行政院國家科學委員會專題研究計畫　期中進度報告

第三代後行動網路支援行動付款之研究(1/2)

計畫類別： 個別型計畫
計畫編號： NSC92-2213-E-009-066-
執行期間： 92 年 08 月 01 日至 93 年 07 月 31 日
執行單位： 國立交通大學資訊工程學系

計畫主持人： 張明峰

計畫參與人員： 黃逸聖、李榮泰、陳建彰、李偉晟

報告類型： 精簡報告

處理方式： 本計畫可公開查詢

中華民國 93 年 6 月 1 日

行政院國家科學委員會補助專題研究計畫 □成果報告
■期中進度報告

第三代後行動網路支援行動付款之研究(1/2)

計畫類別：■ 個別型計畫　　□ 整合型計畫
計畫編號：NSC92-2213-E-009-066-
執行期間：2003.08.01 至 2004.07.31

計畫主持人： 張明峰
共同主持人：
計畫參與人員：

成果報告類型(依經費核定清單規定繳交)：■精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位： 交通大學 資訊工程系

中華民國九十三年五月三十一日

行政院國家科學委員會專題研究計畫成果報告

第三代後行動網路支援行動付款之研究(1/2)

The Study of Mobile Payment for B3G Networks

計畫編號：NSC92-2213-E-009-066-

執行期限：2003.08.01 至 2004.07.31

主持人：張明峰　交通大學資工系

計畫參與人員： 黃逸聖、李榮泰、陳建彰、李偉晟 交通大學資工系

中文摘要

歐洲的行動通訊業者提供使用者利用手機購買小額商品。行動通訊業者有廣大的用戶，也有完備的帳務與收費機制，因此業者可利用此一優勢，推動行動手機機成為行動商務服務之付費工具；行動通訊業者可扮演行動商務銀行的角色。在此一國科會資助的兩年的研究計畫，我們探討第三代後行動通訊網路中行動付帳機制中的用戶認證，及異質網路環境中的付帳機制。我們的系統一方面支援加值服務業者經由行動網路業者對客戶執行身份認證，另一方面行動用戶可經由行動網路業者付費給加值服務業者。我們的系統同時支援預付卡用戶及一般用戶。為支援手機行動付帳，我們在行動網路中新增一記帳付帳閘道及 AAA 伺服器，執行下列功能：1. 與行動網路之預付卡及一般用戶帳務系統介接。2. 對用戶及商家進行身份認證，提供用戶臨時代號以支援匿名付帳。3. 與現有電子付帳系統介接，付款給商家。

關鍵詞：行動付帳，預付卡服務，帳務系統，記帳閘道，付帳閘道。

Abstract

In Europe, mobile handset users can purchase a soft drink from vending machines or pay parking fee by dialing a premium-rate number. Mobile network operators have a large subscriber base and a well functioning billing system. These advantages can be leveraged to make mobile handsets as the payment tools in mobile commerce. Network operator can be the banker in mobile commerce; subscribers purchase products from value-added service providers (VASPs) or merchants, and pay monthly bill to the network operator. In this two-year research project, supported by NSC, we investigate mobile payment infrastructure for B3G (Beyond 3G) network. Our mobile payment system enables a subscriber to make payment to a VASP (or merchant) through the network operator and remain anonymous to the VASP. In addition, the VASP can authenticate a customer through the network operator. The customer can be a pre-paid subscriber or post-paid (monthly bill) one. To support this handset-based mobile payment, a charging and payment gateway, and an AAA server are added to the mobile network to perform the following functions: 1. Interwork the mobile payment with the existing, unchanged pre-paid and post-paid billing system. 2. Authenticate the VASP and mobile payment subscribers, and provide temporary identifiers to subscribers for anonymous payment. 3. Interwork with existing electronic payment systems to make payments to VASPs.

Keywords: mobile payment, pre-paid service, billing system, charging gateway, payment gateway

1. Introduction

Mobile communications have grown rapidly in the past ten years. For example, the penetration rate of mobile phones is over 100% in Taiwan, i.e., many people have more than one mobile phone. The total number of mobile phones has outnumbered that of personal computers worldwide. In addition to mobile telephone service, mobile network operators have also been promoting mobile data service, such SMS (Short Message Service) and GPRS (General Packet Radio Service) [5]. Mobile network operators expect mobile data service can be the next big wave. For now, mobile data service is still at the initial stage with limited success. The DoCoMo i-mode service [20] and the number of short messages transmitted worldwide have increased exponentially. The highly promoted mobile service based on WAP (Wireless Access Protocol) does not realize because of the long transmission delay.

Mobile phones have become personal goods that every person owns. In addition to providing telephone communications at any place, anytime, mobile users in Europe can use mobile phones to buy soft drink from a vending machine, and pay parking fee or gasoline charge. Mobile network operators have a large base of subscribers and a well functioning charging and billing system; they hold the upper hand on making mobile phones as the payment tool for mobile commerce. Mobile network operators can be the banks in mobile commerce. From the user's viewpoints, using mobile phones as a mobile payment tool offers the following advantages: ubiquity, security, localization, convenience, and personalization. However, mobile phones also have limitations, such as limited memory capacity and computation power.

Payment for mobile network usage can be classified into two categories: post-paid and prepaid. For a post-paid user, the CDRs (call detail records) generated by the mobile switches for each phone call are used to produce the monthly bills. A CDR contains the information of a phone call, including the calling party, the called party, the date and time, the duration, the types of the call, etc. The CDR of a mobile phone call includes additional information, such as location area, cell ID, radio channel and the IMEI (International Mobile Equipment Identity) [7]. An MSC sends the CDRs in batch, usually during the off-peak hours, to a central CDR database. The billing system retrieves the CDR database, rates each call and generates the monthly bills for the subscribers.

The charging and billing of mobile data network, such as GPRS network, and its value-added services are based one the extensions of current CDR system. Take GPRS for example, the nodes of GPRS core network, SGSN and GGSN, generate mobility management CDR (M-CDR records user location), SGSN CDR (S-CDR records radio channel usage and QoS) and GGSN CDR (G-CDR records the data volume with external IP network) [6]. The CDRs are relayed by the CGF（Charging Gateway Function）to the billing system, as shown in Figure 1. In addition, 3G UMTS define even more types of CDRs to support the charging and billing system [8,9,10,11].

