M-Commerce and its Security Issues

By SAMEER YADAV
## Contents

1 INTRODUCTION AND OVERVIEW ........................................... 1  
  1.1 Background and Motivation ........................................ 1  
  1.2 History of M-Commerce ........................................... 2  
  1.3 Latest Trends and Consumer Reactions ........................... 3  

2 M-COMMERCE: Basics ............................................. 5  
  2.1 M-Commerce: Definition ........................................ 5  
  2.2 Mobile devices .................................................. 5  
  2.3 Features of m-commerce .......................................... 6  
  2.4 Differences to E-Commerce: Advantages and Disadvantages . 6  
  2.5 Framework ..................................................... 7  

3 KEY ISSUES .................................................... 10  
  3.1 Security Issues .................................................. 10  
  3.2 Wireless User Interface and Middleware Issues .............. 11  
    3.2.1 Wireless and mobile middle-ware for mobile commerce .. 11  
  3.3 Wireless Networking Infrastructure ............................. 12  
  3.4 Issues for Carriers and Developers ............................ 13  

4 SECURITY ISSUES FOR M-COMMERCE .......................... 16  
  4.1 Security of Network technologies ............................... 16  
    4.1.1 GSM ........................................................ 16  
    4.1.2 UMTS ..................................................... 18  
    4.1.3 WLAN .................................................... 19  
    4.1.4 Bluetooth ............................................... 20  
  4.2 Transport Layer Security ....................................... 20  
    4.2.1 SSL/TLS .................................................. 20
CONTENTS

4.2.2 WTLS .................................................. 21
4.3 Service Security ......................................... 21
   4.3.1 Intelligent Network ................................... 21
   4.3.2 Parlay/OSA ........................................... 21
   4.3.3 SMS .................................................. 22
   4.3.4 USSD .................................................. 22
   4.3.5 SIM/USIM Application Toolkit ...................... 22

5 EMERGING M-COMMERCE APPLICATIONS 24
   5.1 Mobile Financial Applications (MFA) ................... 25
   5.2 Mobile Advertising ..................................... 25
   5.3 Mobile Inventory Management (MIM) .................... 26
   5.4 Product Location and Search (PLS) ..................... 27
   5.5 Proactive Service Management .......................... 28

6 M-PAYMENT 29
   6.1 Background on payment systems ......................... 29
   6.2 Distinctive features of payment systems .............. 30
   6.3 Categorization of M-payment systems ................. 31
      6.3.1 Software electronic coins ....................... 31
      6.3.2 Hardware electronic coins ....................... 32
      6.3.3 Background account ............................. 32
   6.4 Standardization and forums ............................ 32

7 CONCLUSIONS AND FURTHER RESEARCH 34
   7.1 Harnessing M-Commerce potential ...................... 34
   7.2 Interesting Research Areas in M-Commerce ........... 34
Chapter 1

INTRODUCTION AND OVERVIEW

Advances in e-commerce have resulted in progress towards strategies, requirements and development of e-commerce application. Nearly all the e-commerce applications envisioned so far assume fixed or stationary users with wired infrastructure, such as a browser on PC connected to the internet using phone lines on LAN. The term E-commerce (electronic commerce) denotes business processes on the Internet, such as the buying and selling of goods. This general definition of e-commerce does not say anything about the kind of device that the end user employs to gain access to the Internet. The underlying technology could be wireline (e.g. using a home PC as end user device) or wireless (e.g. using a mobile phone as end user device).

Many people do not use a PC outside the office, but keep the mobile phone at their side all the times. Mobile commerce is perfect for this group. M-commerce allows one to reach the consumer directly, not his fax machine, his desk, his secretary or his mailbox, but ones consumer directly, regardless of where he is.

The term mobile commerce is all about wireless e-commerce, that is, where mobile devices are used to do business on the Internet, either in the B2B or B2C market. As such, m-commerce is a subset of e-commerce. M-commerce is the delivery of electronic commerce capabilities directly into the hands, anywhere, via wireless technology and putting a retail outlet in the customers hands anywhere. This can be done with just a mobile phone, a PDA connected to a mobile phone or even a portable PC connected to a mobile phone. M-commerce is the market of buying and selling goods with wireless technology such as PDAs and cellular phones primarily within the retail, telecommunications and financial services industries. Many phone companies are enabling services for M-commerce applications and marketing their products to organizations who can utilize M-commerce. Wireless technology has brought its benefits to M-Commerce and its challenges as well.

1.1 Background and Motivation

Electronic commerce has attracted significant attention in the last few years. Advances in e-commerce have resulted in significant progress towards strategies, requirements and development of e-commerce applications. Nearly all the applications
envisioned and developed so far assume fixed or stationary users with wired infrastructure, such as browser on a PC connected to the Internet using phone lines or a Local Area Network. A new e-commerce application such as Wireless e-commerce or Mobile e-commerce will benefit one to reach the consumer directly, regardless of where he is.

Though e-commerce has grown as expected, M-Commerce has not taken off the same way for the use of goods and services. Wireless services are not everywhere and consumers often do not feel safe or happy buying with their phone. As technology increases this may change. As for now, consumers use M-commerce as a portable friend to communicate and to do transactions. When consumers feel secure, they buy. As the younger generation grows with wireless business models will further develop M-Commerce.

