P2P-Paid: A Peer-to-Peer Wireless Payment System

Jerry Gao, Ph.D., Krishnaveni Edunuru, Jacky Cai, and Simon Shim, Ph.D.
San Jose State University, Computer Engineering, San Jose, USA
gaojerry@hotmail.com

Abstract

The fast advance of wireless networking, communication, and mobile technology is making a big impact to daily life. The significant increase of mobile device users in the recent years causes a strong demand on secured wireless information services and reliable mobile commerce applications. Since wireless payment is a critical part of most wireless information services and mobile commerce applications, how to generate secured mobile payment systems becomes a hot research topic in both the e-commerce research community and wireless commerce industry. This paper proposes a peer-to-peer wireless payment system, known as P2P-Paid, to allow two mobile users to conduct wireless payment transactions over the Bluetooth communications. The system uses a 2-dimensional secured protocol, which not only supports the peer-to-peer (P2P) payment transactions between two mobile clients using Bluetooth communications, but also supports the related secured transactions between the payment server and mobile clients. This paper provides a system overview about system functional features, system architecture, and used technologies. Moreover, an integrated security solution for the P2P-Paid system is described. Our first phase implementation is reported, and application examples are given to demonstrate the functions and feasibility of this system.

Keywords: mobile payment, wireless commerce, electronic commerce, secured payment protocol, and mobile payment system, and electronic payment.

1. Introduction

The fast advance of wireless networking, communication, and mobile technology is making a big impact on daily life. As there is a significant increase of mobile device users, more wireless information services and mobile commerce applications are needed [1][2][3]. Since wireless payment is an essential part of mobile commerce applications for mobile device users (such as mobile banking, wireless trading, and mobile shopping), how to build secured wireless payment systems to support mobile payment transactions becomes a hot research topic. According to the Wireless World Forum, mobile payment on wireless devices will provide excellent business opportunities in the coming years. By 2005, Japan, USA, Germany and UK will become four of the largest mobile payment markets in the world because there will be more than 200 million regular mobile users that will spend a total of 222 billion dollars using the new mobile payment system. Therefore, creating secure and cost-effective wireless payment solutions to support mobile device users not only provides good business opportunities, but also brings new technical challenges and issues to engineers. Although now we have a number of types of electronic payment solutions for Internet-based applications and commerce, we are still faced with new issues and challenges in wireless payment because of lack of study and experience in wireless payment. Although there are a number of papers discussing businesses markets, payment process, payment methods and standards in wireless payment [4][5][6][7], there are a very few papers discussing how to build wireless payment systems, including protocols, design issues, and security solutions [8][9][10][11][12].

This paper proposes a peer-to-peer wireless payment system, known as P2P-Paid, to allow two mobile users to conduct wireless payment transactions over the Bluetooth communications. The system uses a 2-dimensional secured protocol, which not only supports the peer-to-peer payment transactions between two mobile clients using Bluetooth communications, but also supports the related secured transactions between the payment server and mobile clients. This paper provides a system overview about system functional features, system architecture, and used technologies. Moreover, an integrated security solution for the P2P-Paid system is described. Our first phase implementation is reported, and application examples are given to demonstrate the functions and feasibility of this system.

The paper is structured as follows. The next section reviews the existing work on wireless payments. Section 3 introduces a 2-dimensional P2P payment protocol. Section 4 presents P2P-Paid system design, including system architecture, functional components, as well as used technologies and other features. The security solutions are

0-7695-2391-9/05 $20.00 © 2005 IEEE

described in Section 5. Application examples of the current system are given in Section 6. Finally, conclusions and future work are included in Section 7.

2. Backgrounds and related work

What is wireless payment? Wireless payment refers to wireless-based electronic payment for mobile commerce to support point-of-sale and/or point-of-service payment transactions on mobile users' devices, such as cellular telephones, smart phones, and personal digital assistants (PDAs), or mobile terminals. What is a wireless payment system? A wireless payment system is a mobile commerce system processes electronic commerce payment transactions supporting mobile commerce applications in wireless networks and wireless Internet infrastructures. In general, wireless payment systems can be used by wireless-based merchants, mobile content vendors, and wireless information and commerce service providers to process and support payment transactions driven from wireless-based commerce applications. This would include wireless-based trading systems, mobile portals, wireless information, and commerce service applications.

The existing wireless payment systems can be classified into three types. The first type is known as *account-based payment systems*, in which each customer is associated with a specific account maintained by the Trusted Third Party like a bank (or a telco). In pre-paid transactions this account will be directly linked to the consumer's savings account. The consumer maintains a positive balance in this account that is debited when a pre-paid transaction is processed. If post-paid transactions are supported, the charges from a transaction are accrued in the consumer's account. The consumer is then periodically billed and pays for the balance of the account to the TTP. At this time, there are three subdivisions of account-based wireless payment systems: a) mobile phone-based payment systems, which enable customers to purchase and pay for goods or services via mobile phones, b) smart card payment systems, which use a smart card, an embedded microcircuit, which contains memory and a microprocessor together with an operating system for memory control, c) credit-card mobile payment systems, which allow customers to make payments on mobile devices using their credit cards. A good example of a phone-based wireless payment system is PhonePaid's mobile payment system (http://www.phonepaid.com). It allows its customers to use GSM mobile phones to pay for goods and services, or transfer money using their PhonePaid accounts. Paybox, raised by Paybox.net AG (http://www.paybox.net), is another example. Y. Lin et al in [9] discuss and compare four different approaches to provide mobile prepaid services. Z. Huang and K. Chen in [12] introduce a payment system which implements Brand's restrictive blinding signature into mobile devices to offer multi-party security. A. Fourati et al in [10] propose an approach, combining the SET protocol with the TLS/WTLS protocols in order to enforce the security services over the WAP 1.X for the payment in the m-commerce. They propose to implement additional services of the SET protocol like the confidentiality of the payment information between the buyer and the payment gateway for data integrity. S. Kungposdan et al in [8] propose a payment protocol for account-based mobile payment. It employs symmetric-key operations which require lower computation at all engaging parties than existing payment protocols. In addition, the protocol also satisfies transaction security properties provided by public-key based payment protocols such as SET and iKP.