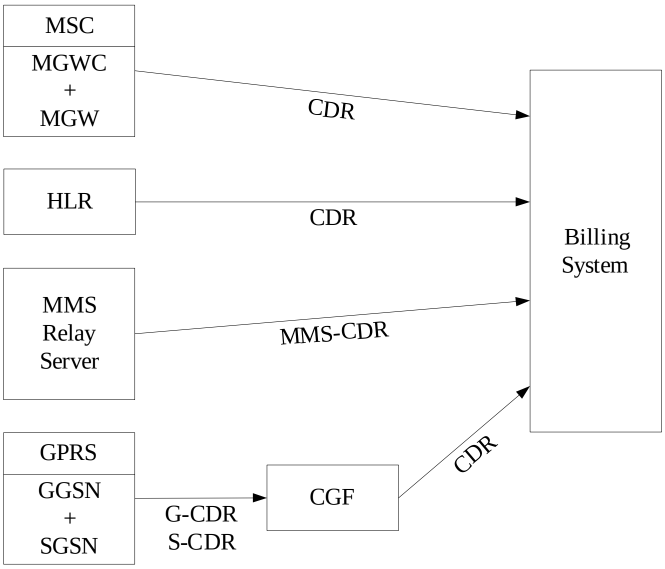

Figure 1: The billing system based on CDRs

There are four approaches to provide mobile prepaid service: hot billing, service node, IN

(Intelligent Network) and handset-based [1,3,17]. The hot billing and the handset-based approaches provide solutions without major changes to the network infrastructure. Intelligent network solution offers real time rating and real time call control, but is not widely deployed today. The service node approach, which utilizes extra voice circuits and switching resources for prepaid calls, provides a variant to the intelligent network solution. real-time billing. The mobile data networks, GPRS and UMTS, extend the IN approach to support prepaid services. The ETSI have defined CAMEL (Customized Application for Mobile Enhanced Logic) phase 3 for service control of short messages and packet data [14]. Figure 2 depicts the CAMEL architecture for the GSM and GPRS prepaid services.

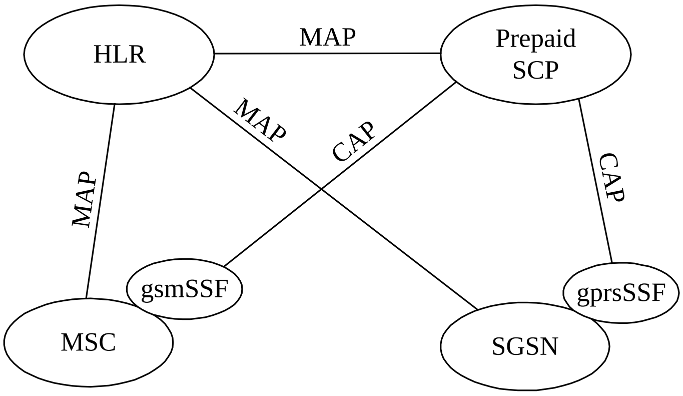

Figure 2: Integrated GSM and GPRS prepaid service based on CAMEL

Mobile payment is an extension of electronic payment; at present, there are more than one hundred of electronic payment schemes [15,16]. Electronic payments can be classified into credit type and debit type payments. The debit type includes electronic cash, electronic check, and bank transfer, etc. Since cash must be deposited in advance, the debit type payments are similar to prepaid accounts in mobile networks. On the other hand, the credit type electronic payments are similar to postpaid accounts; both receive and pay monthly bills.

Important issues that must be considered in electronic payment include the amount of the payment, anonymity, security, and on-line or off-line validation [8,17,19]. Depending on the amount of the payment, electronic payments can be classified into marco-payment (more than US$30), small payment, and micro-payment (less than US$1) [12,21]. Electronic payments should protect the customer’s privacy, just as the merchants do not know the identity of a customer in a cash transaction. The security issues of electronic payment include integrity, authentication, authorization, confidentiality, availability, and reliability. The security issues described above require cryptographic technologies. For electronic payments using off-line verification, no third party is involved besides the merchant and the customer. On the other hand, for those using on-line verification, a trusted third party, such as a bank or a network operator, is involved. On-line verification needs more messages exchanged, but can prevent the users from double spending.

Current mobile phone users can buy goods by dialing a premium-rate number; network operators charged the users based on the number dialed. For example, using the Mobile Pay provided by Sonera, a mobile user dials the number displayed on a vending machine to buy goods from it. Moreover, mobile handsets are used to authenticate the users and to obtain authorization from the user for a payment. Movilpago, Spain, provides merchants terminals, through which a customer’s mobile phone number and the code of the purchased goods are input. The customer’s handset will show the price and the description of the goods. After the customer enters his or her PIN to the handset, the network operator send transaction confirmation messages to both the merchant and the customer. Paybox and GiSMo use similar scheme to support mobile commerce [15].

The mobile commerce examples described above are based on the telephone number of a user to ensure a limited level of user authentication. MobilePay and MobileSmart use the caller identity information provided in the IN. Movilpago, Payboxand GiSMo the callee identity. Each transaction requires at least one phone call connected, or one short message transferred. The mobile network of next generation will be an all-IP network. User authentication based on the caller or callee ID is inadequate for the dynamic mobile commerce. Neither the anonymity requirement for mobile commerce is satisfied by current solutions, since the phone number of the customer is revealed to the merchants. Another limitation of the mobile commerce schemes above is that a mobile user can only purchase goods or value-added service from merchants who have signed contracts with the network operator. Due to the rapid development of wireless LANs, in the near future, there may be numerous independent small wireless networks based on 802.11 wireless LAN. In the independent small networks, value-added services, such as printers, can be provided [8]. To enable a mobile user to buy any products or obtain any service, in any networks, from any merchants (contracted or non-contracted) is an important issue.

