Chapter IX

M-Payment Solutions and M-Commerce Fraud Management

Seema Nambiar, Virginia Tech, USA
Chang-Tien Lu, Virginia Tech, USA

Abstract

Mobile security and payment are central to m-commerce. The shift from physical to virtual payments has brought enormous benefits to consumers and merchants. For consumers it means ease of use. For mobile operators, mobile payment presents a unique opportunity to consolidate their central role in the m-commerce value chain. Financial organizations view mobile payment and mobile banking as a way of providing added convenience to their customers along with an opportunity to reduce their operating costs. The chapter starts by giving a general introduction to m-payment by providing an overview of the m-payment value chain, lifecycle and characteristics. In the second section, we will review competing mobile payment solutions that are found in the marketplace. The third section will review different types of mobile frauds in the m-commerce environment and solutions to prevent such frauds.

Introduction

Mobile commerce (m-commerce) grows dramatically. The global m-commerce market is expected to be worth a staggering US$200 billion by 2004 (Durlacher Research, n.d.; More Magic Software, 2000). M-commerce can be defined as any electronic transaction or information interaction conducted using a mobile device and mobile networks, for example, wireless or switched public network, which leads to transfer of real or perceived value in exchange for information, services or goods (MobileInfo.com). M-commerce involves m-payment, which is defined as the process of two parties exchanging financial value using a mobile device in return for goods or services. A mobile device is a wireless communication tool, including mobile phones, PDAs, wireless tablets, and mobile computers (Mobile Payment Forum, 2002).

Due to the widespread use of mobile phones today, a number of payment schemes have emerged which allow the payment of services/goods from these mobile devices. In the following sections an overall view of the m-payment value chain, the m-payment life cycle and the m-payment characteristics is given. Also the operational issues are analyzed, which are critical to the adoption level of a payment system. The operational issues or characteristics will help in the unambiguous identification of the payment solutions.

M-Payment Value Chain

Many different actors can be involved in mobile payment process (McKitterick & Dowling, n.d.; Mobile Payment Forum, 2002). For example, there is a consumer who owns the mobile device and is willing to pay for a service or product. The consumer initializes the mobile purchase, registers with the payment provider and authorizes the payment. A content provider or merchant sells product to the customer. In the mobile payment context, content can range from news to directory services, shopping and ticketing services, entertainment services, and financial services. The provider or merchant forwards the purchase requests to a payment service provider, relays authorization requests back to the customer and is responsible for the delivery of the content. Another actor in the payment procedure is the payment service provider, who is responsible for controlling the flow of transaction between mobile consumers, content providers and trusted third party (TTP) as well as for enabling and routing the payment message initiated from the mobile device to be cleared by the TTP. Payment service provider could be a mobile operator, a bank, a credit card company or an independent payment vendor. Another group of stakeholders is the trusted third party, which might involve network operators, banks and credit card companies. The main role of the TTP is to perform the authentication and the authorization of transaction parties and the payment settlement.

Finally there are mobile operators who are more concerned with the standardization and interoperability issues. They may also operate mobile payment procedure themselves and provide payment services for customers and merchants. One thing that needs to be considered is who receives the customer data. Customers rarely wish to divulge any information, whereas the same customer information might be important for merchants or content providers for their business. Payment procedures need to ensure that none

of the players receive the data, for example, when customers use a prepaid payment solution to buy goods but also need to require divulging customer information to any of the players considered.

M-Payment Lifecycle

Payment transaction process in a mobile environment is very similar to typical payment card transaction. The only difference is that the transport of payment detail involves wireless service provider. WAP/HTML based browser protocol might be used or payment details might be transported using technologies such as blue tooth and infrared (Mobile Payment Forum, 2002).

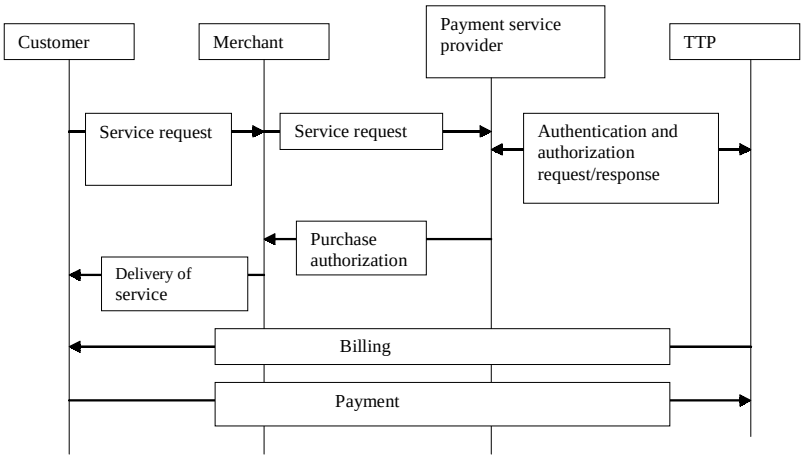
Mobile payment lifecycle shown in Figure 1 includes several main steps (Telecom Media Networks, 2002):

1. *Registration*: Customer opens an account with payment service provider for payment service through a particular payment method.
2. *Transaction*: Four steps are identified in an m-payment transaction.
   (a) Customer indicates the desire to purchase a content using a mobile phone button or by sending an SMS (short message service).
   (b) Content provider forwards the request to the payment service provider.
   (c) Payment service provider then requests the trusted third party for authentication and authorization.
   (d) Payment service provider informs content provider about the status of the authentication and authorization. If customer is successfully authenticated and authorized, content provider will deliver the purchased content.
3. *Payment settlement*: Payment settlement can take place during real-time, prepaid or postpaid mode (Xiaolin & Chen, 2003). A real-time payment method involves the exchange of some form of electronic currency, for example, payment settlement directly through a bank account. In a prepaid type of settlement customers pay in advance using smart cards or electronic wallets. In the post-pay mode, the payment service provider sends billing information to the trusted third party, which sends the bill to customers, receives the money back, and then sends the revenue to payment service provider.

Operational Issues in M-Commerce Payment

Payment schemes can be classified as account based and token based. In the account-based scheme, consumers are billed on their account. This scheme is not suitable for small value transactions. In the token-based scheme, a token is a medium of payment transaction representing some monetary value and requires the support of the payment

Figure 1. M-payment life cycle



provider or TTP. Customers have to convert the actual currency to tokens. There are three different billing methods. One is real time, in which some form of electronic currency is exchanged during the transaction. The payment settlement can also be prepaid where customers pay in advance to have a successful transaction. Another method is the postpaid method in which customers pay after they receive the service/good.