The second type of wireless payment system refers to *Mobile POS payment systems*, which enable customers to purchase products on vending machines (or in retail stores) with their mobile phones. This type of payment system is designed to complement existing credit and debit card systems by enabling mobile users to turn their phones into the payment instruments of their choice. Now there are two types POS payment systems. The first type is known as *automated point-of-sale payments*. They are frequently used in retail vending machines, parking meters or toll collectors to allow mobile users to purchase goods (such as snacks, parking permits, and movie tickets). The other type is known as attended *point-of-sale payments* (shop counters, taxis), which allows mobile users to make payments using mobile devices with the assistance from a service party, such as a taxi driver, or a counter clerk. A typical example of mobile POS payment system is Ultra's M-Pay (http://www.ultra.si/), which enables customers to purchase products on vending machines with mobile phones. M-Pay is based on Ultra's patented payment terminal using voice to transfer authorization data. The user's phone is used to transfer data. This simplifies the terminal design and allows the terminal to focus on safe payment authorization.

The third type is known as Mobile wallets, which is the most popular type of mobile payment option for wireless transactions. Like e-wallets, they allow a user to store billing and shipping information that the user recalls with one-click while shopping from a mobile device [11]. MasterCard's Server-based mobile e-wallets using SET technology are already being used to provide secure transaction capabilities for merchants and cardholders.

Although a number of wireless payment systems have been reported by major players, there are very few technical publications addressing the design and implementation of wireless payment systems and the detailed payment protocols. In this paper, we report our design and implementation on building a wireless payment system for supporting mobile users to conduct wireless payment transactions in a dynamic mobile environment with the support from Bluetooth technology. This type of mobile payments can be used in a dynamic mobile environment to allow a payer and payee to conduct wireless payment transactions for mobile commerce. Typical application examples include:

- Mobile payments between a TAXI passenger and TAXI driver.
- Mobile payments between a merchant in flee market and its customers.
- Mobile payments for parking fees or subways.

3. P2P-Paid payment protocol

The purpose of designing the P2P-Paid payment protocol is to provide a convenient, secure and lightweight protocol built on top of the Bluetooth communication protocol for supporting P2P monetary transactions. P2P-Paid provides various services for mobile users to make P2P monetary transactions securely. Those services include Bluetooth device/service discovery, send/request money, payment management, etc. Multimedia approach is integrated for strong user authentication.

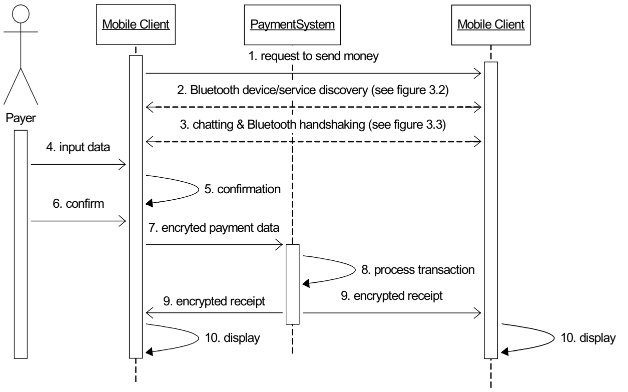


Figure 3.1. P2P-Paid payment transaction sequence

3.1. P2P-Paid mobile payment protocol

Figure 3.1 presents the P2P transaction sequence. It encapsulates four phases: service request, service discovery, authentication and transaction.

Phase 1: Service request. After successfully logging in, the mobile user can select different services (e.g. send money, view account, schedule payment, etc.) provided by the P2P-Paid payment system. The figure above shows the service request for sending money in particular.

Phase 2: Bluetooth service discovery. Bluetooth's Service Discovery Protocol (SDP) provides standard means for a Bluetooth device to query and discover services supported by a peer Bluetooth device. Figure 3.2 below shows a JSR-82 capable MIDlet using the DiscoveryAgent, which provides methods to perform device and service discovery.

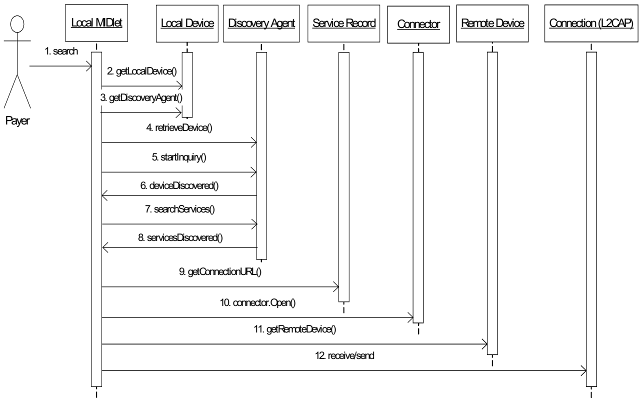


Figure 3.2: Using SDP API sequence

Phase 3: Authentication. Figure 3.3 below shows the authentication procedure when two mobile devices communicate with each other for the first time. Before operating on the payment functions, both the payer and payee should have logged in to the payment system. That is, both mobile devices have already authenticated with the payment system. They all have already received the authentication key from the payment system. K_{init_a} is denoted as the initial key generated by device A; and K_{init_b} is denoted as the initial key generated by device B. K_a and K_b are the unit keys for device A and device B respectively. K_{ab} is the combination key. And K is the negotiated link key, which can be K_a, K_b or K_{ab}. Step 2 to step 8 are the link-creating and paring procedures when two devices communicate with each other at the first time. After the link key is created for these two devices, they don't need to go through those processes again until the link key is expired or deleted.

