Mobile Banking and Payment System Using Bluetooth Media

Khey Banerjee¹, Md. Masud Rana, Md. Margoob Mahfuz, Md. Amjad Khan
Department of Electronics and Communication (ECE)
Khulna University of Engineering and Technology (KUET)
¹kheya2006@yahoo.co.in

Abstract— The considerable increase of mobile device users in recent years causes a strong demand on secured wireless bank services and reliable mobile commerce (m-commerce) applications. Since mobile payment (m-payment) & banking is a critical part of most wireless information services and mobile commerce applications, how to build secured m-payment systems becomes a research hotspot. This work presents an effective mobile payment system (MPS) in existing wireless insecure environments using mobile devices. The proposed framework provides a secure and convenient payment mechanism.

Index Term— Interactive voice response, Mobile payment system, Point of sale and Wireless access protocol.

I. INTRODUCTION
Bangladesh a fast-growing economy where the standard of living in the major urban centers has improved even faster than the overall growth rate. The financial sector of the economy is also evolving rapidly. Although debit cards and credit cards are just in beginning stage, cash continues to be the payment method of choice when consumers pay their monthly bills and pay for their purchases. The objective of this paper is to provide a secure banking & payment method using existing Bluetooth environment. Here a model for secure bank services is developed. We have used Bluetooth enabled mobile device to connect a client to a bank server & give services according to client’s database. When paying monthly bills for utilities and rent, consumers typically have two choices, either pay in cash or with a debit card, which often means standing in line or establish an “automatic payment” arrangement with a bank where the utility bills are debited against the account each month or use electronic banking. In this situation most of consumer choose the first one. Many medium and smaller merchants do not offer debit card payment because of the interchange fee and the cost of acquiring the point of sale (POS) terminals for debit card (and credit card) payment. Thus, cash is the primary payment method when consumers pay for their purchases. Mobile telephone is growing much faster than fixed-line telephone. This paper considers a proposal to develop a payment system that provides secure access to mobile subscribers’ bank accounts. This system would take advantage of the rapidly growing mobile telephone subscriber base to substitute for the use of debit cards in a lower cost manner. It also leads to increased use of electronic payment and decreased amount of waiting in line to pay bills.

II. MOBILE BANKING & PAYMENT SYSTEM
Mobile financial services are a term applied to a range of financial activities conducted using mobile devices, such as cellular phones or personal digital assistants. These activities fall into two broad categories: mobile banking and mobile payments. Mobile banking allows bank customers to check balances, monitor transactions, obtain other account information, transfer funds, locate branches or ATMs, and, sometimes, pay bills. The term mobile payment refers to payment transactions initiated or confirmed using a person’s mobile cellular phone or personal digital assistant. These may be such things as making a purchase at the point of sale, sending money to a person or a business, or purchasing a product or service remotely. [2][3]

A. Technologies behind Mobile Banking and Payment System

Technically speaking most of these services can be deployed using more than one channel. Presently, Mobile Banking is being deployed using mobile applications developed on one of the following four channels.

1. IVR (Interactive Voice Response)
2. SMS (Short Messaging Service)
3. WAP (Wireless Access Protocol)
4. Standalone Mobile Application Clients

IVR or Interactive Voice Response service operates through pre-specified numbers that banks advertise to their customers. Customer's make a call at the IVR number and are usually greeted by a stored electronic message followed by a menu of different options. Customers can choose options by pressing the corresponding number in their keypads, and are then
Mobile banking based on IVR has some major limitations that they can be used only for Enquiry based services. Also, IVR is more expensive as compared to other channels as it involves making a voice call which is generally more expensive than sending an SMS or making data transfer (as in WAP or Standalone clients).

SMS uses the popular text-messaging standard to enable mobile application based banking. The way this works is that the customer requests for information by sending an SMS containing a service command to a pre-specified number. The bank responds with a reply SMS containing the specific information. One of the major reasons that transaction based services have not taken off on SMS is because of concerns about security. The main advantage of deploying mobile applications over SMS is that almost all mobile phones are SMS enabled.

WAP uses a concept similar to that used in Internet banking. Banks maintain WAP sites which customer's access using a WAP compatible browser on their mobile phones. WAP sites offer the familiar form based interface and can also implement security quite effectively. [7][8] A WAP based service requires hosting a WAP gateway. Mobile Application users access the bank's site through the WAP gateway to carry out transactions, much like internet users access a web portal for accessing the banks services.

The following figure demonstrates the framework for enabling mobile applications over WAP. The actual forms that go into a mobile application are stored on a WAP server, and served on demand. The WAP Gateway forms an access point to the Internet from the mobile network.

Standalone Mobile Application Clients-Our implemented method is under this category. Standalone mobile applications are the ones that hold out the most promise as they are most suitable to implement complex banking transactions like trading in securities. They can be easily customized according to the user interface complexity supported by the mobile. In addition, mobile applications enable the implementation of a very secure and reliable channel of communication.