Customers will choose a new payment method only if it allows them to pay in an accustomed method. The different payment settlement methods offered by the provider will hence play a crucial role. Based on payment settlement methods, the payment solutions can also be categorized as smart and prepaid cards solution, electronic cash or digital wallets solution, direct debiting and off-line-procedure solution, and credit cards and payments via the phone bill solution. In the payment using smart card or prepaid card solution, customers buy a smart card or prepaid card where the money-value is stored and then pay off for goods or services purchased. Customers can also upload a digital wallet with electronic coins on a prepaid basis. The smart cards, prepaid cards and digital wallets are thus used for prepaid payment solution. Another form of payment settlement is direct debit from the bank, which is a real-time payment method, since the purchase amount will be deducted as soon as the customer authorizes the payment. Payment method can also be using the phone bill or the credit card, where the customer pays for the good or services purchased at a later time. Payment by phone bill is one of the simplest methods of payment in which a special merchant-specific phone number is called from the mobile phone, which causes a predefined amount to be billed to callers' telephone bill. These types of payment schemes are applicable only to a single payment amount, providing limited security, and requiring users and merchants to share the same mobile operator (Pierce, 2000).

Smart cards can be used for all the three types of payment methods, for example, credit, debit and stored value as well as in authentication, authorization and transaction

processing (Shelfer & Procaccino, 2002). A smart card thus enables the storage and communication of personal information such as value of goods and identity. A smart card can be either a memory card or processing enabled card. Memory cards are one type of prepaid cards, which transfer electronic equivalent of cash to the merchant electronic register. Processor cards, on the other hand, can be used as a debit card, credit card or a stored value card. A major drawback is the large costs associated with replacement of the existing infrastructure. In addition, the model lacks technical interoperability among existing smart card architectures.

The adoption of various payment frequencies in payment process is also a critical factor to make m-commerce payment succeed. It can be pay per view where consumers pay for each view, or increment, of the desired content; for example, downloading Mp3 files, video file or ring tones. It can also be pay per unit, where consumers pay once for each unit successfully completed with the content provider. A consumer would spend a certain number of units during each session, which is subsequently billed to the customer; for example, customer participating in an online game. The third type is a flat rate payment where consumers pay a recurring amount to access content on an unlimited basis for a certain period of time; for example, customer being charged to have access to an online magazine (McKitterick & Dowling, n.d.). The success of a payment solution will also depend on whether it can pay for a wide range of products and services. The payment can be a micro-payment, which refers to a payment of approximately $10 or less. In a micropayment system the number of transactions between each payer and the merchant is large as compared to the amount of each individual transaction. As a result transaction-processing cost grows for such systems. This kind of setting is addressed by a subscription scheme where a bulk amount is paid for which the use of a service is bought for a certain period of time. Traditional account based systems are not suitable for these kinds of transactions and hence the need for third-party payment processors arises which accumulate the transactions that can be paid for at a later time. The payment can also be macro-payments, which refers to larger value payments such as online shopping. It is also important to consider the technical infrastructure required by the customers to participate in a payment system (Krueger, 2001; Mobey Forum Mobile Financial Services Ltd, 2001). Some solutions do not require any changes to the hardware or software, which will then have a trade-off on the security aspect of payment. Some solutions require a sophisticated technology, which may be very secure but may not have taken the user's convenience into consideration. Most current payment solutions are SMS or WAP (Wireless Application Protocol) based. Some of the solutions use dual chip. In addition to SIM (Secure Identification Module), a second chip, such as WIM (Wireless Identity Module), standard smart cards and memory flash cards, is integrated into mobile device to provide the security functionality. The dual slot technology can also be used for payment services. This technology uses a regular SIM-card to identify the mobile device and also provide a second card slot for a credit or debit card integrated within a mobile phone. Payment solutions relying on an external chip card reader, which is connected to the mobile terminal using Bluetooth, infrared technologies or a cable, also come under the dual slot category.

In addition, software based payment solutions have been considered. A software agent based wireless e-commerce environment has been proposed (Maamar et al., 2001), called Electronic Commerce through Wireless Devices (E-CWE). The environment associates

users with user-agents, embodies user-agents with personalization and mobility mechanisms, and relates providers to provider-agents. Initially a J2ME application has to be downloaded which provides the interface to credit card information, including merchant and payment data. Then credit information is posted via HTTPS connection to the payment service provider. All business logic is fetched from the Web server and usually no new software or hardware is required on the device.

Mobile Payment Systems or Solutions

This section will portray current mobile payment solutions and compare them from user perspective of cost, security and convenience. The Electronic Payment Systems Observatory (ePSO) identified over 30 different mobile payment solutions, each with its own particular set of technologies (ePSO, n.d.). Mobile operators provide many solutions: some by financial players and others involving alliances between operators and financial organizations. Most of the solutions involve a relatively similar process.

Existing mobile solutions are categorized based on the payment settlement methods that are prepaid (using smart cards or digital wallet), instant paid (direct debiting or off-line payments), and post paid (credit card or telephone bill). The three payment settlement options may vary in their requirements, process of payment and technologies used. The only requirement to a prepaid type of payment solution is a PIN for authorizing a transaction and a smart card value or stored value card for making payment. The technological requirements range between just a mobile phone to a smart card with a dual slot phone and smart card reader. The payment procedure starts with customers selecting a product or service and the mode of payment. Next, customers authorize the transaction using PIN number and then the payment amount is deducted from the stored value card.

Payment solutions based on payment direct from credit or bank accounts require an agreement between customer and payment provider that authorizes the payment provider to divulge the customer information to merchant and charge the customer. Customers have to divulge their credit card information or bank account number to payment service providers. The transaction also requires a PIN or a password. The technologies in use today for this type of solutions are a dual slot phone with a smart reader, dual chip phones (SIM+WIM), and payment provider calling back the customer's mobile phone. In general the solutions in this category follow the same high-level process. Customers select a product or service and the payment mode and authorize the transaction by entering a PIN or password. The payment provider forwards the card/bank information to the merchant. The payment amount is deducted from bank account or credited to customers' account and paid to the merchant.