The goal of this project is to design a charging and payment gateway and an AAA server for mobile networks to enable mobile users to purchase value-added service and goods using their mobile phones. The existing user authentication mechanism of mobile networks is reused for this mobile payment, and the VASP (value-added service provider) or merchant is paid by the network operators, which in turn charge the users for the transactions. Both post-paid users and pre-paid users are supported. A one-pass authentication scheme has been developed to reduce the number of messages exchanged for user authentication.

2. System Design Principles

Since our goal is to design a mobile payment scheme for the 3G (3rd Generation) mobile networks, and mobile handsets are used for mobile payments, we make the following assumptions in our payment system design.

1. The SIM-card-based user authentication mechanism of the mobile network will be reused.
2. Since a mobile handset can be always on line, on-line user authentication and transaction verification will be used.
3. The merchant can be a trusted one, who signs contracts with the network operator or one without a contract.
4. The user can be a post-paid user, who pays monthly bill, or a pre-paid user, who has deposited cash in his prepaid account.
5. The users can remain anonymous to the merchants without revealing his phone number, or IMSI.

Based on the billing system of a network operator, our mobile payment solution can support features as follow,

1. Charging can be done by transferring an appropriate CDR to the billing system; new types of CDR for mobile payments need to be defined.
2. Charging can also be done by debiting credit from a prepaid account.
3. Reservation of an amount of credit for a delayed payment is supported; the success of the reservation ensures that value-added services of long duration, such as watching a movie, will not be interrupted because of credit depletion.
4. Credit transfer between two accounts is supported.

The mobile payments that we investigate involve at least three parties: a mobile user, the network operator, and a merchant or VASP; their interactions can be depicted in Figure 3. A mobile payment can be divided into three stages:

Stage 1: A mobile user sends a payment request to the network operator; the payment request contains the amount of the payment and the merchant’s ID. Alternatively, the payment request can be sent buy the merchant to the network operator; in this case the payment request may include a digital signature of the user.

Stage 2: The network operator makes an electronic payment to the merchant, and informs the user of the result.

Stage 3: After the payment is made, the network operator transfers the payment record to its billing system.

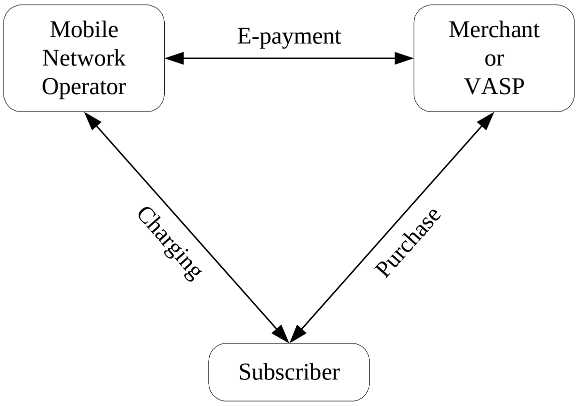

Figure 3: The model of the mobile payment

At stage 1, we need to consider the security of the payment, including data integrity, authentication (for the user and the merchant), confidentiality, and anonymity. At stage 2, a third party, such as a bank, may be involved, i.e., the electronic payment is made through a bank. Due to the diversity of existing electronic payments, we have designed a charging and payment gateway to interwork with the heterogeneous electronic commerce environment. At stage 3, we integrate the mobile payment with the pre-paid accounts and the post-paid accounts of the network operator. Note that if the payment is charged on a prepaid account, the credit charging should be done before or at the same time as the payment is made at stage 2.

Figure 4 depicts our system architecture. Note that an AAA server, and a Charging/Payment Gateway are added to the UMTS network. The function of each component is described below.

1. AAA server and AAA DB: An AAA server and DB provide the authentication, authorization and accounting functions to the users of the network operators. The AAA server support Diameter and SIP protocols [22, 23]. All users should send a SIP registration request message to the AAA server before they want to use the mobile payment service. The AAA server maintains the registration information of the users and checks the users’ privilege of using payment service. The AAA DB stores the user profile.
2. Home Subscriber Server (HSS): The HSS maintains mobile users' identity information, such as directory number, profile, billing information, authentication information, as well as the users’ current locations. The AAA server can retrieve a user’s information from the HSS through Cx interface.
3. GPRS Support Node (GSN): GSNs include SGSNs and GGSNs. They provides the mobile users connections to the Public Domain Network (PDN) through the radio access network. Before connecting the GSNs, the mobile users must be authenticated by a GSN; this GPRS-level authentication will be described in next section.
4. Charging/Payment Gateway (CPGW): The CPGW is responsible for charging users and making payments to the merchants; it receives charging and payment requests from the AAA server.
5. Charging Gateway Function (CGF): The CGF is a standard UMTS entity; it processes the charging information from the GSNs and transfer the collection information to the network operator’s Billing System.
6. Banks or other third parties: They are the financial houses; they provide various payment solutions to the users and merchants. The network operators can cooperate with them.
7. Billing System: The billing system includes the standard offline billing system and online charging system define in 3GPP specifications.

