f\_recv, l, IDmc, IDsp, IDemps-mc, IDemps-sp, E\_emps-mc(Ek\_mc, sp(k)), s\_emps-mc(f\_recv, l, Ek\_mc, sp(k))
4. EMPS-SP → SP: f\_recv, l, IDmc, IDsp, IDemps-mc, IDemps-sp, s\_emps-mc(f\_recv, l, Ek\_mc, sp(k))

#### Analysis:

- **Non-repudiability:**
  
  \[
  NRO_{\text{cd}} = s_{\text{sp}}(f_{\text{cd}}, l, c, E_{\text{emps-sp}}(E_{\text{mc-sp}}(k))), s_{\text{sp}}(f_{\text{cd}}, l, k) \text{ and } NRR_{\text{cd}} = s_{\text{emps-mc}}(f_{\text{cd}}, l, d_{\text{mc-cd}}, t_{\text{mc}}, h(c), h(E_{\text{emps-sp}}(E_{\text{mc-sp}}(k))), y_{\text{cd}}, x_{\text{cd}}) \text{ or } NRO_{\text{cd}} = s_{\text{sp}}(f_{\text{cd}}, l, c, E_{\text{emps-sp}}(E_{\text{mc-sp}}(k))), s_{\text{emps-mc}}(f_{\text{recv}}, l, E_{\text{mc-sp}}(k)) \text{ and } NRR_{\text{cd}} = s_{\text{emps-mc}}(f_{\text{cd}}, l, d_{\text{mc-cd}}, t_{\text{emps-mc}}, d_{\text{mc-cd}}, h(c), h(E_{\text{emps-sp}}(E_{\text{mc-sp}}(k))), y_{\text{cd}}, x_{\text{cd}}), s_{\text{emps-sp}}(f_{\text{recv}}, l, E_{\text{mc-sp}}(k)).
  \]
- **Fairness**: The protocol is strong fairness via [4].
- **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.

4. Discussions

The strengths of EMPS model lie in the holistic approach by extending original payment models to supply non-repudiation solution for other phases of an m-commerce transaction besides the payment phase. The system security is also increased by considering payment service as a semi-trusted third party. The limitation of mobile devices and different payment values are solved in our model too. However, an improvement for completing the security model and its security proof is essential to make the convincing model and protocols.

5. Conclusion and Future Work

We have introduced an extended mobile payment model founded on our considerations about non-repudiation in m-commerce transactions. On this model, three fair non-repudiation protocols for *all fundamental phases* (price negotiation, mobile payment, content delivery) in m-commerce transactions, along with analyses of their properties, have been built. In the future, we intend to standardize communications among parties in this new model and perform performance evaluations of the proposed protocols.

References