The solutions based on charging the customer through phone bill require an agreement between customer and payment provider to charge the customer's phone bill. Such solutions require infrared or bluetooth technologies for establishing connection to the point of sale. In some cases a premium rate is enough. If the mobile phone uses a bluetooth/infrared technology, the point of sale contacts the mobile phone using the technology. Customers will then choose the product or service and authorize the

payment with a button click on the mobile phone. Subsequently, the amount is charged to the phone bill. If the mobile phone uses just a premium rate to select a product or service, the mobile network calls the point of sale to authorize the sale and subsequently the amount is charged to the phone bill.

The following section portrays some current payment solutions such as Paybox, iPIN, m-PayBill, m-Pay and Jalda. A general analysis of the payment solutions based on customer requirements of cost, security and convenience is also provided.

Payment Solutions

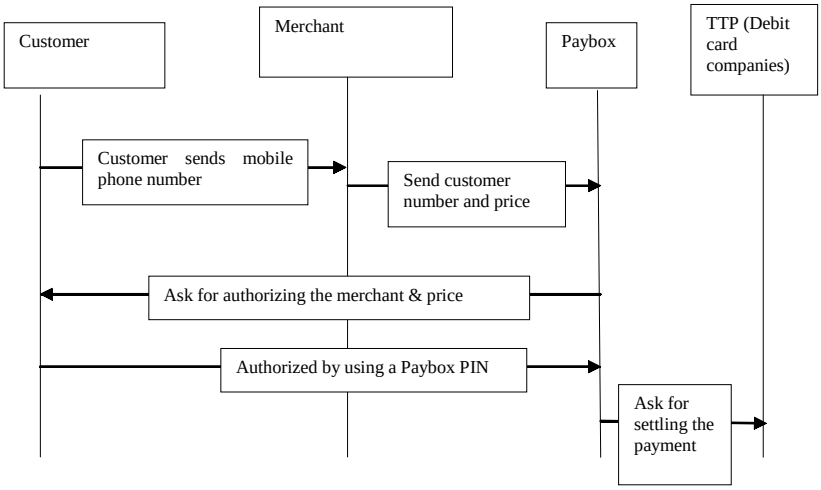
Paybox

One of the most widespread mobile phone payment applications is Paybox (Paybox.net, 2002), which was launched in Germany in May 2000. Later it was launched in Austria, Spain, Sweden and the UK. This service enables customers to purchase goods and services and make bank transactions via mobile phone. The value of purchases or credit transfers is debited from customers' bank account. The infrastructures needed to use Paybox are a mobile phone, a bank account and a paybox registration. A typical real-world mobile transaction using Paybox is given in Figure 2. Customers send their phone number to a merchant. The merchant communicates this phone number and the price. The Paybox system calls the customer and asks for payment authorization. Payers authorize by their PIN. Paybox informs the trusted third party to settle the payment.

The Paybox is very simple and easy to use because of the very limited infrastructures needed and only costs a small annual fee for customers. M-payment is independent. For example, it allows services to customers of any bank or mobile operator. A key advantage of the independent payers is that they enable every mobile user to use the service upon registration, regardless of their mobile service provider. This independency of Paybox is also helpful to merchants since teaming up with such a payer is more efficient than teaming up with three or more separate mobile operators. Paybox also promises to provide a fraud protected cost effective system. The disadvantages are that the operation of Paybox is expensive since the system has to make voice calls using integrated voice recognition system (IVR) to the customer, which could range over various durations. In addition, there is no data privacy and customer and merchant have no proof of transaction, which might be a possible cause of fraud. The high latency also restricts it to high value transactions (Fischer, 2002). Most of all the transaction can be done only using a GSM enabled phone.

An annual fee is charged to customers, but there is no transaction fee involved. Paybox can be used with any mobile phone. Hence infrastructure costs are low. Peer to peer transactions come with an extra cost. Customers need to know only the PIN number to participate and the IVR system will then guide them through the rest of the payment process. Processing of transactions is fast. Paybox is suitable for macro as well as small payments. Paybox can also be used for peer-to-peer transactions where customers can send and receive money to other participants. Paybox owns customers' data and does not give the personal data to any other parties involved in the process. However, one

Figure 2. Paybox transaction



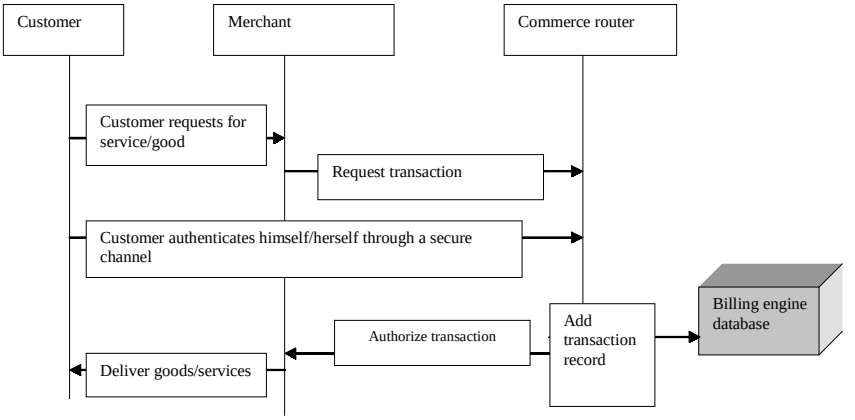
drawback is that both customers and merchants do not have any proof of the transaction. Some fraud prevention techniques are promised by Paybox (Paybox.net, 2001), including address checking and correction using fuzzy logic tools, using checksums for credit card numbers and bank account numbers, checks on the demographic data, credit history checks, and address verification by sending the final PIN.

iPIN

iPIN is a privately held corporation based in Belmont, CA (USA) (ePSO, n.d.; Cap, Gemini, Ernst &Young, 2002). iPIN's Enterprise Payment Platform (EPP) is a leading end-to-end electronic and mobile commerce payment technology. It allows virtual point of sale and peer-to-peer payments over fixed as well as wireless networks. Seven software components have been identified in iPIN (Cap, Gemini, Ernst &Young, 2002). The main component of the iPIN payment system is the commerce router, which manages transactions throughout the payment lifecycle. It serves the user-interface pages and manages all end-user customer account activity. The repository is used for managing configurations and merchant information. Billing engine does the transaction fee calculation and facilitates account settlement. The merchant POS controller connects to the merchant's point of sale. The payment gateway connects to financial providers such as banks and credit card companies. The business intelligent module of iPIN keeps track of the success and returns on investments. The usage of the iPIN multiple payment instruments enables a customer to choose prepaid, debit or credit solution.