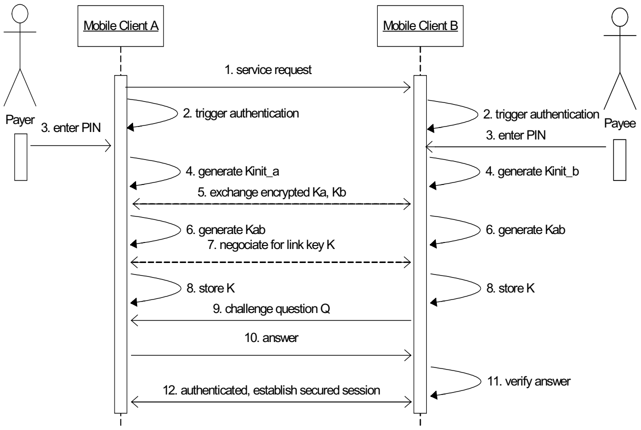
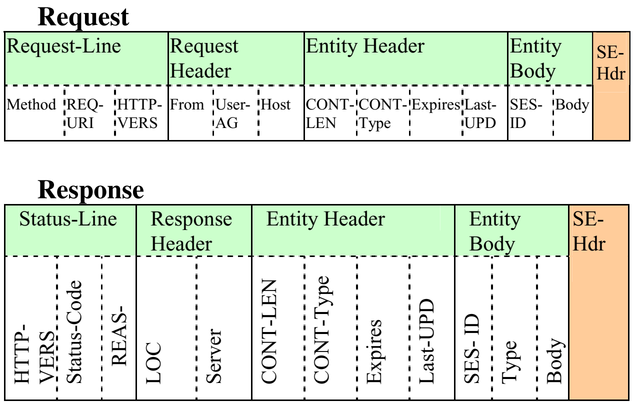


Figure 3.3. P2P-Paid mobile client authentication

Phase 4: Transaction. After step 3 in Figure 3.1, a secured session has been established for the two mobile devices, and the payer already has the payee's ID to which the payment is sent. All the payer needs to do is to enter the amount, payment description and confirm the transaction. In step 8, the system checks the payer's account for efficient balance. If there is not enough money, the transaction cannot be completed and the payer has to go back to step 4 to re-enter payment amount.

3.2. P2P-Paid Message Format

P2P-Paid client-server message format: P2P-Paid application takes the user input from the client (mobile, web). The client communicates with the P2P-Paid server by using HTTP request and response to send or receive messages. The formats of the request and response messages are shown in Figure 3.4. A security header is attached for each message sent across the Internet or the air. The security header is described separately in section 5, the security solution section.



Note: SE-Hdr→Security Header, LOC→Location, CONT-Type→Content Type, SES-ID→Session ID, HTTP-VERS→HTTP-Version, REAS-Phrase→Reason-Phrase, CONT-LEN→Content Length, User-AG→User Agent, Last-UPD → Last Updated.

Figure 3.4. P2P-Paid client-server message format

P2P-Paid Bluetooth message format: P2P-Paid Bluetooth Protocol is used to establish a connection and send data between two MIDlet clients, where these clients are considered as peers. This protocol carries the L2CAP packets in small units. This protocol uses the HCI interface to organize the data between software and hardware. Figure 3.5 below shows the P2P Bluetooth message format.

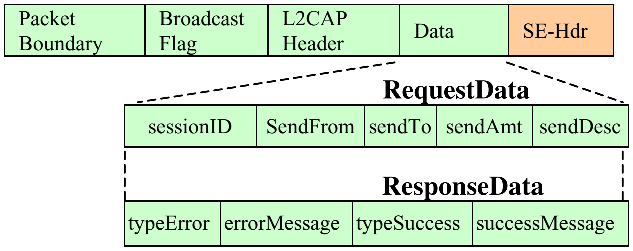


Figure 3.5. P2P-Paid Bluetooth message format

Packet boundary: Packet Boundary flag identifies whether the packet data carries the start of the L2CAP packet. The L2CAP packets are divided into small units as mentioned above. The first packet is always set to START flag and the remaining packets are set to CONTINUE flag.

Broadcast flag: Broadcast Flag distinguishes the data between point-to-point and broadcast communication.

L2CAP header: L2CAP Header contains two bytes of Channel Identifier (CID), two bytes of total length of L2CAP.

Data: the data section is the XML document wrapped inside the L2CAP packet. It is either request or response message type; and the elements in the request and response message are different as shown on the figure.

4. System overview

P2P-Paid is a mobile payment system, which has been developed at San Jose State University as a research prototype system since 2004. It's objective is to develop a wireless-based payment system to assist mobile users to perform mobile payment transactions over mobile phones. In the existing mobile payment system, payment transactions are conducted over a wide area network, P2P-Paid is a mobile payment system which not only allows mobile users to perform electronic payment transactions over a wide area network, but also supports them to conduct peer-to-peer mobile payment transactions on mobile phones over a Bluetooth wireless network.

The P2P-Paid system provides the following major functions to mobile phone users over its mobile client interface:

- **P2P party discovery:** Both payee and payer discover each other over the Bluetooth network.
- **P2P session management:** After the party discovery, the session management allows a user to establish or drop a P2P payment session over the Bluetooth network.
- **P2P payment management:** This allows a user to conduct a P2P mobile payment transaction over the Bluetooth network based on an established P2P payment session. The P2P payment transactions are

carried out using the 2-D payment transaction protocols defined in the previous section.

- **Account management:** This allows a user to perform basic account management functions, such as checking account balance, and displaying an account summary.
- **Payment scheduling:** This allows a user to set up, update, delete, and view payment schedules using mobile phones.
- **Payee management:** This allows a user to perform payee management functions on a mobile phone, such as adding, editing, deleting, and viewing the payee information.