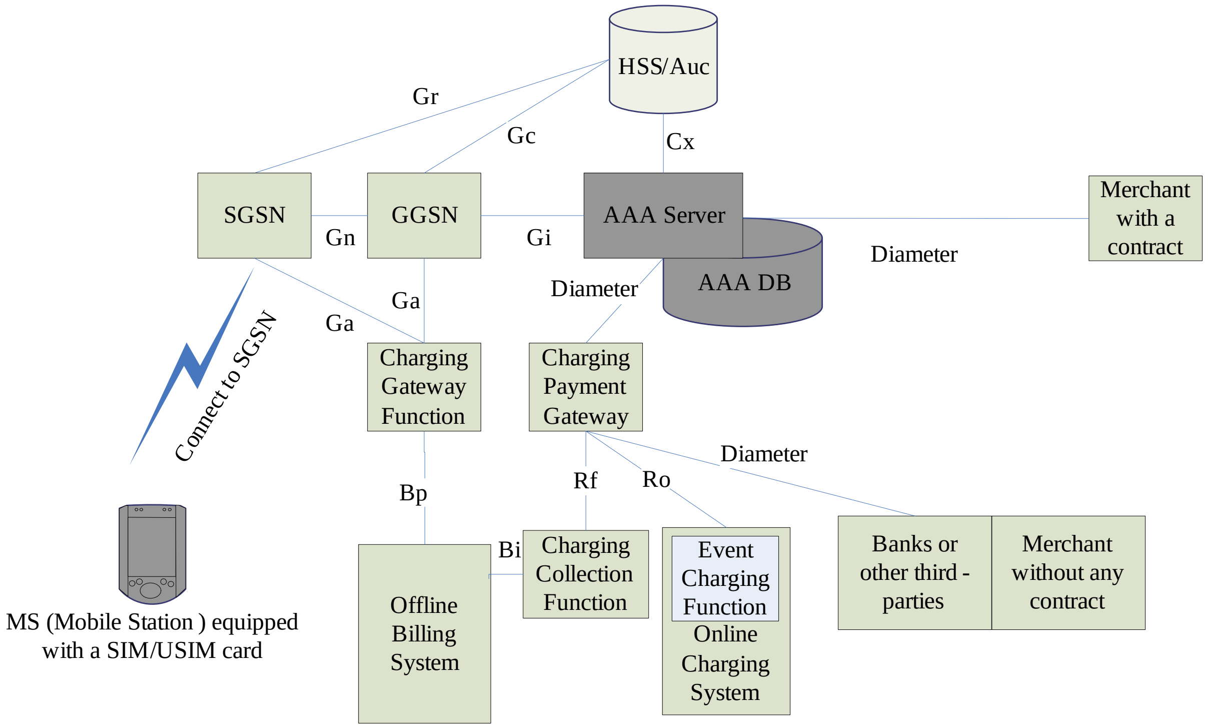

Figure 4: The System Architecture.

3. User Authentication

This section presents a one-pass authentication (performed at the GPRS level) that can authenticate an mobile payment user without explicitly performing the mobile-payment-level authentication. In our approach, the SGSN implements a SIP Application Level Gateway (ALG) that modifies the format of SIP messages (to be elaborated). The GPRS authentication (Steps **G*.1** – **G*.6** in Figure 5) is a GPRS authentication procedure.

After GPRS authentication (Steps **G*.1** – **G*.6**; these steps are exactly the same as **G.1** – **G.6** in the 3GPP GPRS authentication), the MS performs PDP context activation to obtain access to the GPRS service. Then the MS registers to the mobile payment AAA server through steps **I*.1** – **I*.5** in Figure 5:

Step **I*.1**: The MS sends a SIP REGISTER message to the SGSN with the parameter IMPI = impi.

Step **I*.2**: Note that after PDP context activation, the SGSN can identify the IMSI of the MS that transmits the GPRS packets. The SIP ALG in the SGSN adds the IMSI value (i.e., imsi) of the MS in the REGISTER message and sends it to the AAA server.

Step **I*.3**: The AAA server stores the pair (imsi, impi) in the MS record, and sends the Server Assign Request message to the HSS/AuC with the parameter IMPI = impi.

Step **I*.4**: The HSS/AuC uses the received IMPI value impi as an index to retrieve the IMSI and user profile of the MS. We denote $\mathrm{IMSI}_{\mathrm{HSS}}$(impi) as the IMSI value retrieved from the HSS/AuC. The HSS/AuC stores the AAA server name and sends the Server Assignment Answer to the AAA server (with the parameters $\mathrm{IMSI}_{\mathrm{HSS}}$(impi) and User Profile).

Step **I*.5**: The AAA server checks whether the value imsi and the $\mathrm{IMSI}_{\mathrm{HSS}}$(impi) are the same. If so, the AAA server sends the 200 OK message to the SGSN. If $\mathrm{IMSI}_{\mathrm{HSS}}$(impi) ≠ imsi, then it implies the registration is illegal.

Step **I*.6**: Suppose that $\mathrm{IMSI}_{\mathrm{HSS}}$(impi) = imsi. The SGSN sends the 200 OK message to the MS. At this point, the mobile payment registration procedure is successfully completed.