A typical transaction using the iPIN payment system is shown in Figure 3. Customers initiate purchase requests to merchant. The merchant sends an authorization request to

Figure 3. Transaction in an iPIN payment solution



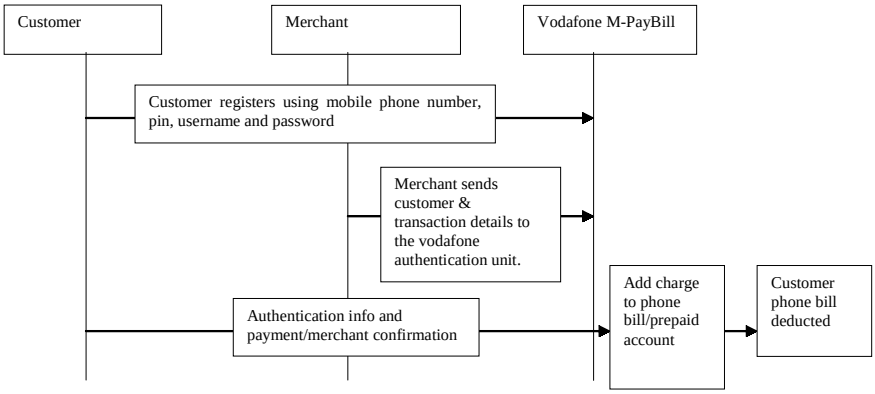
the issuer's commerce router. Customers are redirected to the commerce router for authenticating themselves after a secure session is established with the commerce router. After successful authentication is complete, the commerce router authorizes the transaction. Then the router establishes a transaction record in the database and sends the authorization response to the merchant. The merchant then sends a clearing message to the commerce router, confirming the transaction.

iPIN offers users a secure and efficient way to purchase virtual goods and services with a variety of connected devices including Web, WAP, SMS and IVR. Throughout the purchase process, the enterprise houses the user's personal profile and guarantees payment to merchants without actually transferring customers' private financial information. Fees are based on transactions. There is no setup fee for the customer. The only effort by consumers is to open or activate an account. Users are afforded several payment options including micro payment, and can choose to associate these charges to a prepaid account, monthly bill, and bankcard or loyalty program. Available via a mobile handset, self-care tools let users access detailed transaction histories, set account preferences such as spending limits and preferred account details, and receive answers to frequently asked questions. iPIN provides for interoperability between a group of individual payment networks, allowing merchants from one network to sell to users from other networks, while giving users access to a larger group of merchants and products.

Vodafone m-PayBill

m-PayBill supports virtual POS for micro and small payments (ePSO, n.d.; Vodafone M-Pay bill, n.d.). The bill is charged to customers' phone bill or from the prepaid airtime. The requirements for this payment solution are a WAP phone or a Web browser to settle the payment. Figure 4 shows a typical micro payment transaction using Vodafone. The Vodafone customers register for m-PayBill online by entering their mobile phone number,

Figure 4. Transactions in Vodafone-mPayBill solution



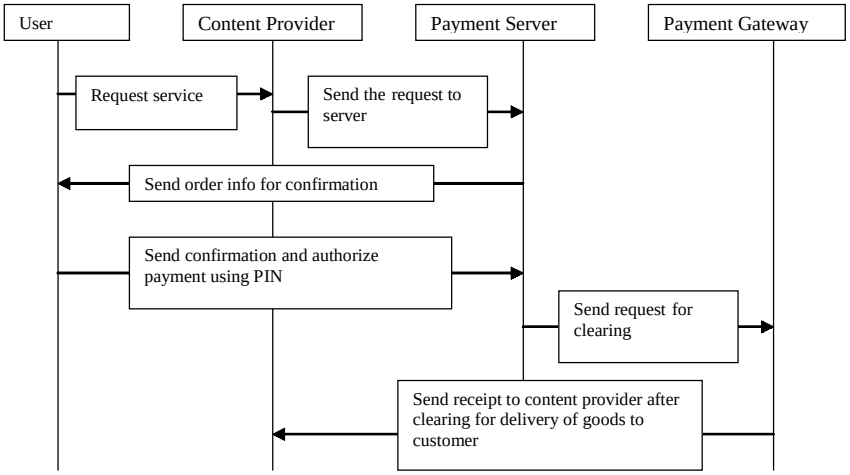
choosing a username, a password, and a four-digit PIN. When using a WAP phone the user is asked to enter the PIN for identification. Purchase amount is then charged to the phone bill or deducted from prepaid airtime.

m-PayBill membership is free; there are no basic or transaction fees. No extra infrastructure needed to perform the transaction except for a WAP phone. m-PayBill provides interoperability by having service providers outside of European Union plus Norway, Iceland and Liechtenstein. The personal information is transferred to the service providers in other countries for purchases outside the European Union. The security of the information will then depend on the privacy policy of that country. Payment information is maintained on the server and does not change hands, thus preventing any chances of fraud. The process is basically easy to understand and provides faster transactions. Customers already registered with the Vodafone network operator need not register again to use the procedure. Payment solution, however, is only applicable to micro-payments.

m-Pay

m-Pay is a mobile payment solution developed in corporation between PBS, Orange and Gem plus (PBS ,n.d.). It is a server-based credit/debit card payment solution via mobile phone for goods ordered via telephone sales and on the Internet through the PC or a WAP mobile phone. To use this application the user sends a written application to Orange asking to link the payment data to the GSM data in a payment server. Activating the payment function on the mobile phone requires an individually allocated PIN-code, which is connected to the SIM-card in the mobile phone. A typical transaction using m-Pay is given in Figure 5.

Figure 5. Payment transaction in an m-Pay solution



Customers request a service or product from the content provider. This request in the form of an SMS message is sent to payment server, which takes care of authorizing the payment request. Payment server sends the order information to customers for confirmation, which customers do by using a personal identification number presented in the SIM card. The server will then translate the mobile phone number into a valid card number and conduct a debit/credit card transaction. This confirmation is sent to the payment gateway for clearing, after which a receipt is generated by the gateway and sent to the content provider.