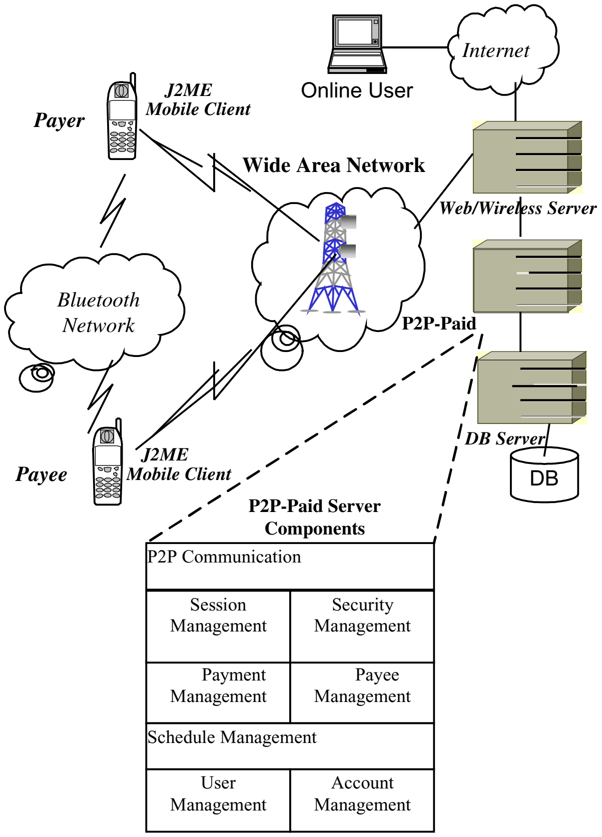


Figure 4.1. P2P-Paid system architecture

To assist mobile users, the P2P-Paid system also provides them with essential web-based payment functions through an online user interface. The basic functions include:

- User registration and service registration to set up a user ID and account ID, update user profile information.
- User online security and authentication checking.
- Account management for payment, such as balance checking, transaction history reporting.
- Mobile payment scheduling which allows users to schedule their payments.
- Payment management which allows users to perform online payment transactions.
- Mobile payee management which allows the user to perform payee management online.

4.1. P2P-Paid system architecture

As shown in Figure 4.1, P2P-Paid system has a 4-tier architecture, which includes mobile client, middleware, P2P-Paid server, and database server.

Mobile client: It includes a) J2ME-based P2P mobile client software for mobile phone users, and b) HTML-based online client for online accesses. The P2P mobile client software includes the following functional parts:

- **User interface:** It supports the interactions with a mobile user to accept and process user requests, and displays the system responses.
- **P2P service module:** It supports Peer-to-Peer interactions between two mobile phone users (payer and payee) to conduct the payment party discovery based on the Service Discovery Protocol, and carries out a P2P-payment transaction over a Bluetooth Network using the Bluetooth L2CAP protocol. Both the payer and payee must be registered with the system through online registration on the Web.
- **Mobile security module:** It performs basic security functions with the support of the security management in the P2P-Paid server, including mobile user authentication and voice verification. In the current version, the voice verification has not been completely implemented.
- **Mobile payment module:** It supports P2P mobile payment communications between a mobile client and the P2P-Paid server over a wireless Internet infrastructure. A 2-D wireless payment protocol is implemented here.

Middleware: It includes an Apache Tomcat Web Server with the wireless Internet support and other middleware software, such as Java JSP and Servlets.

Payment database server: It is a database server (MySQL Server) that works with the database access programs to maintain necessary mobile user and account information, and mobile payment transactions.

P2P-Paid server: It works with middleware by communicating with mobile client software to support the wireless payment functions. As shown in Figure 4.1, the P2P-Paid server consists of the following functional components:

- **P2P communication:** It implements the peer-to-peer 2-D payment protocol to support all mobile payment communications between a mobile client and the server.

- **User management:** It supports user registration and maintains two types of user information, including registered mobile users and administration users.
- **Account management:** It manages and maintains user payment service accounts.
- **Payment management:** It manages and maintains all mobile payment transaction records.
- **Schedule management:** It manages and maintains mobile payment schedules, such as adding, updating, or deleting a payment schedule for mobile user. Whenever a scheduled payment is due, a payment process will be invoked.
- **Payee management:** It manages and maintains the payee records for a mobile user, such as adding, updating, and deleting a payee record.
- **Session management:** It establishes and controls a mobile payment session for mobile payment transactions.
- **Security management:** It supports several security functions, including user access control (such as authentication checking), security key management, and voice verification.

4.2. Implementation status and used technologies

The first version of the P2P-Paid system only implemented the P2P payment protocol with basic security support. The voice verification feature will be added in the later version. The current server is deployed on an *Apache Tomcat Web Server (Version 5.0.28*). On the mobile client side, the J2ME Wireless Toolkit Emulator (Version 2.2) is used to develop and test the MIDP client. In addition, we used JSR 82 (Java APIs for Bluetooth) to test the Bluetooth communications. The Bluetooth API is used to provide an interface to Bluetooth wireless networking, including device discovery and data exchange. In addition, the kXML parser is used to parse xml data on MIDP client and Xercer parser is used on the P2P-Paid server.

5. The P2P-Paid security solution

The basic security solution of the P2P-Paid system is an integration of the secured payment protocol, a biometric verification, and optimized conventional security methods. It provides the following security features: a) service registration, b) access control, c) security code attachment, and d) speaker verification.

a) Service registration: Before using the P2P-Paid payment services, a user must first register with the system. There are two types of registration a user must go through. They are online registration on the Web and mobile registration. On completion of web registration, a user account is created; and a key pair is associated with the web client and the system server (see figure 5.1). On completion of mobile registration, a voiceprint is created for the user for future mobile authentication; and a key pair is also associated with the mobile device and the system server (see figure 5.2).