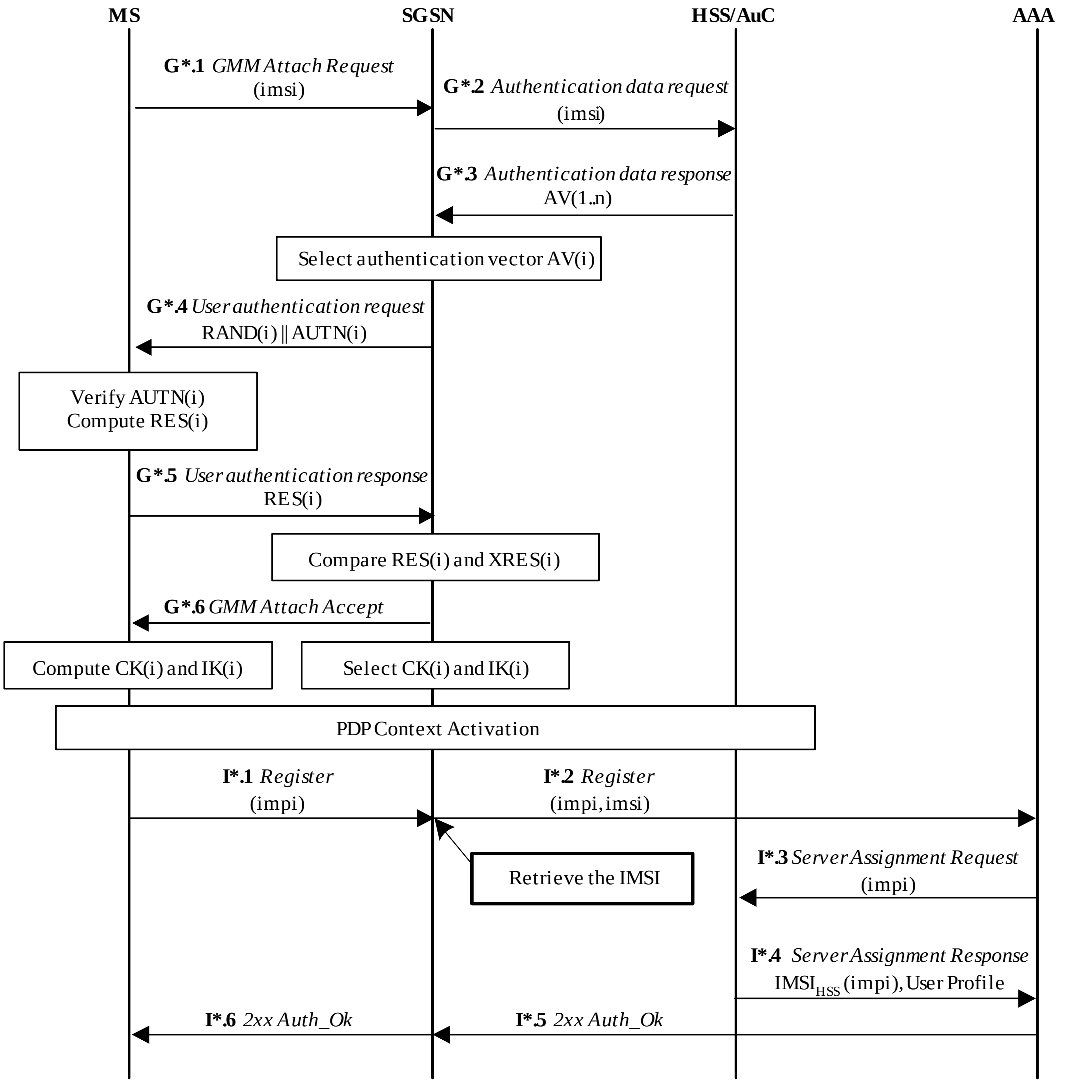

Figure 5: One-Pass Mobile Payment Authenticaion

4. Message Flow of a Mobile Payment

Two commands, Accounting Request and Account Answer, defined in Diameter base protocol can be used for charging and payment functions. Since payments may be made to a third party, such as a merchant and a VASP, new AVPs (Attribute Value Pairs) are defined to support flexible payment methods. Merchant-Name indicates the identity of the merchant to whom the payment is made. Request-Account-Action indicates the payment method that the user chooses; 0: prepaid, 1: postpaid, and 2: bank transfer. Service-Unit indicates the amount of the payment. Accounting-Record-Type has been defined in Diameter base protocol, and we use it in the same way; 1: EVENT_RECORD, 2: START_RECORD, 3: INTERIM_RECORD and 4: STOP_RECORD.

Figure 6 illustrates the message flow of a mobile payment. The payment can only be made after a mobile handset completes the registration operation.

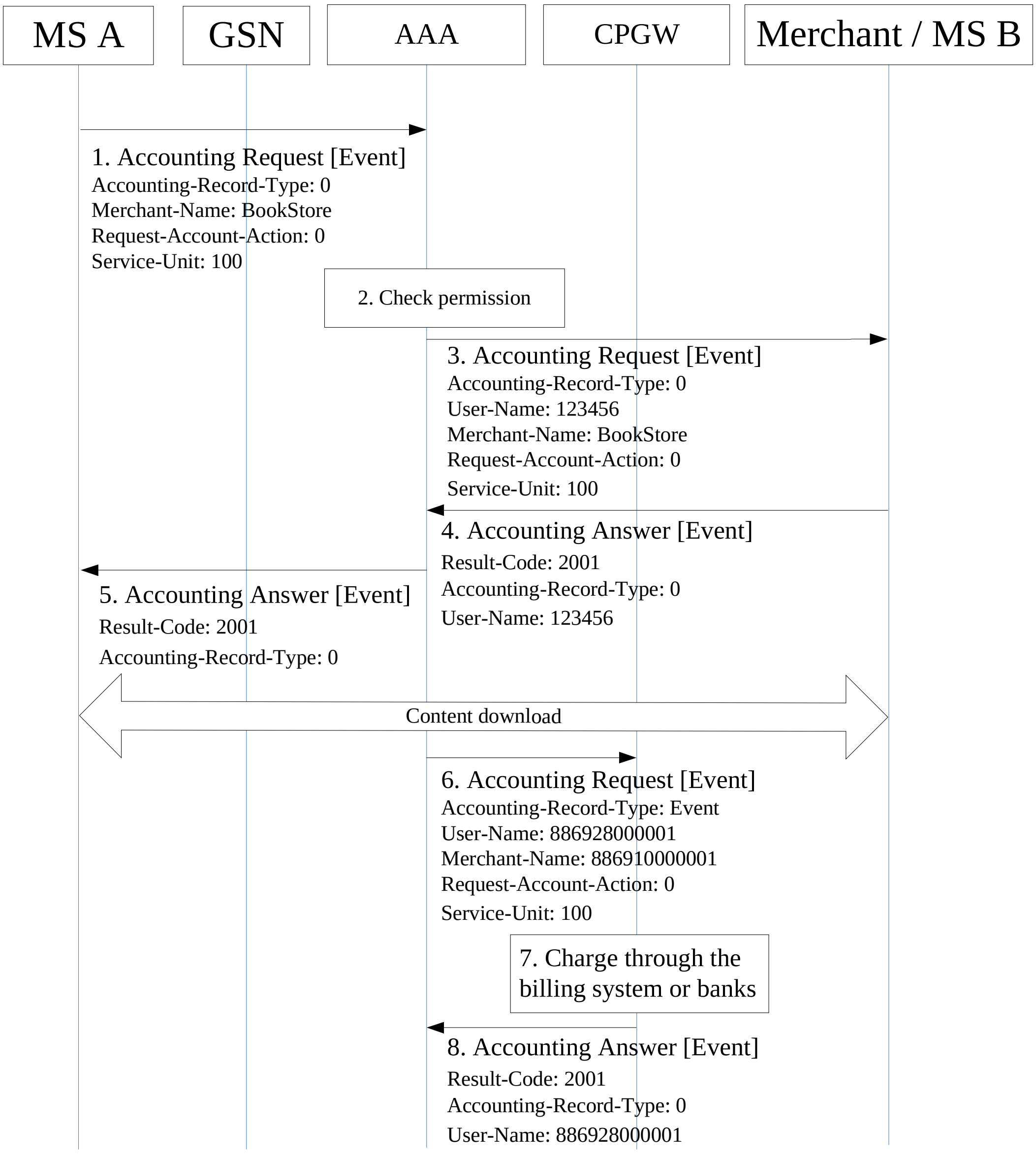
MS A
GSN
AAA
CPGW
Merchant / MS B
1. Accounting Request [Event]
Accounting-Record-Type: 0
Merchant-Name: BookStore
Request-Account-Action: 0
Service-Unit: 100
2. Check permission
3. Accounting Request [Event]
Accounting-Record-Type: 0
User-Name: 123456
Merchant-Name: BookStore
Request-Account-Action: 0
Service-Unit: 100
4. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
User-Name: 123456
5. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
Content download
6. Accounting Request [Event]
Accounting-Record-Type: Event
User-Name: 886928000001
Merchant-Name: 886910000001
Request-Account-Action: 0
Service-Unit: 100
7. Charge through the billing system or banks
8. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
User-Name: 886928000001