Customers must first register with Orange to use m-Pay. The registration is free but a new "Orange" SIM card required and payment confirmation service provided comes with a cost. An advantage with regards to cost is that customers need not buy new handsets to use the solution. None of the sensitive information is put on air. A payment receipt will be sent, whereupon customers receive notification in the form of an SMS message. The payment is carried out by exchange of e-payment certificates. The PBS payment server verifies any transaction from the SIM card, which ensures that the merchant is approved to trade and also that the card has not been reported stolen or stopped from further transactions. To use this payment application, users have to download a script over the air to activate the dormant payment application in their SIM card. The payment transaction will take less than 10 seconds. After the PIN code has been accepted by the SIM application, customers are able to buy airtime and the amount will automatically be drawn from their credit/debit card account.

Jalda

Jalda is an account-based system wherein both consumers and retailers are connected to a special account managed by a payment provider, who usually acts as the certificate authority (Dahlström, 2001; ePSO, n.d.). For payments using mobile phones, the certificate is stored centrally with the payment provider. Users authorize a transaction through a PIN-code. It can also be used for Internet transactions, in which case the certificate is stored in the hard drive. Jalda is a session-based Internet payment method that enables payment by the second, item, quantity, mouse click, search, character, page, or practically any other parameters. Jalda consists of two parts: an application program interface (API) and a payment server that administers user data and keeps track of transactions. The Jalda actors are consumers who use Jalda API applications to purchase via the mobile phone and the content provider who uses the Jalda API to charge consumers for service.

The system enables customers to be charged by whatever parameter the content provider desires. The content provider deducts a small transaction fee from the customer phone bills. The infrastructure required is a WAP phone. Security of payments is guaranteed by using strong authentication and non-repudiation protocols. Self-administration interface enables users to control their account. A payment receipt is sent to users, which may be stored in the WAP phone. Jalda is an account-based payment method, enabling both prepaid and credit-based payments. The accounts are managed and held by the payment provider and the payment provider usually acts as the certificate authority. Jalda can also be used for normal payments as well as micro-payments. The Jalda micropayment protocol is based on a concept of a payment session that is initiated by the payer by accepting and electronically signing a session contract with the merchant. The payment provider will then verify the contract for the vendor. After successful verification the vendor can then start keeping track of the service used by sending periodic indications when the consumer is consuming the service.

Jalda supports interoperability but does not enforce it as a global standard. Hence two payment providers need to make an agreement before the respective users can purchase goods from the other payment provider's merchants.

Other Solutions

Nokia launched a dual chip solution called EMPS (Electronic Mobile Payment Services). One chip was a usual SIM (subscriber identity module) card and the other was a WIM (WAP Identity module) for making mobile payments. Parkit is used in some cities of Finland to pay for parking. In this solution a service number of the parking area is called after which parking is registered and customers end the parking by calling again to a nationwide "ending number". The parking fee will be included on customers' telephone bill, credit card bill or a separate bill.

Table 1.The categorization of payment solutions

Payment Solutions	Instant Paid	Prepaid	Postpaid
Paybox	X		
IPIN	X	X	X
m-PayBill		X	X
m-Pay	X		X
Jalda		X	X

Table 2. Summary of the payment solutions

Payment Model	COST	CONVENIENCE	SECURITY
Paybox	An annual fee is charged to customer, but no transaction fee involved. Peer-to-peer transaction comes with extra cost. Infrastructure costs are low.	Useful for macro, micro and peer-to-peer transactions. Customer required to know only the PIN number to participate.	Customer personal data kept in the Paybox server and not exchanged with other participants. Fraud prevention techniques employed.
iPIN	No setup fee. Fees are based on transactions. Infrastructure costs are low.	Several payment options including micro-payments are offered. Interoperability between groups of individual payment networks is provided.	Enterprise houses users' personal data and guarantees privacy.
Vodafone m-PayBill	Membership free. No basic or transaction fees. Infrastructure cost does not exist except that the customer might require a WAP enabled phone.	Only applicable to micro-payments. Payment process is more customer friendly. Customer registered with Vodafone operator can automatically use the solution.	Interoperability between various countries is provided, but requires transfer of personal information. The privacy of the data will depend on the countries' privacy policy.
m-Pay	Registration is free. A new Orange SIM card is needed, which comes with a cost. Payment confirmation is also provided with a cost.	Customers need to download a script to activate applications on SIM card. Payment transaction is fast.	Payment carried out by exchange of certificates. Customer receives payment confirmation in the form of SMS. Server verifies every transaction from SIM card
Jalda	Content provider charges a small transaction fee from customers' phone bills. The customer might require a WAP enabled phone.	It can be used for normal as well as micro-payments, and supports interoperability but has not been enforced as a global standard.	Usage of strong authentication and non-repudiation protocols guaranteed. Payment receipt sent to user.

General Analysis of the Payment Solutions

Payment solutions can be categorized on the basis of the payment settlement methods, which are instant-paid, postpaid, prepaid or a combination of these. In the prepaid solution, customers buy a smart card where the amount equivalent is stored and then pay of this for goods or services desired. Subscription of services can also be considered as prepaid type of payment. The prepaid type of solutions allows privacy to users since at

no point of the process is it required to disclose any personal data. The instant paid solution is that payment settlement is done as soon as users confirm the payment as in direct debiting systems. In the postpaid solution customers pay for goods or services later. Payment by credit card and phone bill is an example. Table 1 shows this categorization for Paybox, iPIN, m-PayBill, m-Pay and Jalda.

The key to the acceptance of a mobile payment procedure is in the hands of customers. The determinants affecting the adoption of a payment solution are cost, security and convenience. Cost includes direct transaction cost, fixed cost of usage and cost for technical infrastructure on the part of the customer. *Security* is evaluated by confidentiality of data and confirmation of the payment. *Convenience* means ease, comfort, fast processing and number of accepting merchants and interoperability. Table 2 gives a summary of the payment solutions based on the customer requirements.

Fraud Management Systems in M-Commerce

Fraud is defined as access or usage of the network with the intent of not paying for the service accessed. It can be either external or internal to the operator's network, and often involves both. Telecommunication fraud is estimated at 22 billion US dollars (USD) per year and growing annually at 2 billion USD (18 billion to fixed line fraud and 4 billion attributed to cellular). The convergence of voice and data communications, which has been driven by the tremendous uptake of the Internet and mobile phone ownership, has made fraud a high priority item on the agenda of most telecommunication operators. The advent of e-commerce activity further compounds the problem as industry analysts predict phenomenal growth in e-commerce over the next 3 years, with 40% of all e-commerce transactions expected to occur using mobile devices such as phones and personal assistants.