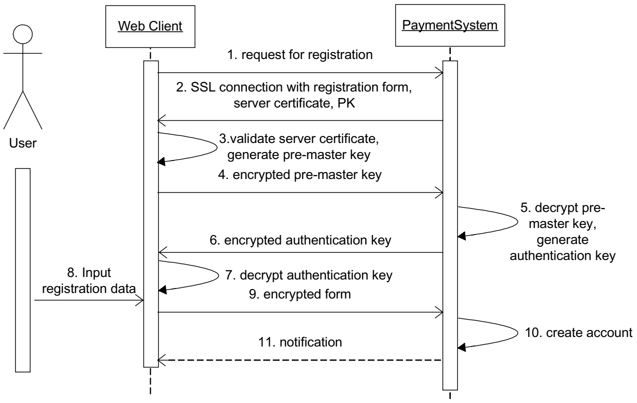

Web Client
PaymentSystem
User
1. request for registration
2. SSL connection with registration form, server certificate, PK
3.validate server certificate, generate pre-master key
4. encrypted pre-master key
5. decrypt pre-master key, generate authentication key
6. encrypted authentication key
7. decrypt authentication key
8. Input registration data
9. encrypted form
10. create account
11. notification

Figure 5.1. Secured web registration sequence

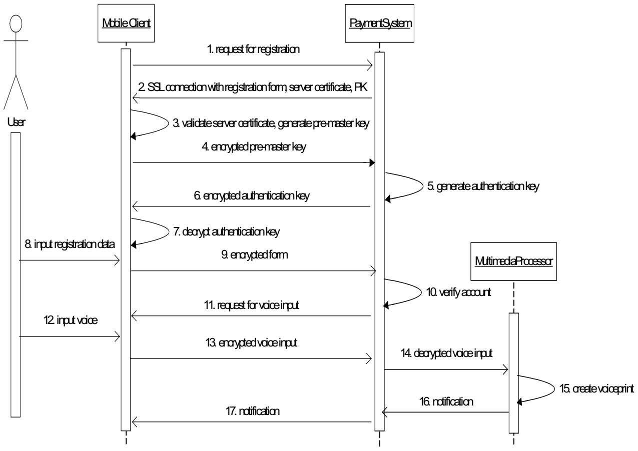

Mobile Client
PaymentSystem
User
MultimediaProcessor
1. request for registration
2. SSL connection with registration form, server certificate, PK
3. validate server certificate, generate pre-master key
4. encrypted pre-master key
5. generate authentication key
6. encrypted authentication key
7. decrypt authentication key
8. input registration data
9. encrypted form
10. verify account
11. request for voice input
12. input voice
13. encrypted voice input
14. decrypted voice input
15. create voiceprint
16. notification
17. notification

Figure 5.2. Secured mobile registration sequence

b) Access control: Authorization comes after authentication. In order to use the P2P-Paid payment service, a mobile user has to login the system first. Only valid user receives the access to the system. There are two types of login: web login and mobile login. Web login requires the user to enter the valid user ID and password. Mobile login requires the user to enter user ID, PIN and voiceprint. Figure 5.3 below presents the P2P-Paid mobile login procedures.

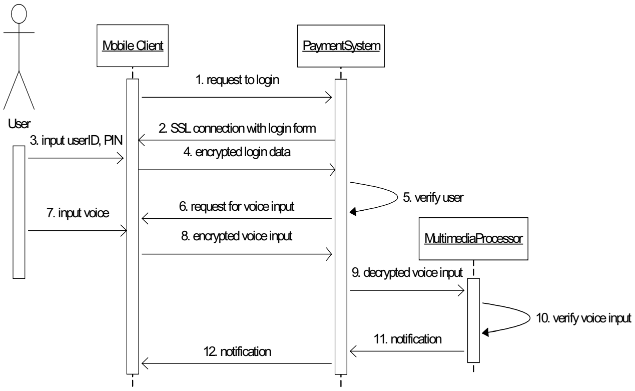


Figure 5.3. Secured mobile login sequence

c) Security Code Attachment: As mentioned in the previous section, any sensitive data is encrypted before transmitting over the network. A security header is attached on each piece of message sent across the Internet or the air. The security header carries the information about the secured protocol. Each entity in the security header can be null or contains value depends on what type of information is sent. To reduce the overhead of encryption and decryption, we have selected the optimized pubic key encryption algorithm given in [18] for the implementation to mobile clients. According to the study in [17][18], this algorithm has shown the potential advantage over other existing algorithms (such as Montgomery MM and Radix-r) in the computation complexity and system overhead.

The format of the security header is shown below.

MAC	Key Used	Key Length	Encrypted Fields (e.g. userID, PIN, account No.)

Figure 5.4. Security Header format

MAC: MAC is the message authentication code. In the context of client to server communication, MAC can be the authentication key used to allow data authentication (see Figure 5.1 for how the authentication key is generated). This allows the receiver to verify the integrity of the message. In the context of Peer-to-Peer communication, the MAC is the link key between two devices.

Key used: For the first time when client connects to the server or when two mobile devices communicate with each other, they have to negotiate what key is used for establishing the secured connection. In the context of client to server communication, the authentication key can be used; while in the context of peer-to-peer Bluetooth communication, either unit key or combination can be used as the link key.

Key length: Due to the ability of different devices for handling different key lengths, an appropriate key length must be negotiated before two devices can start encrypting the traffic between them.

Encrypted fields: This field indicates what fields or which pieces on the message are encoded. What fields to be encrypted depends on the implementation of the application, but in general, all sensitive data such as user ID, password, PIN, account number, etc. should be encrypted before transmitting across the network.

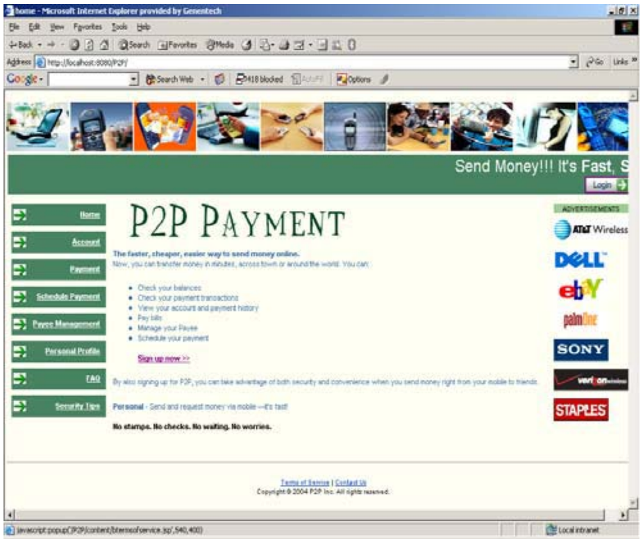
d) Speaker Verification: Speaker verification, as a subclass of voice recognition, is the process of automatically recognizing who is speaking on the basis of individual information included in speech waves. Its task is a hypothesis-testing problem where the system has to accept or reject a claimed identity associated with an utterance [13]. There are two types of speaker verification approaches: text-dependent and text-independent. We use speaker verification as a part of the security solution in P2P-Paid. The basic idea is enhance the system authentication procedures by integrating speaker verification and conventional password (or PIN) checking. Based on our research, there are a number of existing biometric verification systems [13][14][15][16], in which the feature vectors and trained model of a speech are based on a set of world models. To obtain a more accurate model that represents better speech characteristics, a large set of world models is needed. This can be time-consuming. Since most existing solutions are not designed to address mobile client limitations (such as dynamic mobile environment and limited computing power), we are working on to develop a refined text dependent speaker verification module to focus on optimizing feature extracting for each mobile user. Before using the P2P-Paid services with a mobile device, a user has to be authenticated by verifying his/her voiceprint. With this approach, the system is able to perform the authentication for the mobile device and mobile user who is using the device.