Figure 6: Message Flow of a Mobile Payment

1. When the user decides to purchase or download the content from a merchant, he or she uses the MH to send an Account Request message with the user, merchant and payment information to the AAA server.
2. The AAA Server checks whether the user has the privilege to use the payment service. For a prepaid user, the AAA server needs to check if the user account has enough credit.
3. Assume that the user passes the privilege check. The AAA server sends an Account Request message to the merchant.
4. The merchant examines the payment transaction and sends the results in an Account Answer message to the AAA server.
5. The AAA server relays the Account Answer message to the MS.
6. Assume that the transaction succeeded. The AAA server sends an Account Request message with the payment information to the CPGW.

7. The CPGW issues a fund transfer with the payment method specified by the user to the billing system. The detail will be described in next session.
8. The CPGW sends an Account Answer message to inform the AAA server of the charging results.

5. Message Flow of the Charging Function

The Charging/Payment Gateway (CPGW) is responsible for charging users and making payments to the merchants; it receives charging and payment requests from the AAA server. For a prepaid user, the CPGW notifies the ECF (Event Charging Function) of the online charging system, as shown in Figure 4; The ECF debits the charge from the user's prepaid account in real-time. The protocol used for communications between the CPGW and ECF is Diameter. For a post-paid user, The CPGW sends a Payment CDR, a new CDR type we defined, to the CCF (Charging Collection Function) of the offline billing system, as shown in Figure 4; the billing system generates monthly bills from the CDR collected.

A merchant who signs a contract with the network operator can own a prepaid and/or postpaid account. In this case, the payment to the merchant can be done in the same way as a prepaid or a post-paid user is charged, but the merchant is charged with a negative Requested-Service-Unit value, i.e., the balance of the account increases by the charging. If a merchant does not own any account with the network operator, the payment must be made through a third party financial institute, such as a bank. In this case, we use the account functions of Diameter protocol to make the payment, as shown in Figure 4.

There are many possible charging and payment scenarios, because of the combinations of various types of the user and the merchant involved in a payment. We will present the message flows of two scenarios: 1. a prepaid user pays a merchant with a prepaid account, and 2. a postpaid user pays a merchant with a postpaid account. The message flows of other scenarios are similar.

Figure 7 illustrated the message flow of charging a prepaid user and payment made to a merchant with a prepaid account. After the user and merchant confirm the payment, as described in Figure 6, charging is performed in the following steps:

1. The AAA server sends the CPGW an Accounting Request message indicating prepaid account transfer, the account information, and the service unit.
2. The CPGW sends an Accounting Request message to the ECF to debit the service unit, 100 in this example, from the user's prepaid account.
3. After the ECF performs event charging control to the 3G online charging system and debits the user's prepaid account, the ECF sends the result to the CPGW.
4. The CPGW sends an Accounting Request message to the ECF. Note that the value of Request-Service-Unit is set -100 to increase the merchant's credit in his account.
5. After the ECF performs event charging control to the 3G online charging system and credits the merchant's prepaid account, the ECF sends the result to the CPGW.
6. The CPGW sends the results to the AAA server.