Many mobile payment solutions failed since they were unable to accumulate critical user mass. Merchants and consumers expressed their distrust in the electronic payment systems (Dahleberg & Tuunainen, 2001). The possible modes of fraud that will be experienced within m-commerce payment activity will encompass frauds related to security breaches in the underlying payment model, as well as in the underlying carrier network. A number of technologies are being used to prevent and detect these kinds of frauds. The frauds that can occur in the m-commerce environment have thus been categorized as mobile phone fraud, mobile network fraud and fraud specific to the m-commerce transaction process.

Mobile Phone Fraud

Criminals and hackers have devoted time and money to develop and refine their techniques, applying them to mobile phones as well. Not only is mobile phone fraud

profitable, the stolen handsets have also provided anonymity to callers engaged in criminal activities. The various types of mobile phone fraud may be classified into two categories: subscription fraud and cloning fraud. Subscription fraud occurs from obtaining a subscription to a service, often with false identity details and no intention of paying. Cases of bad debt are also included in this category. In subscription fraud, all the calls for an account are fraudulent so there is no fraud-free period. Rules that are good for one time period may not be relevant for future time periods because calling behavior changes over time.

A signature-based system has been proposed in Cahill, Lambert et al. (2000). This system is event-driven rather than time driven so that fraud can be detected as it is happening and not at fixed intervals of time. It is based on the concept of account signatures, which may describe call durations, times between calls, days of week and times of day, terminating numbers, and payment methods for the particular account. All fraud records for particular kind of fraud are put into a fraud signature. For detecting a possible fraud, the call is scored by comparing its probability under the account signature to its probability under a fraud signature. Calls that are unexpected under the account signature and expected under the fraud signature receive higher scores and will be considered as more suspicious.

Cloning is the complete duplication of a legitimate mobile identification, namely, the MIN/ESN pair. Cloned phones can be identified with a technology called call pattern analysis. When a subscriber's phone deviates from its normal activity, it triggers an alarm at the service provider's fraud management system. It is put into queue where a fraud analyst ascertains whether the customer has been victimized and then remedies the situation by dropping the connection.

Location awareness of the mobile phone can be used to detect clones within a local system and to detect roamer clones (Patel, 1997). The success of these techniques is based on the assumption that the legitimate phones will stay powered up most of the time. Clones, by definition, will exist at a different location from the legitimate mobile phone. Clone detection within a user's current system can be recognized by "too many locations" and "impossible locations". A phone cannot be making a call from one cell site, and sending a registration message from another. In the cases of too many locations, fraud can be detected when getting registration messages from two different locations at almost the same time or getting two registration messages in an interval shorter than the re-registration period. Impossible location or velocity violation occurs when after a registration message at a location, another registration attempts from a location that is impossible to reach in the time elapsed. For the roaming, fraud is detected by monitoring handsets locations at the Home Location Register (HLR) and registration messages from Mobile Switching Center at Visitor Location Register (MSC/VLR) when mobiles enter a new system.

Mobile Network Fraud

A mobile wireless network is vulnerable due to its features of open medium, dynamic changing network topology, cooperative algorithms, lack of centralized monitoring and

management point, and lack of a clear line of defense. There are many techniques to prevent mobile network intrusion such as secure MAC, secure routing and encryption. Intrusion detection approaches can be broadly classified into two categories based on model of intrusions: misuse and anomaly detection. Misuse detection refers to attempting to recognize the attacks of previously observed intrusions in the form of a pattern or signature, and monitor the occurrence of these patterns; for example, frequent changes of directory or attempts to read a password file. Anomaly detection refers to establishing a historical normal profile for each user, and then using sufficiently large deviation from the profile to indicate possible intrusions.

Anomaly detection is a critical component of the overall intrusion detection and response mechanism. Trace analysis and anomaly detection should be done locally in each node and possibly through cooperation with all nodes in the network. In the anomaly detection model (Zhang & Lee, 2003), the attack model consists of attack on routing protocols wherein attacks behave by acting on routing protocols, or it may be a traffic pattern distortion. The audit data of the model are comprised of the local routing information and position locator of the mobile node. Classifiers are used as intrusion detectors and features are selected from the audit data. There are five steps to detect a possible intrusion in the network: selecting audit data, performing appropriate data transformation, computing classifier using training data, applying the classifier to test data, and post-processing alarms to produce intrusion reports.

A technique called Trace modulation has been used in Nobile, Satyanarayanan, and Nguyen, 1997), where the end-to-end characteristics of a wireless network are recreated. Trace modulation is transparent to applications and accounts for all network traffic sent or received by the system under test. These techniques can be used to detect possible bugs in the mobile network system

M-Commerce Payment Specific Fraud

Various types of frauds may arise due to security breaches in the payment model. With the mobile Internet, a fraudster can pick sensitive information out of the air. The vulnerabilities may include infection of the mobile device by a virus, use of PINs and passwords, which are easily guessable, possibility of messages getting lost, spoofing on cardholder or the payment provider and message replay. The requirements for protecting m-commerce transactions are similar to those for protecting fixed-line transactions. Sensitive data, for example, must be secured during transmission. The following sections state various frauds that may occur during the payment life cycle and the availability of the prevention and management schemes.

Fraud Prevention During Payment Authentication

Just as with the fixed line Internet, authenticating a user's identity may be the hurdle at which demand for m-commerce services could fall. Authentication is a process of associating a particular individual with an identity. Two different techniques have been

used for authorization. One is a knowledge-based approach in which individuals use the "personal knowledge" about something, like a password or a PIN to identify themselves. The other is a token based approach in which the identification is done based on something a person has, like a driver's license number and credit card number. Both these approaches are susceptible to fraud due to lost or stolen tokens and also due to personal identifications that are used by fraudsters (Miller, 1994). A distributed scheme that solves the problem of uncovering the PIN has been proposed in Tang, Terziyan, and Veijalainen (2003). The authors suggest that instead of storing the entire PIN digits in the SIM of the mobile device, a part of the PIN is stored in the remote machine in the network. The PIN verification then involves both the mobile device and the remote machine, each verifying their respective parts of the PIN.