The speaker verification model implements a new algorithm to choose better feature vectors for each mobile user. This algorithm is designed based on the fact that only those stable features in a voice signal can better be used for the feature vector set. For example, during enrolment procedures, some Mel-frequency cepstral coefficients (MFCC) and linear prediction cepstral coefficients (LPCC) may not change or change slightly from time to time. However, some of those coefficients could change significantly in different utterances. Those coefficients that don't change or change slightly can be said to be more stable and better represent the speech characteristics than those that change. Therefore, only those stable coefficients should be selected to build the reference models during enrolment and used to compare those coefficients during verification. Since the selection of those coefficients is different for each mobile user, the system is able to compare them dynamically for each user during verification. In theory, this optimized feature extracting approach should be more accurate in speaker verification because each voice model is built based on individual speaker. In addition, the approach should be faster and simpler because a smaller set of coefficients is used for feature extracting and a smaller set world model is used for training. The detailed implementation and experimental results of the speaker verification will be reported in the future publications.

6. Application Examples

In this section, we used a payment scenario to demonstrate two mobile users to conduct a peer-to-peer payment transaction on mobile phones using our first prototype P2P-Paid system. After registering with the P2P-Paid's online interface (see Figure 6.1), two mobile users (Veni and Dharani) start their mobile sessions in the following steps:

- **Step 1: Mobile logon.** A mobile user (say Veni) needs to login the P2P-Paid system using her PIN and voice input. During this step, the system performs the authentication and access control) using her input PIN and voice. Note that the first version of P2P-Paid system did not implement voice verification feature.
- **Step 2: Party discovery.** After logging in, Veni sees a welcome page (see Figure 6.2(a)), and a main menu with different options (see Figure 6.2(b)). Figure 6.2(c) to (f) shows a party discovery scenario in which Veni selects the Bluetooth network option first; next she is taken to the nickname page where she can enter a nickname to avoid the ambiguity. Then, she searches for the right mobile devices, and issues a connection request.
- **Step 3: Party connection.** As shown in Figure 6.2(g) - (i), once connected, both parties (Veni and Dharani) are taken to a Chat window where they can start their communications for mobile payments.
- **Step 4: Party authentication.** Before exchanging payment information, both mobile users have to authenticate each other with their authentication code to ensure trustworthiness on the Bluetooth network. The P2P-Paid server performs user verification in the background and sends back the results to both users. Figure 6.2(j) - (l) shows the scenario.
- **Step 5: Mobile payment.** Figure 6.2(m) shows that Veni issues a payment request when she receives payment account information from Dharani. The mobile payment request will be processed by the P2P-Paid sever and its transaction record will be stored on the server's database.
- **Step 6: Payment confirmation.** After a payment transaction is completed, confirmation messages are sent to both parties to confirm the completion of a payment transaction. Figure 6.2(n) and (o) shows the scenario.



home - Microsoft Internet Explorer provided by Genentech

Address http://localhost:8080/P2P/

P2P PAYMENT

The faster, cheaper, easier way to send money online.

Now, you can transfer money in minutes, across town or around the world. You can:

- Check your balances
- Check your payment transactions
- View your account and payment history
- Pay bills
- Manage your Payee
- Schedule your payment

Sign up now >>

By also signing up for P2P, you can take advantage of both security and convenience when you send money right from your mobile to friends

Personal - Send and request money via mobile—it's fast!

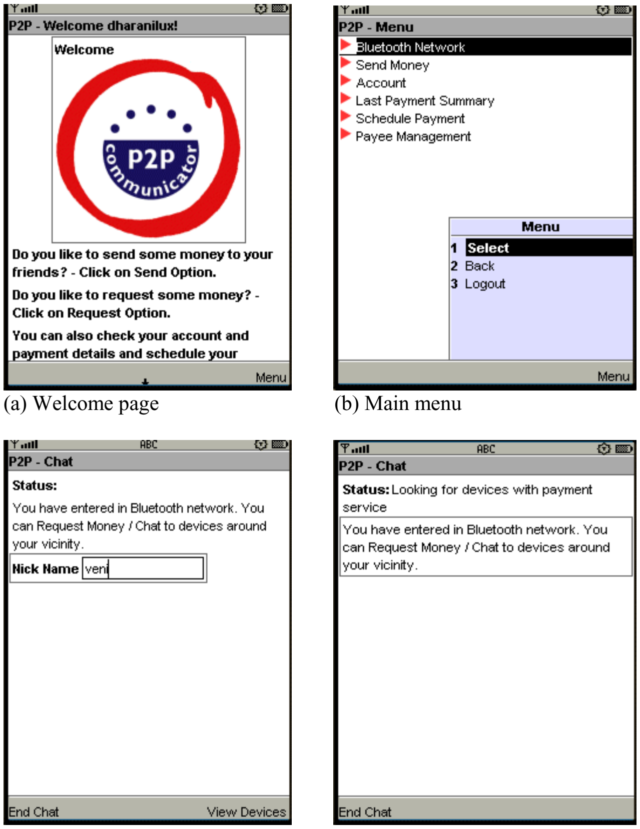
No stamps. No checks. No waiting. No worries.