The emergence of M-commerce, a synonym for wireless e-commerce allows one to do the same function that can be done over the internet. This can be done by connecting a PDA to a mobile phone, or even a portable PC connected to a mobile phone. Mobile Commerce is perfect for the group who always keep a mobile phone by side all the times. A study from the wireless data and computing service, a division of strategy analytics, reports that the mobile commerce market may rise to The report predicts that transactions via wireless devices will generate about 14 billion dollars a year. With the omnipresent availability of mobile phones (and other mobile devices), M-commerce services have a promising future, especially in the B2C market. Future applications include buying over the phone, purchase and redemption of ticket and reward schemes, travel and weather information, and writing contracts on the move. However, the success of m-commerce very much depends on the security of the underlying technologies. For example, today the charge back rate for credit card transactions on the Internet is 15 percent, versus 1 percent for POS (Point-of-Sales) credit card transactions. Chargeback rates grow to 30 percent when digital products are sold. For m-commerce to take off, fraud rates have to be reduced to an acceptable level. As such, security can be regarded as an enabling factor for the success of m-commerce applications. In this paper, we discuss two main areas of m-commerce that are relevant to security, namely

- Network technology - In m-commerce, all data is transmitted via a mobile telecommunication network. Here, we consider existing network and service technologies for 2G (2nd Generation), 3G (3rd Generation) and other wireless systems.

- M-payment (mobile payment) - Doing business on the Internet requires the payment of goods and services. M-payment systems have different requirements and characteristics than e-payment systems. Here, we give an overview of current payment technology.

1.2 History of M-Commerce

Mobile commerce was born in 1997 when the first two mobile-phones-enabled Coca Cola vending machines were installed in the Helsinki area in Finland. The machines accepted payment via SMS text messages. The first mobile phone-based banking
service was launched in 1997 by Merita Bank of Finland, also using SMS. In 1998, the first sales of digital content as downloads to mobile phones were made possible when the first commercial downloadable ringtones were launched in Finland by Radiolinja. Two major national commercial platforms for mobile commerce were launched in 1999: Smart Money (http://smart.com.ph/money/) in the Philippines, and NTT DoCoMo’s i-Mode Internet service in Japan. Mobile-commerce-related services spread rapidly in early 2000. Norway launched mobile parking payments. Austria offered train ticketing via mobile device. Japan offered mobile purchases of airline tickets.

The first book to cover mobile commerce was Tomi Ahonen’s M-profits in 2002. The first university short course to discuss mobile commerce was held at the University of Oxford in 2003, with Tomi Ahonen and Steve Jones lecturing. As of 2008, UCL Computer Science and Peter J. Bentley demonstrated the potential for medical applications on mobile devices. PDAs and cellular phones have become so popular that many businesses are beginning to use mobile commerce as a more efficient way to communicate with their customers. In order to exploit the potential mobile commerce market, mobile phone manufacturers such as Nokia, Ericsson, Motorola, and Qualcomm are working with carriers such as AT&T Wireless and Sprint to develop WAP-enabled Smartphones. Smartphones offer fax, e-mail, and phone capabilities.

Since the launch of the iPhone, mobile commerce has moved away from SMS systems and into actual applications. SMS has significant security vulnerabilities and congestion problems, even though it is widely available and accessible. In addition, improvements in the capabilities of modern mobile devices make it prudent to place more of the resource burden on the mobile device.

More recently, brick and mortar business owners, and big-box retailers in particular, have made an effort to take advantage of mobile commerce by utilizing a number of mobile capabilities such as location based services, barcode scanning, and push notifications to improve the customer experience of shopping in physical stores. By creating what is referred to as a ’bricks & clicks’ environment, physical retailers can allow customers to access the common benefits of shopping online (such as product reviews, information, and coupons) while still shopping in the physical store. This is seen as a bridge between the gaps created by e-commerce and in-store shopping, and is being utilized by physical retailers as a way to compete with the lower prices typically seen through online retailers.

1.3 Latest Trends and Consumer Reactions

The latest trends of e-commerce include electronic bill pay, digital signatures, online banking just to name a few. Electronic bill pay is essentially paying your household bills over the internet. In most cases, it works like this. The consumer subscribes to an EBP provider, deposits funds (or you allow them access to your bank account) with them and as the consumer receives their bills in the mail, they in turn email them to their EBP provider with the date that they want the invoices paid. This latest trend has also taken off in the housing market. Allowing prospective buyers to sign closing contracts without taking time off is wonderful. Consumers love this idea. These contracts are legally binding and hold the same weight in court as if
Online banking is the banking industry to compete with one another and with the electronic bill pay providers. Online banking allows consumers to check their balances, pay bills, purchase certificate of deposits and apply for loans all from the consumers home. This is a wonderful service that the banking industry has offered. The drawback for consumers is with servers crashing and hackers downloading your banking information. Whereas, the banking industry has taken extreme measures to ensure the consumers privacy no system is hacker proof.