The increased use of wireless devices in m-commerce makes the need for identity verification even more important yet difficult to ensure; hence the need of biometrics in this field becomes more important. A biometric identification process for smart cards has been proposed in Jain, Hong, and Pankanti (2000). A biometric system has been defined as a system that makes personal identification based on some physical or behavioral characteristics of the person. In the enrollment phase a characteristic feature of the individual is scanned and converted to a digital representation. This digital form is then processed to a compact but expressive form called a template, which is stored in the smart card. During the recognition phase the biometric reader captures the characteristic and converts it into a digital form. The generated template is compared with the one stored in the smart card to establish the identity of the individual. In voice biometric systems mobile phone speakers are identified and verified based on their voice. The significant difference between a regular biometric system and the voice biometric system is that the regular one processes an image for identification whereas the voice biometric system processes acoustic information. This difference in processing results in a major difference in their acceptance since the regular biometric system requires extra infrastructure like image scanner whereas the voice biometric system can be deployed in the existing telecom systems using specialized applications (Markowitz, 2000). Radio frequency fingerprinting has been used to identify mobile phones. The Supervisory Audio Tones (SAT) tone frequency, SAT tone deviation, maximum deviation, frequency error, supervisory frequency, and supervisory tone deviation are used to fingerprint or individualize a mobile phone (Boucher, 2001).

It is being observed that the mobile phone is vulnerable to malicious software like viruses, which might be capable of creating unauthorized copies of the PIN or password when the user creates an authentication response to the payment provider. Therefore the various possibilities of virus infection in mobile phones should also be addressed. Two kinds of applications infected by virus can be downloaded. One is the signed application, which is authenticated by checking the signature using the public key stored in the mobile phone. The other is an unsigned application, which is basically un-trusted, and is the basic cause of identity fraud. To prevent such a fraud it would be appropriate to limit the access of the application to a sensitive resource on the mobile device by systematic denial or by sending a prompt to the user for validation.

Fraud During Payment Transaction and Settlement

A fraudulent transaction requires the fraudster to be in possession of the customer signature, such as PIN or password, and also to be able to send the response message to the payment provider. A possible way to prevent such a fraud is to send an authentication request number from authentication server to customer together with the authentication request, which should be unique for the transaction and should only be used for the message exchange with the cardholder.

The authentication gateway in a mobile commerce environment injects messages into the mobile network through a Short Message Switching Center for SMS as the transport or Unstructured Supplementary Services Data Center (USSDC) when using USSD as the transport. The messages pass through the Signaling System 7 (SS7) based network associated with the mobile network. This is the signaling network used for control of the mobile network. It is possible that SMS messages can be read or manipulated if the SMS switching center is accessible to the user. The capture of the messages is a source of mass fraud attacks. Hence mobile operators involved in the payment process should be encouraged to review their procedures for protecting all the vulnerable parts of their network, including the BSSs, SS7 networks and the SMSC/USSDC and their interfaces.

To decrease the probability of fraud, prepaid solutions were introduced which allow users to access specific services for which they pay in advance. In GSM mobile networks the prepaid solutions are intelligent network, which allows automatic call termination when the prepaid value reaches zero. Fraud prevention during payment settlement generally involves supporting the non-repudiation property of mobile networking. Zhou and Lam proposed an efficient technique for non-repudiation of billing using digital signatures and hashing mechanisms (Zhou & Lam, 1998). In this scheme a mobile user needs to submit a digital signature when requesting a call along with a chained hash value. After this, a series of hashed values are released at predefined intervals, which allows at most the last unit of service in dispute. The problem of uncollectible debt in telecommunication services is addressed by using a goal-directed Bayesian network for classification, which distinguishes customers who are likely to have bad debt (Maamar et al., 2001). Digital data can be copied and a user can spend a valid electronic coin several times. Requiring the vendors to contact the financial institution during every sale, in order to determine whether the dollar spent is still good, can prevent double spending. Double spending can also be prevented using tamper resistant smart cards, which contain a small database of all transactions. Double spending can also be detected, in which case a double spender is identified when the cash is settled in the bank. In another detection mechanism tamper resistant device, “Observer” is used to prevent double spending physically. This allows the owner to spend the coin once in an anonymous manner, but the identity of the owner would be revealed if he or she tries to use it again (Chaum & Pedersen, 1992). The detection schemes thus do not prevent but deter double spending and also do not require any specific hardware.

Research Issues and Conclusions

Research Issues

Without a wide popularity and usage, any given payment solution will not survive, regardless of its different attractive features. The disappearance of some innovative electronic payment procedures like eCash serves as an example of this fact. A mobile payment procedure today should not only consider the option of low to medium macro-payments, but also include at least the potential for further development in the direction of cost-effective micro payments.

Apart from the widespread acceptance of the solution by customers, another issue that remains to be solved is an issue of different mobile payment service providers. Because of their existing customer base, technical expertise and familiarity with billing, mobile telephone operators are natural candidates of the service providers. However, risk management and the need to ensure the cooperation of different providers for interoperability in an efficient m-payment system may complicate the issue. Future payment models may be the bank-dominated models where the mobile phones will provide just another way for customers to access their bank account. The PKI security standard, which is now widespread in the e-commerce scenario, can be applied to the m-commerce scenario as well. Integrating PKI into a single SIM handset needs further study. Finally, EMV, a standard for debit and credit bankcards, deserves consideration.

Conclusions

Mobile security and payment are central to m-commerce. Today, a number of competing mobile payment solutions have already found their way into the marketplace. In this chapter we surveyed several payment solutions and listed some fraud management schemes, which are central to a successful payment solution.

An important point which influences the establishment of the mobile payment procedure is the technical infrastructure needed on the customer side. A sophisticated technology may fail if the customer is not able to handle it with ease. On the other hand, simple procedures based on simple message exchange via short messaging services (SMS) may prove profitable. Thus, at present and in the future the important payment solutions will be SMS-based, which can easily be charged to the mobile phone bill of customers. Some other procedures may integrate two or more solutions. An important observation is that m-payments are still in their infancy. The m-payment solutions are still being developed with standards defined on individual business segments, which is a major reason for market fragmentation in this area even though the mobile marketplace is global. Other interesting areas related to m-commerce payment not mentioned in this chapter are issues of standardization and interoperability. These issues will have to be resolved for these solutions to reach their full potential, especially in places like Europe, where there are a large number of mobile operators and users who tend to roam into different areas.

Mobile commerce can only be conducted if all parties believe that there is adequate security. The majority of users of mobile commerce technologies are concerned about security. A sound security policy includes identifying security risks, implementing effective security measures, and educating users on the importance of security procedures. Fraud management systems are becoming increasingly important for wireless carriers. The challenge is to monitor and profile the activity of the users and to be alert to the changing nature of fraud.