Terms of Service | Contact Us

Copyright © 2004 P2P Inc. All rights reserved.

javascript:popup('P2P/content/termsofservice.jsp',540,400)

Figure 6.1. P2P-Paid online home page



P2P - Welcome dharanilux!

Welcome

Do you like to send some money to your friends? - Click on Send Option.

Do you like to request some money? - Click on Request Option.

You can also check your account and payment details and schedule your

P2P - Menu

P2P - Chat

Status:

You have entered in Bluetooth network. You can Request Money / Chat to devices around your vicinity.

Nick Name veni

P2P - Chat

Status: Looking for devices with payment service

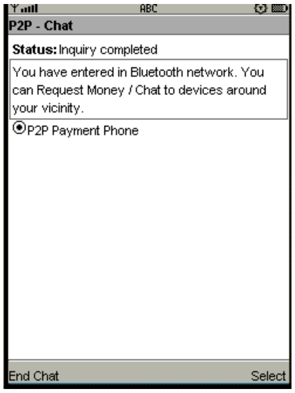
You have entered in Bluetooth network. You can Request Money / Chat to devices around your vicinity.

(a) Welcome page

(b) Main menu

(c) Nickname page

(d) Search for devices

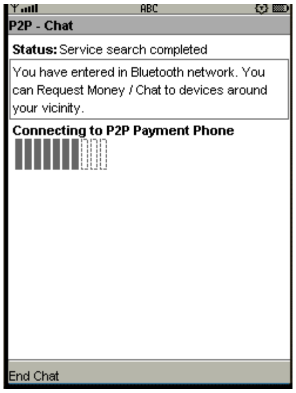


Status: Inquiry completed

You have entered in Bluetooth network. You can Request Money / Chat to devices around your vicinity.

◉P2P Payment Phone

(e) Devices in Bluetooth network

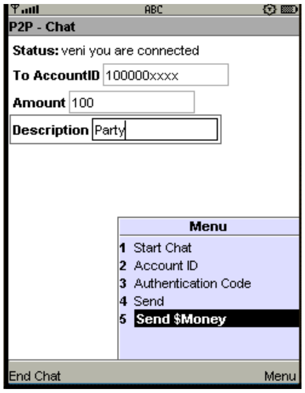


Status: Service search completed

You have entered in Bluetooth network. You can Request Money / Chat to devices around your vicinity.

Connecting to P2P Payment Phone

(f) Connecting to a selected client



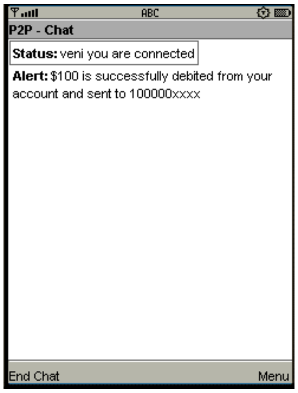
Status: veni you are connected

To AccountID 100000xxxx

Amount 100

Description Party

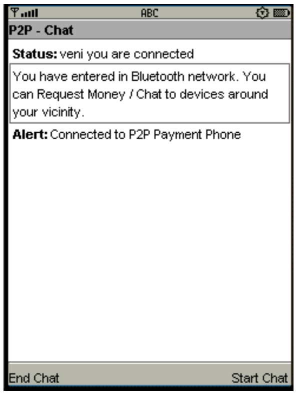
(m) Veni issues a payment



Status: veni you are connected

Alert: $100 is successfully debited from your account and sent to 100000xxxx

(n) A confirmation to payer

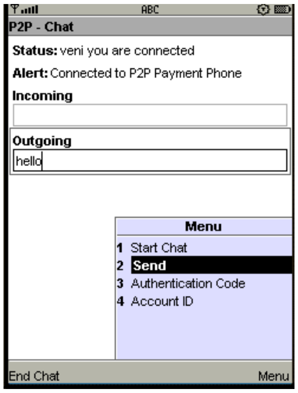


Status: veni you are connected

You have entered in Bluetooth network. You can Request Money / Chat to devices around your vicinity.

Alert: Connected to P2P Payment Phone

(g) An alert to Veni



Status: veni you are connected

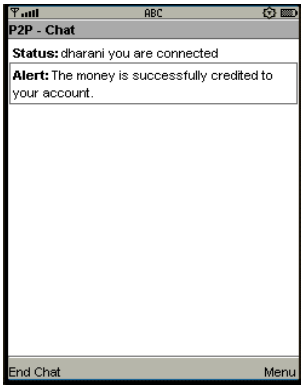
Alert: Connected to P2P Payment Phone

Incoming

Outgoing

hello

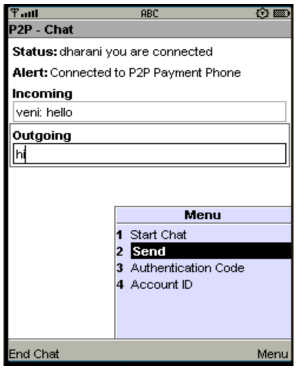
(h) Veni's chat window



Status: dharani you are connected

Alert: The money is successfully credited to your account.

(o) A confirmation to payee



Status: dharani you are connected

Alert: Connected to P2P Payment Phone

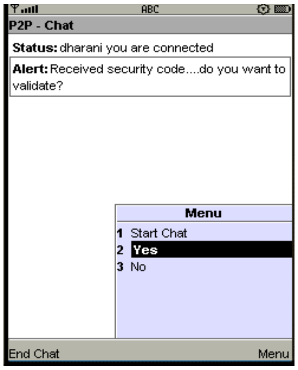
Incoming

veni: hello

Outgoing

hi

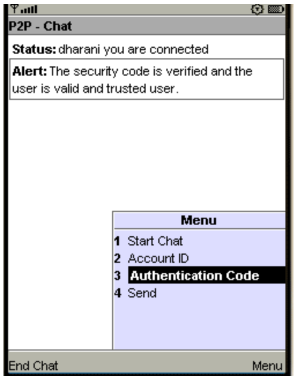
(i) Dharani's chat window



Status: dharani you are connected

Alert: Received security code....do you want to validate?