Researchers see games as an avenue to attract more consumers as they become more efficient with their phones. An area of promise for M-Commerce is in the travel industry. A consumer stuck in traffic or suddenly aware of an unexpected urgent meeting has a need to pay for an airline/train ticket or secure a hotel room. This is possible with M-Commerce. Arranging business meetings or short conferences is a common use of mobile communicating in the business world. Buying stock over the phone is a convenience for some. Retail consumers still enjoy browsing at stores or through catalogues. As technology becomes more common in the consumers lifestyle, business models will become more apparent for M-Commerce.
Chapter 2

M-COMMERCE: Basics

2.1 M-Commerce: Definition

There are many definitions of the term m-commerce. Common to all definitions is that a terminal or mobile device is employed to communicate over a mobile telecommunication network. There are different views as of the purpose of this communication. Some definitions restrict m-commerce to transactions involving a monetary value, whereas other definitions generalize the term to services that involve communication, information, transaction, and entertainment. Summarizing, we define m-commerce as using a mobile device for business transactions performed over a mobile telecommunication network, possibly involving the transfer of monetary values.

2.2 Mobile devices

M-commerce is not just about using mobile phones as end user devices. The following list gives an overview of different kinds of mobile devices:

- Mobile phone
- PDA (Personal Digital Assistant)
- Smart phone - The smart phone combines mobile phone and PDA technology into one device
- Laptop Earpiece (as part of a Personal Area Network)

Each mobile device has certain characteristics that influence its usability, such as

- Size and color of display
- Input device, availability of keyboard and mouse
- Memory and CPU processing power
- Network connectivity, bandwidth capacity
• Supported operating systems (e.g. PalmOS, Microsoft Pocket PC)

• Availability of internal smart card reader (e.g. for a SIM card in mobile phones)

Depending on these factors, the services that the end user can receive differ considerably. Moreover, depending on the network technology used for transmission, the bandwidth capacity varies and influences the kind of services that the end user is able to receive. In mobile phones, there exist three solutions to internal smart cards: single SIM, dual chip, and dual slot. Single SIM is the solution that is most widely available today, where all confidential user information is stored on one smart card. Dual chip means that there are two smart cards in the mobile phone, one for user authentication to the network operator and one for value-added services like m-payment or digital signature. A dual slot mobile phone has a SIM card and a card slot for a full-sized external smart card. With this solution different cards can be used one after the other. Moreover, the cards can also be used in traditional POS and ATM terminals.

2.3 Features of m-commerce

• Anytime and anywhere access to business processes managed by computer-mediated networks.

• Access takes place using mobile communication networks, making availability of these services independent of the geographic location of the user.

2.4 Differences to E-Commerce: Advantages and Disadvantages

In comparison to e-commerce, m-commerce offers both advantages and disadvantages. The following list summarizes the advantages of m-commerce [1]:

• Ubiquity - The end user device is mobile, that is, the user can access m-commerce applications in real time at any place.

• Accessibility - Accessibility is related to ubiquity and means that the end user is accessible anywhere at any time. Accessibility is probably the major advantage by comparison with e-commerce applications involving a wired end user device.

• Security - Depending on the specific end user device, the device offers a certain level of inherent security. For example, the SIM card commonly employed in mobile phones is a smart card that stores confidential user information, such as the users secret authentication key. As such, the mobile phone can be regarded as a smart card reader with smart card.

• Localization - A network operator can localize registered users by using a positioning system, such as GPS, or via GSM or UMTS network technology, and
offer location-dependent services. Those services include local information services about hotels, restaurants, and amenities, travel information, emergency calls, and mobile office facilities.

- **Convenience** - The size and weight of mobile devices and their ubiquity and accessibility makes them an ideal tool for performing personal tasks.

- **Personalization** - Mobile devices are usually not shared between users. This makes it possible to adjust a mobile device to the users needs and wishes (starting with the mobile phone housing and ringtones). On the other hand, a mobile operator can offer personalized services to its users, depending on specified user characteristics (e.g. a user may prefer Italian food) and the users location (see above).

The following list summarizes the main disadvantages of m-commerce:

- Mobile devices offer limited capabilities (such as limited display). Between mobile devices these capabilities vary so much that end user services will need to be customized accordingly.

- The heterogeneity of devices, operating systems, and network technologies is a challenge for a uniform end user platform. For this reason, standardization bodies consisting of telecommunication companies, device manufacturers, and value-added service providers integrate their work. For example, many current mobile devices implement an IP stack to provide standard network connectivity. At the application level, the Java 2 Micro Edition (J2ME) offers a standardized application platform for heterogeneous devices.

- Mobile devices are more prone to theft and destruction. According to a government report, more than 700000 mobile phones are stolen in the UK each year. Since mobile phones are highly personalized and contain confidential user information, they need to be protected according to the highest security standards.

- The communication over the air interface between mobile device and network introduces additional security threats (e.g. eavesdropping).