One requirement of mobile applications clients is that they require to be downloaded on the client device before they can be used, which further requires the mobile device to support one of the many development environments like J2ME. J2ME is fast becoming an industry standard to deploy mobile applications and requires the mobile phone to support Java.

The major disadvantage of mobile application clients is that the applications needs to be customized to each mobile phone on which it might finally run. J2ME ties together the API for mobile phones which have the similar functionality in what it calls 'profiles'.

Bluetooth Media-Bluetooth is an open standard specification for a radio frequency (RF)-based, short-range connectivity technology that promises to change the face of computing and wireless communication. It is designed to be an inexpensive, wireless networking system for all classes of portable devices, such as laptops, PDAs (personal digital assistants), and mobile phones. It also will enable wireless connections for desktop computers, making connections between monitors, printers, keyboards, and the CPU cable-free.

A complete Bluetooth system will require these elements:
- An RF portion for receiving and transmitting data
- A module with a baseband microprocessor
- Memory
- An interface to the host device (such as a mobile phone)

This basic system will vary, however, depending on whether the Bluetooth module is independent of the host or embedded. The RF portion can be implemented as a module or as a single chip. A module includes a short-range radio transceiver, an
external antenna, and a clock reference (required for synchronization).

Bluetooth is essentially a networking standard that works at two levels:

- It provides agreement at the physical level
- It provides agreement at the protocol level, where products have to agree on when bits are sent, how many will be sent at a time, and how the parties in a conversation can be sure that the message received is the same as the message sent.

The big draws of Bluetooth are that it is wireless, inexpensive and automatic. The older Bluetooth 1.0 standard has a maximum transfer speed of 1 megabit per second (Mbps), while Bluetooth 2.0 can manage up to 3 Mbps. Bluetooth 2.0 is backward-compatible with 1.0 devices.

Bluetooth networking transmits data via low-power radio waves. It communicates on a frequency of 2.45 gigahertz (actually between 2.402 GHz and 2.480 GHz, to be exact). This frequency band has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM).

One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of about 1 milliwatt. By comparison, the most powerful cell phones can transmit a signal of 3 watts. Even with the low power, Bluetooth doesn’t require line of sight between communicating devices.

Bluetooth can connect up to eight devices simultaneously. With all of those devices in the same 10-meter (32-foot) radius, one might think they’d interfere with one another, but it’s unlikely. Bluetooth uses a technique called spread-spectrum frequency hopping that makes it rare for more than one device to be transmitting on the same frequency at the same time. In this technique, a device will use 79 individual, randomly chosen frequencies within a designated range, changing from one to another on a regular basis. In the case of Bluetooth, the transmitters change frequencies 1,600 times every second, meaning that more devices can make full use of a limited slice of the radio spectrum. Since every Bluetooth transmitter uses spread-spectrum transmitting automatically, it’s unlikely that two transmitters will be on the same frequency at the same time.

Bluetooth is a standard communications protocol primarily designed for low power consumption, with a short range (power-class-dependent: 100m, 10m and 1m, but ranges vary in practice; see table below) based on low-cost transceiver microchips in each device.

<table>
<thead>
<tr>
<th>Class</th>
<th>Maximum Permitted Power (mW)</th>
<th>Range (approximate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>100 mW</td>
<td>20 dBm</td>
</tr>
<tr>
<td>Class 2</td>
<td>2.5 mW</td>
<td>4 dBm</td>
</tr>
<tr>
<td>Class 3</td>
<td>1 mW</td>
<td>0 dBm</td>
</tr>
</tbody>
</table>

III. PROPOSED BANKING & PAYMENT METHOD

In countries like Bangladesh, where internet speed is low, lot of congestion in peak hour, payment method using SMS, WAP are not suitable. Here we have proposed a method that uses Bluetooth as a media. The proposed method uses Java components to provide end-to-end client authentication & data confidentiality between wireless J2ME based clients & J2EE based servers. This section presents system model, security solutions for payment system & functioning of scheme.

A. System Model

Our proposed system model is given below. Here a bank server is store house of all transaction information. Client is connected to server via Bluetooth connection. There is an application running on client’s mobile device. The application is based on J2ME. There is software running on server which is connected to bank database. [1][9]

The purpose of mobile application is to send request to the server to perform payment activities such as: current balance, balance transfer, last transaction date, bill payment etc.

![Client-Server System model](image-url)
B. Flow chart

![Flow chart of system model](image)

C. Detailed Pictorial Description of the system [11][12]

Server Search—First of all client who wants to be connected to bank server should have an account in the bank database. When clients want to be connected with bank database first he/she has to find the bank server using Bluetooth connection.

Fig. 4. Searching Bank Server (client side)

Fig. 5. Waiting for client (Server side)
After finding a server client send a request to connect with server. Server then check the client’s mobile device address i.e. Bluetooth address in its database as it is eligible to be connected or not. If client mobile device address is in server database, client gets connected.

Account verification—After connected to server client account will be verified with client account ID & password. If the account ID & password match with bank database then client will be permitted for further processing. It’s also preventing hacker’s to enter into the service.