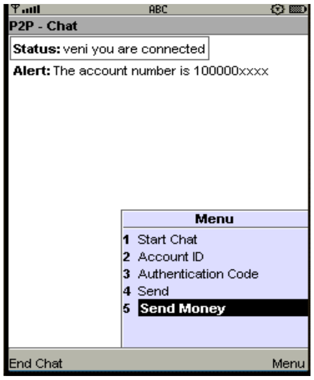
(j) Dharani receives the code



Status: dharani you are connected

Alert: The security code is verified and the user is valid and trusted user.

(k) An alert message to Dharani



Status: veni you are connected

Alert: The account number is 100000xxxx

(l) Veni receives accountID

Figure 6.2. Mobile payment scenarios

7. Conclusions and Future Work

This paper reports our current research efforts on developing the P2P-Paid system to support mobile phone users to conduct peer-to-peer wireless payment transactions. The P2P-Paid system provides both online payment and mobile peer-to-peer payment functions. It implements a 2-D wireless payment protocol which not only supports mobile payment transactions over a wireless Internet, but also supports wireless payment transactions between two mobile phones over a Bluetooth network. This paper reports the system architecture, design, payment protocol, and security strategy. Moreover, application examples of the first prototype are presented. The future work of this research is to develop and implement a lightweight speaker verification solution to support mobile user authentication and authorization for mobile payment transactions.

Acknowledgement

This research was conducted with the support of 2003 California Higher Education Grant from Intel Corp. for learning and study wireless technologies at anytime and anywhere. Many thanks to Krishnaveni Edunuru and Dharani Govindan for their implementation work, Intel's Jerry Kissinger for his support to San Jose State University, and Dr. Sigurd Meldal for his support to the Wireless Technology Laboratory.

References

1. H.M. Yunos, J Gao, and S. Shim, "Wireless Advertising's Challenges and Opportunities: IEEE Computer", Vol. 36, No. 5, May 2003.
2. J. Ondrus, and Y. Pigneur, "A Disruption Analysis in the Mobile Payment Market", Proceedings of the 38th Hawaii International Conference on System Sciences, 2005 (HICSS-38'05).
3. N.M. Sadeh, M-Commerce: Technologies, Services, and Business Models, Wiley, John & Sons, Inc., March 2002.
4. L. Antovski, and M. Gusev, "M-Payments", Proceedings of the 25th International Conference Information Technology Interfaces, 2003 (ITI'03).
5. K. Pousttchi, and M. Zhenker, "Current Mobile Payment Procedures on the German Market from the View of Customer Requirements", Proceedings of the 14th International Workshop on Database and Expert Systems Application, 2003 (DEXA'03).
6. S. Nambiar, and T.L. Chang, "M-Payment Solutions and M-Commerce Fraud Management", Retrieved September 9, 2004 from http://europa.nvc.cs.vt.edu/~ctlu/Publication/M-Payment-Solutions.pdf
7. X. Zheng, and D. Chen, "Study of Mobile Payments System", Proceedings of the IEEE International Conference on E-Commerce, 2003 (CEC'03).
8. S. Kungpisdan, B. Srivnivasan, and P.D. Le, "A Secure Account-Based Mobile Payment Protocol", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004 (ITCC'04).
9. Y. Lin, M. Chang, and H. Rao, "Mobile prepaid phone services", IEEE Personal Communications, 7(3): 6-14, June 2000.
10. A. Fourati, H.K.B. Ayed, F. Kamoun, and A. Benzekri, "A SET Based Approach to Secure the Payment in Mobile Commerce", In Proceedings of 27th Annual IEEE Conference on Local Computer Networks (LCN'02) November 06 - 08, 2002, Tampa, Florida.
11. D. Hennesy, "The Value of the Mobile Wallet", Retrieved on 2/16/2005 at: http://www.valista.com/downloads/whitepaper/mobile_wallet.pdf
12. Z. Huang, and K. Chen, "Electronic Payment in Mobile Environment", In Proceedings of 13th International Workshop on Database and Expert Systems Applications (DEXA'02) September 02 - 06, 2002. Aix-en-Provence, France.
13. J. Olsson, "Text Dependent Speaker Verification with a Hybrid HMM/ANN System", Retrieved January 5, 2005 from http://www.speech.kth.se/ctt/publications/exjobb/exjobb_jolsson.pdf.
14. D.A. Reynolds, T.F. Quatieri, and R.B. Dunn, "Speaker Verification Using Adapted Gaussian Mixture Models", Retrieved January 5, 2005 from http://www.cse.ohio-state.edu/~dwang/teaching/cis788/papers/Reynolds-dsp00.pdf.
15. D. Neiberg, "Text Independent Speaker Verification Using Adapted Gaussian Mixture Models", Retrieved January 5, 2005 from http://www.speech.kth.se/~neiberg/neiberg02mst.pdf.
16. T.B. Nordstrom, H. Melin, and J. Lindberg, "A Comparative Study of Speaker Verification Using the Polycost Database", Retrieved January 11, 2005 from http://www.speech.kth.se/ctt/publications/papers/icslp98_1359.pdf
17. S. Marinov, "Text Dependent and Text Independent Speaker Verification System: Technology and Application", Retrieved January 19, 2005 from http://www.speech.kth.se/~rolf/gslt_papers/SvetoslavMarinov.pdf.
18. N. Potlapally, S. Ravi, A. Raghunathan, and G. Lakshminarayana, "Algorithm Exploration for Efficient Public-Key Security Processing in Wireless Handsets", Design Automation and Test in Europe (DATE), March 2002.
19. N.R. Potlapally, S. Ravi, A. Raghunathan, and G. Lakshminarayan, "Optimizing Public-Key Encryption for Wireless Clients", IEEE International Conference on Communications (ICC), May 2002.