### 2.5 Framework

We are aware that consensus within business and industry of future applications is still in its infancy. However, we are interested in examining those future applications and technologies that will form the next frontier of electronic commerce. To help future applications and to allow designers, developers and researchers to strategize and create mobile commerce applications, a four level integrated framework is proposed. These four levels are as follows: **m-commerce applications, user infrastructure, middleware and network infrastructure** which simplifies the design and development. By following this framework a single entity is not forced to do everything to build m-commerce systems, rather they can build on the functionalities
provided by others. The framework also provides a developer and provider plane to address the different needs and roles of application developers, content providers and service providers. Fig. 2.1 depicts the Framework of M-commerce in brief (cf. [10]).

Content provider can build its service using applications from multiple application developers and also can aggregate content from other content providers and can supply the aggregated content to a network operator or service provider. Service providers can also act as content aggregators, but are unlikely to act as either an application or content provider due to their focus on the network and service aspects of m-commerce.

Wireless carriers can play a very active and important role in the mobile commerce applications and services due to the fact that mobile user is going through their network to perform all mobile commerce transactions. Mobile user is likely to prefer a common bill for voice, data and mobile commerce services. Fig.2.2 shows the Life Cycle of Mobile commerce (cf. [10]).
Figure 2.2: Mobile Commerce Life Cycle
Chapter 3

KEY ISSUES

3.1 Security Issues

As mentioned earlier, m-commerce is not possible without a secure environment, especially for those transactions involving monetary value. Depending on the point of views of the different participants in an m-commerce scenario, there are different security challenges. These security challenges relate to:

- The mobile device - Confidential user data on the mobile device as well as the device itself should be protected from unauthorized use. The security mechanisms employed here include user authentication (e.g. PIN or password authentication), secure storage of confidential data (e.g. SIM card in mobile phones) and security of the operating system.

- The radio interface - Access to a telecommunication network requires the protection of transmitted data in terms of confidentiality, integrity, and authenticity. In particular, the user’s personal data should be protected from eavesdropping. Different security mechanisms for different mobile network technologies (i.e. in 2G, 3G, etc.) will be presented in Chapter 4.

- The network operator infrastructure - Security mechanisms for the end user often terminate in the access network. This raises questions regarding the security of the user’s data within and beyond the access network. Moreover, the user receives certain services for which he/she has to pay. This often involves the network operator and he/she will want to be assured about correct charging and billing.

- The kind of m-commerce application - M-commerce applications, especially those involving payment, need to be secured to assure customers, merchants, and network operators. For example, in a payment scenario both sides will want to authenticate each other before committing to a payment. Also, the customer will want assurance about the delivery of goods or services. In addition to the authenticity, confidentiality and integrity of sent payment information, non-repudiation is important.
CHAPTER 3. KEY ISSUES

3.2 Wireless User Interface and Middleware Issues

To make the application described previously a reality, several functional components are necessary as highlighted in the first figure. Although it is able to do some simple mobile commerce transactions using a simple hand-held device, many sophisticated mobile commerce applications require other capabilities. For example,

- Dynamic, adaptable and smart user interface that learns from and with user,
- Ability to accept user input in many forms including voice,
- Ability to display rich and usable contents,
- Location awareness and ability to track users, products and devices,
- Multi network interfaces for increased and reliable wireless access,
- Basic security features to handle malicious code, support for authenticating user, services and applications,
- Ability to work with and adapt to mobile commerce applications with diverse requirements,
- Possible support for context awareness,
- Ability to discover and download upgraded applications and software proactively,
- An operating system that can manage resources to support many of the functions.

Some of these features are already available in hand-held devices. Many of these capabilities will increase the size and weight significantly, and thus, potentially affect the usability and portability of these devices.

3.2.1 Wireless and mobile middle-ware for mobile commerce

Traditionally, middle-ware unites different applications, tools, networks and technologies; allowing user access via a common interface. Mobile middle-ware can be defined as an enabling layer of software that is used by the applications development to connect the m-commerce applications with different networks and operating systems without introducing mobility awareness in the applications.

To allow for web content to be accessible from everywhere, from PCs to TVs to palm devices to cellular phones, the World Wide Web consortium (W3C) had developed several recommendations. These recommendations include the Extensible Makeup Language (XML) for richer semantic information, improved Cascading Style Sheets (CSS) and Extensible Style Sheet Language (XSL) to further separate content from presentation, and a Document Object Model (DOM) which defines a language independent application programming interface that applications can use to access
and modify the structure, content and style of HTML and XML documents. Fig. 3.1 above shows the Mobile middleware for application and content adaptation (cf. [9]).

3.3 Wireless Networking Infrastructure

In this section the wireless networking requirements for various mobile commerce applications are being discussed. Mobile commerce applications would present five general networking requirements: location management, multicast support, network dependability, and support for Quality-Of-Service, and the ability to roam across multiple wireless networks. To help network designers and developers, we translate these five networking requirements into more specific attributes as shown in the Table 3.1 below (cf. [13]).
<table>
<thead>
<tr>
<th>Networking requirements</th>
<th>Specific attributes</th>
</tr>
</thead>
</table>
| Multicast support       | • support for multicast in infrastructure wireless networks  
                          • support for multicast in ad hoc wireless networks (much more difficult due to dynamic topology and other factors)  
                          • group connectivity under mobility/failure  
                          • synchronization/atomicity of transactions from multiple users |
| Network dependability   | • impact and frequency of component failure  
                          • fault-tolerant design  
                          • user access to multiple networks  
                          • levels of network availability |
| Quality of service      | • bandwidth requirements  
                          • delay and delay variation  
                          • tolerable loss characteristics |
| Roaming across multiple networks | • handoff among multiple wireless networks  
                                   • keeping track of users across networks |