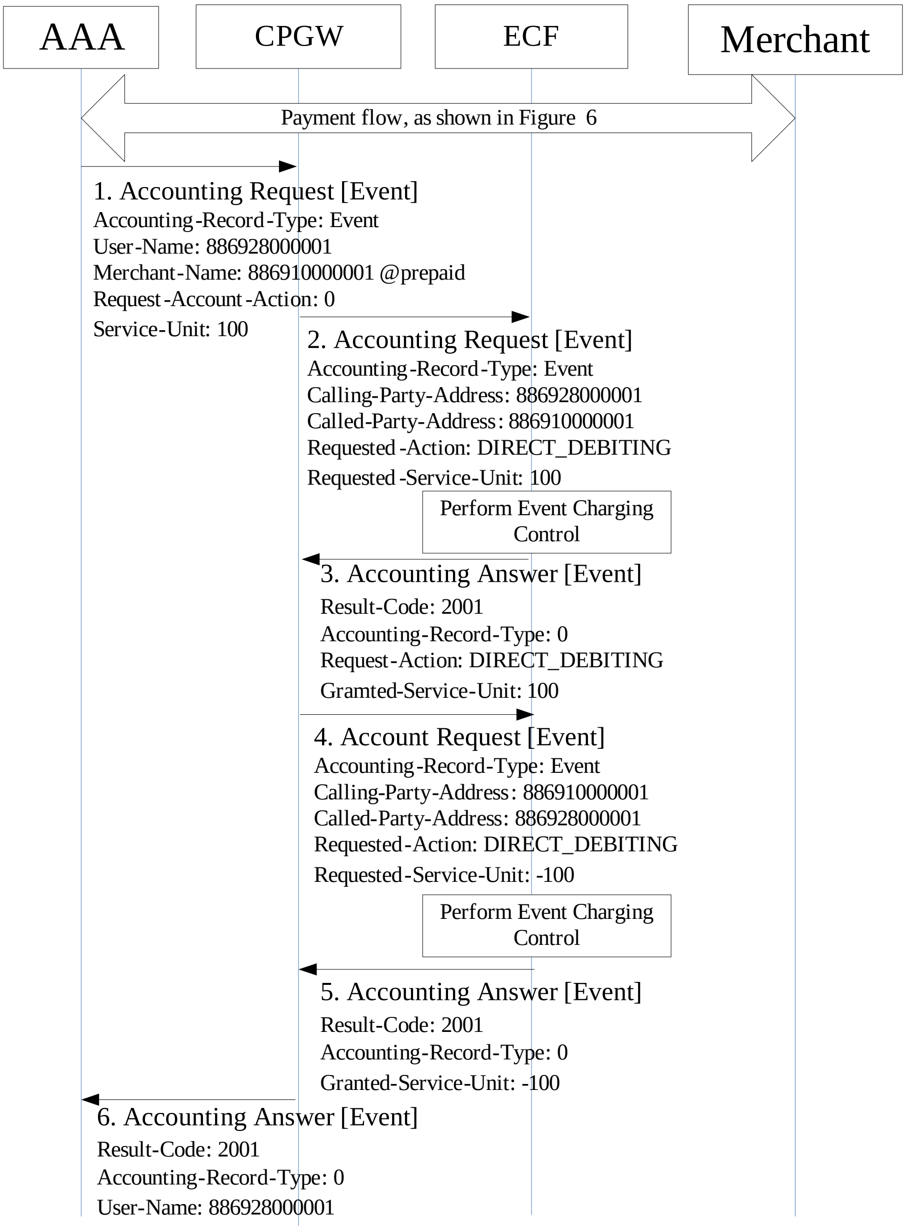
AAA
CPGW
ECF
Merchant
Payment flow, as shown in Figure 6
1. Accounting Request [Event]
Accounting-Record-Type: Event
User-Name: 886928000001
Merchant-Name: 886910000001 @prepaid
Request-Account-Action: 0
Service-Unit: 100
2. Accounting Request [Event]
Accounting-Record-Type: Event
Calling-Party-Address: 886928000001
Called-Party-Address: 886910000001
Requested-Action: DIRECT_DEBITING
Requested-Service-Unit: 100
Perform Event Charging Control
3. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
Request-Action: DIRECT_DEBITING
Gramted-Service-Unit: 100
4. Account Request [Event]
Accounting-Record-Type: Event
Calling-Party-Address: 886910000001
Called-Party-Address: 886928000001
Requested-Action: DIRECT_DEBITING
Requested-Service-Unit: -100
Perform Event Charging Control
5. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
Granted-Service-Unit: -100
6. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
User-Name: 886928000001

Figure 7: Message Flows of Charging Prepaid Accounts

Figure 8 illustrated the message flow of charging a postpaid user and payment made to a merchant with a post account. After the user and merchant confirm the payment, as described in Figure 6, charging are performed in the following steps:

1. The AAA server sends the CPGW an Accounting Request message indicating postpaid account transfer, the account information, and the service unit..
2. The CPGW sends an Accounting Request message to the CCF. The Calling-Party-Address indicates the user’s identity, and the Called-Party-Address indicates the merchant’s identity.
3. After the CCF creates a Payment CDR of the user, the CCF sends the result to the CPGW.
4. The CPGW sends an Accounting Request message to the CCF. Note that the value of Request-Service-Unit is set negative to credit the merchant’s account.
5. After the CCF creates a Payment CDR of the merchant, the CCF sends the result to the CPGW.

6. The CPGW sends the result to the AAA server.

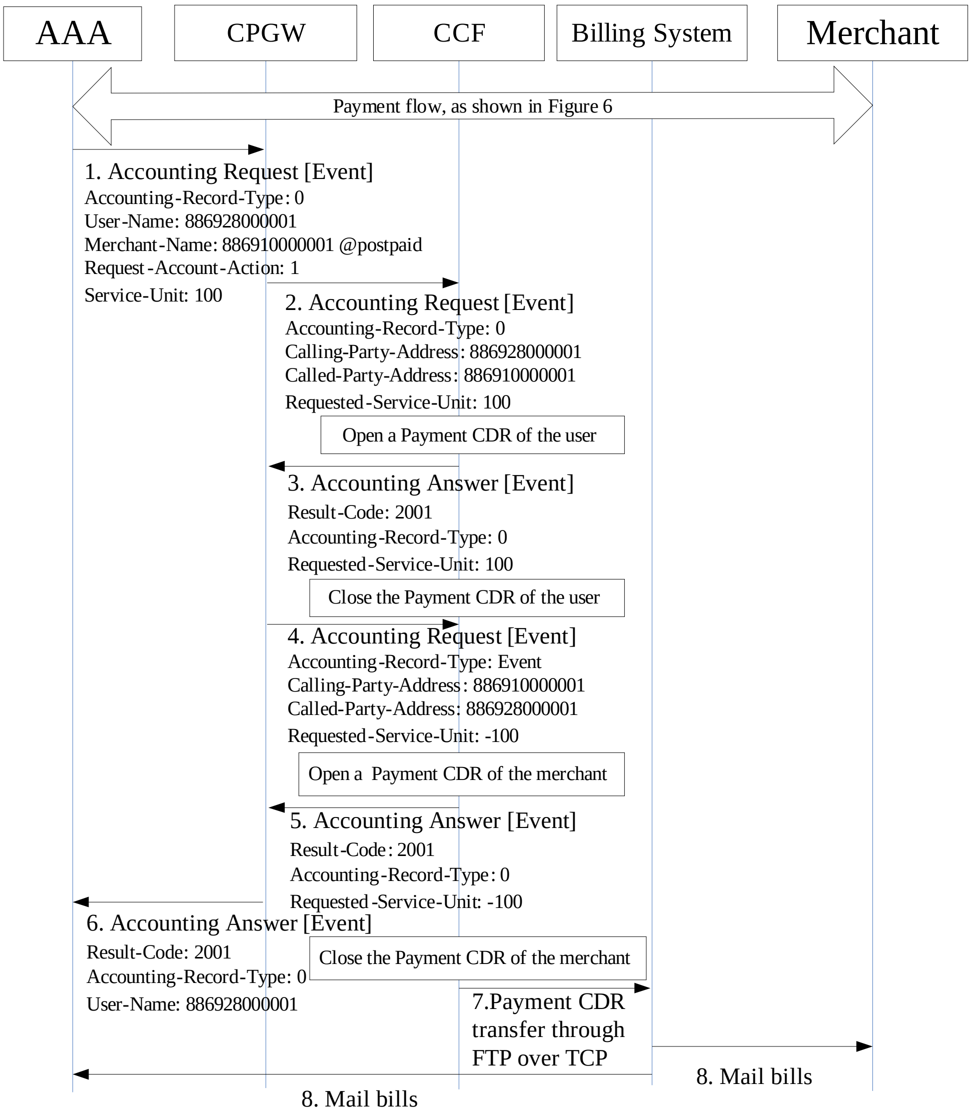
AAA
CPGW
CCF
Billing System
Merchant
Payment flow, as shown in Figure 6
1. Accounting Request [Event]
Accounting-Record-Type: 0
User-Name: 886928000001
Merchant-Name: 886910000001 @postpaid
Request-Account-Action: 1
Service-Unit: 100
2. Accounting Request [Event]
Accounting-Record-Type: 0
Calling-Party-Address: 886928000001
Called-Party-Address: 886910000001
Requested-Service-Unit: 100
Open a Payment CDR of the user
3. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
Requested-Service-Unit: 100
Close the Payment CDR of the user
4. Accounting Request [Event]
Accounting-Record-Type: Event
Calling-Party-Address: 886910000001
Called-Party-Address: 886928000001
Requested-Service-Unit: -100
Open a Payment CDR of the merchant
5. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
Requested-Service-Unit: -100
6. Accounting Answer [Event]
Result-Code: 2001
Accounting-Record-Type: 0
User-Name: 886928000001
Close the Payment CDR of the merchant
7.Payment CDR transfer through FTP over TCP
8. Mail bills
8. Mail bills