Service Query—After verification is success, client can access the service given by bank server. Suppose the bank server give the services like Account Information, Last Transaction Date, Bill Payment and Bank Offers. Then the scenario will be just like below.
After receiving request from a client, bank server search the service in database corresponds to client account. For example if client wants to get account information then server search account details correspond to client account & send it client’s mobile device.

Bill Payment: To pay bill, a client just need to know the recipient account number. Then client select Bill Payment option & then enter the recipient account number & amount of bill, then the amount will be transferred into that account.

IV. ADVANTAGES AND DISADVANTAGES OF THE PROPOSED SYSTEM AND IT’S SOLUTIONS

The biggest advantage that mobile banking offers to banks is that it drastically cuts down the costs of providing service to the customers. The customers can check their balance on the phone and authorize the required amounts for payment. The customers can also request for additional information. There are number of reasons that should persuade banks in favor of mobile phones.
They are set to become a crucial part of the total banking services experience for the customers. Also, they have the potential to bring down costs for the bank itself. Such messages also bear the virtue of being targeted and personal making the services offered more effective. They will also carry better results on account of better customer profiling. [10][13]

Yet another benefit is the anywhere/anytime characteristics of mobile services. A mobile is almost always with the customer. As such it can be used over a vast geographical area. The customer does not have to visit the bank ATM or a branch to avail of the bank’s services. As such with mobile services, a bank will need to hire even less employees as people will no longer need to offer phone based credit systems. This will make credit cards redundant and also aid in checking credit card fraud apart from enhanced customer convenience. The use of mobile technologies is thus a win-win proposition for both the banks and the bank’s customers. The banks add to this personalized communication through the process of automation. For instance, if the customer asks for his account or card balance after conducting a transaction, the installed software can send him an automated reply informing of the same. These automated replies thus save the bank the need to hire additional employees for servicing customer needs.[4][5][6]

Bluetooth Vulnerabilities and Security Risks

• Blue-jacking is the process of sending unsolicited messages, or business cards, to Bluetooth-enabled devices. This does not involve altering any data from the device, but nonetheless, it is unsolicited. Devices that are set in non-discoverable mode are not susceptible to blue-jacking.

• Blue-snarfing is a method of hacking into a Bluetooth-enabled mobile phone and copying its entire contact book, calendar or anything else stored in the phone’s memory. By setting the device in non-discoverable, it becomes significantly more difficult to find and attack the device.

• The backdoor attack involves establishing a trust relationship through the pairing mechanism, but ensuring that it no longer appears in the target’s register of paired devices. In this way, unless the owner is actually observing their devices at the precise moment a connection is established, they are unlikely to notice anything untoward, and the attacker may be free to continue to use any resource that a trusted relationship with that device grants access to. This means that not only can data be retrieved from the phone, but other services, such as modems, or Internet, WAP and GPRS gateways may be accessed without the owner’s knowledge or consent.

• The virus is malicious software that uses Bluetooth technology to seek out available Bluetooth devices and send itself to them. Furthermore, the user has to manually accept and install the malware in order to infect the phone.

The modification required to allow client in online banking:

If any client wants to do online banking, the software of mobile need to modified to allow client to connect with online banking using GPRS or other network.

The modification of Bluetooth authentication scheme to remove security threats:

From a analysis [14] its append that both users & Bluetooth application developers have responsibilities & opportunities to minimize the risk of compromise via Bluetooth.

User should follow these best practice security guidelines:

- Enable Bluetooth functionality only when necessary.
- Keep device as close together as possible when Bluetooth links are active.
- Independent monitor devices & links for unauthorized Bluetooth activity.
- Make devices discoverable only when it is necessary.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.
- Use device firewalls, keep device anti-virus software up to date.
- Use mixed key letter/number as password

Bluetooth application developers should consider designing to the following guidelines:

- Passkeys should be at least eight digits long. Passkeys must not be valid indefinitely.
- Require authorization for all incoming connection requests, & don’t accept connections, files or other objects from unknown & not-trusted sources.
- Use non-descriptive Bluetooth device names on each device & identify all paired & connected Bluetooth device by hardware (MAC) address.
- Program each device to initiate authentication immediately after the initial establishment of the Bluetooth connection.

Prohibit the user from changing or controlling Bluetooth security features.

V. CONCLUSION

The improvisation of mobile payments will make possible new and unforeseen ways of convenience and commerce. Unsuspected technological innovations are possible when mobile payments become feasible and ubiquitous. However there are concerns about usefulness, acceptable applications, security, usability and reliability of this technology. The range of Bluetooth communication can be further increased. It is on research how to increase range up to an acceptable distance. For convenience of Bluetooth application, network security is a hand-off. Vendors, those providing services may implement costly infrastructure for security. But different demography showed that consumers are willing to pay for better convenience.

REFERENCES


Java™ 2 Platform, Enterprise Edition Technical Overview (J2EE Overview).


Deitel & Deitel, “Java How To Program”.

James Keogh, “The complete Reference J2ME”.


Systems and Network Analysis Center Information Assurance Directorate www.nsa.gov/snac