Table 3.1: *Wireless infrastructure requirements for mobile commerce*

### 3.4 Issues for Carriers and Developers

Wireless carriers can play a very active and important role in the mobile commerce applications and services due to the fact that a mobile user is going through their network to perform all mobile transactions. Service providers can also act as content aggregators but are likely to act as a clearing house for content and application providers in advertising and distributing their products to its customers.
<table>
<thead>
<tr>
<th>Issues</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network processing and storage requirements</td>
<td>• Band width and delay requirements (real-time vs. non-real time applications)</td>
</tr>
<tr>
<td></td>
<td>• Mobile device capabilities</td>
</tr>
<tr>
<td></td>
<td>• Disconnected operation</td>
</tr>
<tr>
<td></td>
<td>• Multicasting for group communications</td>
</tr>
<tr>
<td></td>
<td>• Symmetric vs. asymmetric processing and storage</td>
</tr>
<tr>
<td>Application Development</td>
<td>• Use of any existing Software Development Kit (SDK)</td>
</tr>
<tr>
<td></td>
<td>• Simulation of environment where application will be used</td>
</tr>
<tr>
<td></td>
<td>• Maximum number of simultaneous users</td>
</tr>
<tr>
<td></td>
<td>• The size of application code</td>
</tr>
<tr>
<td></td>
<td>• Support for secure transactions</td>
</tr>
<tr>
<td></td>
<td>• Support for fixed users</td>
</tr>
<tr>
<td>Compatibility and interoperability</td>
<td>• Independence from the underlying wireless access technologies</td>
</tr>
<tr>
<td></td>
<td>• Independence from the device functionalities</td>
</tr>
<tr>
<td></td>
<td>• Interoperability with IP</td>
</tr>
<tr>
<td></td>
<td>• Compatibility with Wireless Application Protocol (WAP)</td>
</tr>
<tr>
<td>Desirable features</td>
<td>• Support for intermittent connectivity</td>
</tr>
<tr>
<td></td>
<td>• Adaptive to the user and network environment</td>
</tr>
<tr>
<td></td>
<td>• Support for “atomic” transactions</td>
</tr>
<tr>
<td></td>
<td>• Easy upgradability</td>
</tr>
<tr>
<td></td>
<td>• User specified features invocation</td>
</tr>
</tbody>
</table>

Table 3.2: Some important issues for applications developers
Wireless carriers are also to face challenges involving how to price mobile commerce services, and because several carriers are likely to be involved in completing a mobile commerce transaction, another issue is how to divide revenues among multiple carriers. There are many important issues that need to be addressed before mobile commerce applications can be widely deployed. These include the development of new business models for charging wireless customers and for revenue division among providers, maturity of application software, middle-ware support, vendor support and user trust necessary for conducting mobile transactions. There are some important issues for developers of m-commerce applications. These issues are presented in the Table 3.2 above (cf. [13]). Due to the potential values of many mobile commerce applications, atomic transactions may be necessary. It is possible that the mobile middle-ware may provide most of such functions and thus reducing the amount of work needed to support atomic transactions.
Chapter 4

SECURITY ISSUES FOR M-COMMERCE

In this chapter, we give an overview of the technologies which are relevant to secure m-commerce transactions. We focus on those network and service technologies which are specific to mobile devices.

4.1 Security of Network technologies

We first discuss the security of network technologies used for mobile commerce.

4.1.1 GSM

GSM (Global System for Mobile Communication) is the current European standard for mobile communications. Since GSM handsets are popular and widespread, they have to be considered as the major device for mobile commerce at the moment. In the first years of GSM (beginning of the 1990s), the devices were very limited with respect to their capabilities other than telephony. Dial-in data sessions over circuit switched connections were possible but relatively slow (9.6 Kbit/s) and required a separate device (computer) which reduces mobility. As the GSM core network was extended with more and more data service elements, the cellular phones also became more powerful. A number of data services were established:

- SMS (Short Message Service) allows the exchange of 160 character short messages over the signaling channel.

- WAP (Wireless Application Protocol) permits access to internet content and applications formatted in WML (Wireless Mark-up Language). At first, WAP was based on circuit switched connections.

- HSCSD (High Speed Circuit Switched Data) provides higher data rates by channel bundling.

- GPRS (General Packet Radio Service) extends GSM with packet oriented services. With GPRS, the mobile node can stay “always on” without blocking...
a connection timeslot with the base station. GPRS can also be used as a bearer service for WAP and SMS.

The basic architecture of GSM including GPRS, IN (intelligent network) and SMS components is depicted in Figure 4.1 above (cf. [3]).