References

Boucher, N.J. (2001). *The cellular radio handbook: A reference for cellular system operation* (4th ed.). New York: A Wiley-Interscience Publication, John Wiley & Sons Inc.

Cahill, M.H., Lambert, D., Pinheiro, J.C., & Sun, D.X. (2000). Detecting fraud in real world. In J. Abello, P. Pardalos & M. Resende (Eds.), *Handbook of massive datasets*. New York: Kluwer Press.

Chaum, D., & Pedersen, T. (1992). Wallet databases with observers. In E. Brickell (Ed.), *Proceedings of Crypto 92* (vol. 0740 of LNCS, pp. 89-105).

Dahleberg, T., & Tuunainen, V. (2001). Mobile payments: The trust perspective. *Workshop Sollentuna September 2001*. Retrieved September 14, 2003, from http://web.hhs.se/cic/seamless/Portal/Documents/Sollentuna/Abstract_Dahlberg_Tuunainen.doc

Dahlström, E. (2001). The Jalda payment method. *ePSO-Newsletter*, *5*(5). Retrieved September 13, 2003, from http://epso.jrc.es/newsletter/vol05/5.html

Fischer, I.M. (2002). *Towards a generalized payment model for Internet services*. Masters thesis. Technical University of Vienna.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. C*ommunications of the ACM, 43*(2). Retrieved September 14, 2003, from the ACM Digital Library.

Krueger, M. (2001). The future of m-payments - business options and policy issues. *Electronic Payment Systems Observatory (ePSO) Institute for Prospective Technological Studies*. Retrieved September 2003, from http://www.e-pso.info/epso/index.html

Maamar, Z., Yahyaoui, H., Mansoor, W., & Heuvel, W. (2001). Software agents and wireless e-commerce. *ACM SIGecom Exchanges*, *2*(3). Retrieved September 14, 2003, from the ACM Digital Library.

Markowitz, A.J. (2000). Voice biometrics. *Communications of the ACM, 43*(9). Retrieved September 14, 2003, from the ACM Digital Library.

McKitterick, D., & Dowling J. (*2003*). *State of the art review of mobile payment technology*. Retrieved September 14, 2003, from Trinity College Of Dublin, Department of Computer Science Web site: http://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf

Miller, B. (1994). Vital signs of identity [biometrics]. *IEEE Spectrum Magazine, 31*(2), 22-30. Retrieved September 14, 2003, from the IEEE Xplore Online Delivery System.

Mobey Forum Mobile Financial Services Ltd. (2001). *The preferred payment Architecture Technical Documentation*. Retrieved September 2003, from http://ipsi.fraunhofer.de/mobile/teaching/m-commerce_ws0203/payment/MobeyTechnical.pdf

Mobile Commerce Report. Retrieved September 9, 2003, from http://www.durlacher.com/downloads/mcomreport.pdf

MobileInfo.com: M-Commerce. Retrieved September 9, 2003, from http://www.mobileinfo.com/Mcommerce/index.htm

Mobile Payment Forum. (2002). *Enabling secure, interoperable, and user-friendly mobile payments*. Retrieved September 9, 2003, from http://www.mobilepaymentforum.org/pdfs/mpf_whitepaper.pdf

Mobile Payments in M-Commerce, White paper. (2002). Retrieved September 2003, from Cap, Gemini, Ernst and Young Web site: http://www.cgey.com/tmn/pdf/MobilePaymentsinMCommrce.pdf

More Magic Software (2000, November 24). *Payment transaction platform*. Retrieved September 9, 2003, from http://www.moremagic.com/whitepapers/technical_wp_twp021c.html

Nobile, B.D., Satyanarayanan, M., & Nguyen, G.T. (1997). Trace-based mobile network emulation. *Proceedings of the ACM SIGCOMM '97 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication.* Retrieved September 14, 2003, from the ACM Digital Library.

Patel, S. (1997). Location, identity and wireless fraud detection. *IEEE International Conference on Personal Wireless Communications, 17-19 Dec.* (pp. 515-521). Retrieved September 14, 2003, from the IEEE Xplore Online Delivery System.

Paybox: *ePSO Inventory Database* (n.d.). Retrieved September 13, 2003, from http://www.e-pso.info/epso/index.html

Paybox.net. (2001). Paybox security, Whitepaper, business and technical information regarding the security at paybox. Retrieved September 2003, from http://www.paybox.net/publicrelations/public_relations_whitepapers.html

Paybox.net. (2002). *Mobile commerce delivery made simple: Whitepaper*. Retrieved September 13, 2003, from http://www.paybox.net/publicrelations/public_relations_whitepapers.html

Payment Technology. Retrieved September 13, 2003, from Trinity College Of Dublin, Department of Computer Science Web site: http://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf

PBS. (n.d.). *Mobile payment*. Retrieved September 14, 2003, from http://www.pbs.dk/english/produkter/mbetaling.htm

Pierce, M. (2000). *Multi-party electronic payments for mobile communications.* Doctoral dissertation. University of Dublin.

Shelfer, K.M., & Procaccino, J.D. (2002). Smart card evolution. *Communications of the ACM, 45*(7). Retrieved September 14, 2003, from the ACM Digital Library.

Tang, J., Terziyan, V., & Veijalainen, J. (2003). Distributed PIN verification scheme for improving security of mobile devices. *Mobile Networks and Applications, 8*(2). Retrieved September 14, 2003, from the ACM Digital Library.

Telecom Media Networks. (2000, September). Mobile payments-commerce. Retrieved September 13, 2003, from http://www.cgey.com/tmn/pdf/MobilePaymentsinMCommrce.pdf

Vodafone M-Pay Bill. (n.d.). *What is Vodafone m-pay bill?* Retrieved September 2003, from http://mpay-bill.vodafone.co.uk/w_mpay.html

Xiaolin, Z., & Chen, D. (2003). Study of mobile payment systems. *IEEE International Conference on E-commerce* (pp. 24-27). Retrieved September 14, 2003, from the IEEE Xplore Online Delivery System.

Zhang, Y., & Lee, W. (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Networks, 9*(5). Retrieved September 14, 2003, from the ACM Digital Library.

Zhou, J., & Lam, K. (1998). Undeniable billing in mobile communication. *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking* (pp. 284-290). Retrieved September 14, 2003, from the ACM Digital Library.