Figure 8: Message Flows of Charging Postpaid Accounts

6. Conclusion

In the first year of this two-year research project, supported by NSC, we have investigated mobile payment infrastructure for B3G (Beyond 3G) network. We design a mobile payment system that enables a subscriber to make payment to a VASP (or merchant) through the network operator and remain anonymous to the VASP. The customer can be a pre-paid subscriber or post-paid (monthly bill) one. A one-pass user authentication utilizing the SIP ALG of the SGSN has been developed. In addition, we have developed a charging and payment gateway, and an AAA server to perform the following functions: 1. Interwork the mobile payment with the existing pre-paid and post-paid billing system of the UMTS network. 2. Interwork with existing electronic payment systems to make payments to VASPs.

Reference

1. K. Boman, G. Horn, P. Howard and V. Niemi, “UMTS Security,” IEE Electronics & Communication Engineering Journal, Oct. 2002, pp. 191-204.
2. M.-F. Chang, Y.-B. Lin and W.-Z. Yang, “Performance of hot billing mobile prepaid service,” Computer Networks Journal, vol. 36, Jul. 2001, pp. 269-290.

3. M.-F. Chang, W.-Z. Yang and Y.-B. Lin, “Performance modeling of service node in mobile prepaid service,” IEEE Trans. on Vehicular Technology, vol. 51, 2002, pp. 587-612.
4. ETSI, “Cx and Dx interfaces based on the Diameter Protocol; Protocol details,” TS. 29.229.
5. ETSI, “General Packet Radio Service (GPRS) Service description; Stage 2,” TS 23.060.
6. ETSI, “GPRS Charging,” TS 101.393.
7. ETSI, “Service Aspects ; Charging and billing,” TS 22.115.
8. ESTI, “Telecommunication management; Charging management; Charging data description for the CS domain,” TS 32.205.
9. ESTI, “Telecommunication management; Charging management; Charging data description for the PS domain,” TS 32.215.
10. ESTI, “Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS),” TS 32.225.
11. ESTI, “Telecommunication management; Charging management; Charging data description for application services,” TS 32.235.
12. S. Glassman, et al., “The Millicent Protocol for Inexpensive Electronic Commerce,” Proc. 4th Int. World Wide Web Conference, Dec. 1995, pp. 603-618.
13. H. Knospe and S. Schwiderski-Grosche, “Future Mobile Networks: Ad-hoc Access Based on Online Payment with Smartcards,” Proc. PIMRC, pp. 197-200.
14. C.-H Liu., et. al., “CAMEL Evolution and PPS Evaluation,” IEEE Intelligent Workshop, 2001, pp. 9-13.
15. D. O'Mahony, M. Peirce, and H. Tewari, “Electronic Payment Systems for E-Commerce,” 2nd Ed., Artech House, 2001,
16. M. Peirce, “Multi-Party Electronic Payments for Mobile Communications,” Ph.D. Thesis, University of Dublin, Trinity College, Oct. 2000.
17. S. Schwartz, “AAA adds to prepaid woes,” Billing World and OSS Today, May 2001.
18. S. Schwiderski-Grosche and H. Knospe, “Secure Mobile Commerce,” IEE Electronics & Communication Engineering Journal, Oct. 2002, pp. 228-238.
19. U. Varshney, “Mobile Payments,” IEEE Computer, Dec. 2002, pp. 120-121.
20. G. Vincent, “Learning from i-mode,” IEE Review, Nov. 2001, pp. 13-18.
21. S. Yen, L. Ho and C. Huang, “Internet Micropayment Based on Unbalanced One-Way Binary Tree,” Proc. Cryp TEC ’99, July 1999, pp. 155-162.
22. P. Calhoun Airespace, Inc., “Diameter Base Protocol” RFC 3588, IETF, September 2003.
23. J. Rosenberg, Henning Schulzrinne, G. Camarillo, E. Schooler, Mark Handley et al., “SIP : Session Initiation Protocol”, RFC 3261, IETF, June 2002.