The mobile station communicates over the wireless interface with a base transceiver station (BTS) which is part of a base station subsystem (BSS). The base station controller (BSC) is connected with a MSC (Mobile Switching Centre) and a SGSN (Serving GPRS Support Node). The latter two are the central switching components for circuit and packet switched data. When a customer subscribes, the GSM home network assigns the mobile station a unique identifier, the international mobile subscriber identity (IMSI), and an authentication key Ki. The IMSI and the secret authentication key Ki of the mobile station (MS) are stored in the SIM (subscriber identity module), which is assumed to be tamper proof. On the network side, the IMSI, Ki and other information are stored in the HLR (Home Location Register) and AuC (Authentication Centre). GSM provides the following security features for the link between the mobile station and the network (cf. [7]):

- IMSI confidentiality
- IMSI authentication
- User data confidentiality on physical connections
- Connectionless user data confidentiality
- Signaling information element confidentiality

GSM provides the basic security mechanisms for m-commerce transactions. In particular, the mobile customer authenticates towards the network with a challenge/response protocol based on the secret key Ki. Furthermore, the wireless link between the mobile station and the BTS is encrypted with a symmetric key which is also derived from Ki. The secret key Ki is never sent over the network. But there are
weaknesses: since the network is not authenticated, a false base station can perform a “man-in-the-middle” attack. The base station can suppress IMSI confidentiality and encryption and this is not even visible to the mobile station.

4.1.2 UMTS

UMTS (Universal Mobile Telecommunication System) is the next generation (3G) mobile telecommunication system and a further development of GSM. The major difference to GSM is the radio network (UTRAN) with its transition to the WCDMA (Wideband Code Division Multiple Access) radio technology. Two new network components, RNC (Radio Network Controller) and Node B are introduced in UTRAN. Furthermore, the security protocols have been modified and now the RNC is responsible for de-/ciphering. The main components of the GSM/GPRS core network with MSC, SGSN etc. can be reused or evolved to UMTS. This is depicted in Figure 4.2 above (cf. [3]).

In general, the security architecture of UMTS is carefully designed to fix the security weaknesses of GSM (cf. [6], [11]). As is described above, the main problems of GSM originate from two facts: authentication is one way (the mobile station does not authenticate the network), and encryption is optional. In UMTS, authentication is mutual, and encryption is mandatory unless the mobile station and the network agree on an enciphered connection. In addition, integrity protection is always mandatory and protects against replay or modification of signaling messages. Sequence numbers in authentication vectors protect against reuse of authentication vectors by network impersonators. UMTS introduces new cipher algorithms and longer encryption keys. Thus, UMTS does not seem to have any obvious security holes.
4.1.3 WLAN

The IEEE standard 802.11 specifies families of Wireless Local Area Networks (WLAN) which operate in the unlicensed 2.4 GHz and 5 GHz band. The standards specify the physical layer and the medium access control layer. For the network layer and above, WLAN employs a classical IP stack. A number of commercial products (even for PDAs) are available, and IEEE 802.11b, offering 11 Mbit/s raw bandwidth, is currently very popular. When operated in the infrastructure mode, the mobile station attaches to an Access Point which provides connectivity to fixed net IP networks or to other mobile stations. In the default mode, WLAN does not provide any security. This means that a mobile attacker can eavesdrop and manipulate all the wireless traffic with standard tools. In order to provide a certain level of security, the IEEE defined WEP (Wired Equivalent Privacy). WEP was designed to provide:

- Authentication to protect the association to an AP
- Integrity protection of MAC frames
- Confidentiality of MAC frames

The protection is based on secret WEP keys of either 40 or 104 bits. Concatenated with a clear text initialization vector, the secret key serves as input for the RC4 stream cipher. But it has been shown that authentication and integrity protection is completely insecure and encryption is at least partly insecure. It suffices for an attacker to intercept a single successful authentication exchange between a mobile station and the AP to be able to authenticate without knowing the secret keys. Furthermore, since a CRC checksum is used for integrity protection, an attacker can modify the data and adapt the checksum accordingly. For example, if the position of commercially sensitive information (e.g. an amount) within a datagram is known, the corresponding bits can be XORed with any value. With a large number of intercepted frames, the WEP keys can even be recovered, breaking the encryption. Furthermore, since the WEP keys are network keys, preserving their secrecy is difficult for private networks and impossible for public WLAN hotspots. In recent work of the IEEE Task group on security (TgI), the new security standard IEEE 802.1X has been adopted. 802.1X is a framework for authentication and key management which employs the Extensible Authentication Protocol for a variety of authentication mechanisms, e.g. certificate based TLS. But the weaknesses of
WEP cannot be remedied by the new authentication and key management schemes in 802.1X. The IEEE is currently working towards a new standard (WEP2), and a number of proposals are in circulation. Another approach is to employ VPN (virtual private network) technologies and in particular IPsec in order to establish network layer security. The IPsec protocol (or more specifically the ESP Tunnel protocol) is an internet standard (cf. [8]) for the protection of IP packets between two nodes (e.g. a mobile station and a security gateway). This architecture is depicted in Figure 4.3 above (cf. [3]). Note that link layer specific information (e.g. MAC addresses) is still unprotected.

4.1.4 Bluetooth

Bluetooth is a wireless technology developed by the Bluetooth Special Interest group and is mainly aiming at ad hoc piconets and connections to peripheral devices. Bluetooth is also operating in the unlicensed 2.4 GHz band and can be considered as a de-facto-standard. The Bluetooth specification defines a complete OSI stack, so, unlike WLAN, it is not restricted to IP connectivity. Although raw bandwidth is limited to 1 Mbit/s, the Bluetooth technology will probably often be used in the future to connect devices in the personal environment, which makes it relevant for m-commerce. Bluetooth specifies three security modes, including “no security”. Bluetooth provides link layer security with a challenge-response protocol for authentication and a stream cipher encryption of user and signaling data (cf. [2]). When the connecting devices do not share a key in advance, they have to establish an initialization key in a pairing procedure. This is based on a PIN, which must be entered into both devices (or imported from some application). Bluetooth can currently be considered secure for small ad hoc networks, provided the pairing happens in a safe environment and the PIN is strong enough. The existing attacks are still theoretical in nature. However, privacy requirements may not be met since the Bluetooth device address (unique MAC address) allows the tracing of personal devices and hence their owner.

4.2 Transport Layer Security

The above technologies provide security for the wireless link between mobile customer and access network or access device. If the access network is considered secure and the m-commerce transaction is completely handled within the access network, this may be sufficient. But often, an m-commerce transaction involves parties outside the access network (merchant, payment service provider etc.). In this section, we discuss end-to-end security for mobile devices. This protects applications which communicate over an IP port.

4.2.1 SSL/TLS

The SSL/TLS protocol is by far the most widely used internet security protocol. Its main application is the HTTPS protocol (HTTP over SSL), but it may also be used as a standalone protocol. SSL requires a bidirectional byte stream service
(i.e. TCP). SUN has implemented a client side version of SSL for limited devices, called KSSL (Kilobyte SSL). KSSL does not offer client side authentication and only implements certain commonly used cipher suites, but it has a very small footprint and runs on small devices using the J2ME platform.

4.2.2 WTLS

The WAP forum has standardized a transport layer security protocol (WTLS) as part of the WAP 1 stack. WTLS provides transport security between a WAP device (e.g. a mobile phone) and a WAP gateway which performs the protocol transformation to SSL/TLS. Hence, no real end-to-end security is provided and the WAP Gateway needs to be trusted. Note that the WAP Forum now proposes a WAP 2 stack which is a classical TCP/IP stack on a wireless bearer medium. This permits end-to-end SSL/TLS sessions.

4.3 Service Security

Here, we discuss the security of network services which can be used for m-commerce transactions.

4.3.1 Intelligent Network

With the introduction of the IN (Intelligent Network) technology to GSM networks, additional services could be realized. The IN architecture for GSM (called CAMEL, Customized Application for Mobile Enhanced network Logic) was adapted from the fixed network standard ETSI Core INAP, and was originally designed for circuit switched calls (CAMEL phase 1 and 2). The IN is triggered during call handling at the MSC if the HLR entry indicates subscription to an IN service. With CAMEL phase 3, the IN services can also be applied to SMS and to packet data services. The IN component SCP (Service Control Point) controls the call or data service via the CAMEL Application Part (CAP) protocol which runs on top of the SS7 (Signaling System Number 7) protocol. Prominent examples of IN services are the transformation of dialed numbers (e.g. to realize Virtual Private Nets) and prepaid services. The IN platform provides some flexibility for the generation of m-commerce services. IN handling can e.g. be triggered by a specific called party, a calling party, an USSD string (requiring CAMEL phase 2), mobile originating SMS (requiring CAMEL phase 3) or mobile terminating SMS (requiring CAMEL phase 4). The security of an IN service depends on the underlying GSM or UMTS network security (see above) and on the specific characteristics of the service application.

4.3.2 Parlay/OSA

Parlay/OSA (Open Service Access) is an initiative of the industry (Parlay group), ETSI and 3GPP and aims at introducing standard interfaces to network services. The IN platform and their SS7 based protocols like INAP and CAP are relatively complex and generation of services is reserved to operators and manufactures. Now
Parlay offers standard application programming interface which allows service provisioning on IT platforms using standard middleware. The Parlay/OSA framework then provides gateway functionality between applications and Service Capability Features (SCF’s) of the IN. M-Commerce applications can then access core network functionality, e.g. inquire status and location of a mobile user, send messages or place calls. Parlay/OSA applications are portable among networks which is usually not possible with IN services. Security is an important issue, since Parlay/OSA potentially opens the core network to intruders. Parlay/OSA specifies authentication and encryption on the application layer. But the security also depends on the underlying network architecture, e.g. firewalls and strict policies should protect core network components.

4.3.3 SMS

SMS (short message service) is a very popular data service for GSM networks. Although SMS messages are limited to 160 characters, a considerable number of m-commerce scenarios are based on this service. The sender and receiver of an SMS are identified by its IMSI which an attacker cannot forge without breaking the GSM/UMTS security mechanisms (e.g. by cloning a SIM card). Hence SMS messages can be used for authentication (at least towards the network). Furthermore, SMS data is transmitted in the GSM (UMTS) signaling plane, which ensures the confidentiality of messages. However, the protection ends in the GSM or UMTS network, there is no end-to-end security, and the network operator and its infrastructure (e.g. SMSC, Short Message Service Centre) must be trusted (when no other security mechanisms are applied to the SMS message, confer section on SIM/USIM Applications below).

4.3.4 USSD

The GSM Unstructured Supplementary Service Data (USSD) service allows data communication between a mobile station and either the HLR, VLR, MSC or SCP in a way transparent to the other network entities. Unlike the asynchronous SMS service, an USSD request opens a session which may induce other network operations or an USSD response before releasing the connection. Mobile originated USSD may be thought as a trigger for a network operation. USSD works with any mobile phone since the coded commands are entered in the same way as a phone number. With USSD, roaming can be offered for prepaid GSM customers before IN services (CAMEL) are implemented in a network. Another USSD application (requiring CAMEL phase 2) is replenishing a prepaid account by incorporating the voucher number in an USSD string. In principle, any transaction, e.g. a payment operation, could be triggered by USSD data. USSD possesses no separate security properties; instead it relies on the GSM/UMTS signaling plane security mechanisms.

4.3.5 SIM/USIM Application Toolkit

The SIM and USIM Application Toolkits (SAT and USAT respectively) allow operators and other providers to create applications which reside in the SIM/USIM. These
applications can e.g. send, receive and interpret SMS or USSD strings. Currently, there exists banking applications using SAT. The required security mechanisms are:

- Authentication
- Message Integrity
- Replay detection and sequence integrity
- Proof of receipt and proof of execution
- Message Confidentiality
- Indication of the security mechanisms used

However, it depends on the applications whether these security mechanisms are implemented and whether their cryptographic strength is sufficient.
Chapter 5

EMERGING M-COMMERCE APPLICATIONS

There are potentially an unlimited number of mobile applications, we attempt to identify several important classes of applications and provide examples within each class. Table 5.1 summarises the different types of Mobile Applications with their category and examples.

<table>
<thead>
<tr>
<th>Type of Mobile Applications</th>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Advertising</td>
<td>B2C</td>
<td>Sending user-specific and location advertisements</td>
</tr>
<tr>
<td>Mobile Inventory Management</td>
<td>B2B,B2C</td>
<td>Location tracking of goods, people, etc</td>
</tr>
<tr>
<td>Mobile Shopping</td>
<td>B2C,B2B</td>
<td>Ordering items by a mobile device</td>
</tr>
<tr>
<td>Wireless Reengineering</td>
<td>B2C,B2B</td>
<td>Improvement of Business Services</td>
</tr>
<tr>
<td>Mobile Office</td>
<td>B2C</td>
<td>Working from traffic jams, conferences, etc</td>
</tr>
<tr>
<td>Wireless Data Center</td>
<td>B2B,B2C</td>
<td>Information downloaded by mobile users / vendors</td>
</tr>
<tr>
<td>Mobile Entertainment</td>
<td>B2C</td>
<td>Video on demand and other services</td>
</tr>
<tr>
<td>Mobile Distance Education</td>
<td>B2C</td>
<td>Taking a class using streaming audio and video</td>
</tr>
</tbody>
</table>

Table 5.1: Different types of Mobile Applications
5.1 Mobile Financial Applications (MFA)

Mobile financial applications are likely to be one of the most important components of m-commerce. They could involve a variety of applications such as mobile banking and brokerage service, mobile money transfer, and mobile payments as shown in the figure. One interesting mobile financial application is micro payment involving small purchases such as vending and other items. A mobile device can communicate with a vending machine using a local wireless network to purchase desired items. Micro-payments can be implemented in a variety of ways. One way is that the user could make a call to a certain number where per minute charges equal the cost of the vending item. This approach has been used by SONERA, a finish wireless provider, in the famous Coke machine service. In effect it collects money from the users and credits it to the vending providers. Figure 5.1 below shows various Mobile Financial Services available presently (cf. [13]).

![Figure 5.1: Several Mobile Financial Services](image)

5.2 Mobile Advertising

Mobile advertising is also a very important class of mobile commerce applications. Using demographic information collected by wireless service providers and information on the current location of mobile users, much targeted advertising can be done. The advertising messages sent to the user can be location-sensitive and can inform a user about various on-going specials (shops, malls and restaurants) in surrounding areas as shown in Figure 5.2 below which shows a possible scenario for mobile advertising and shopping.

This type of advertising can be performed using Short Messaging Service (SMS) or by using short paging messages to mobile users. The messages can be sent to all users located in a certain area, a user-specific message can be sent independent of the users’ current location. Since the services need the current location information of a user, a third party may be needed to provide location services. However this may require a sharing of revenues between the network service provider and location service provider. As more wireless bandwidth becomes available, content rich advertising involve audio, pictures and video clips can be produced for individual users.
with specific needs, interests, and inclinations. It is also possible that direct advertising to users may be performed without much control from the wireless service providers.

Figure 5.2: A possible scenario for mobile advertising and shopping

5.3 Mobile Inventory Management (MIM)

This class of application involves location tracking of goods, services and even people. The tracking of goods may help service providers in determining the time of delivery to customer, thus improving customer service and obtaining a competitive edge over other business. One very interesting application is rolling inventory—which
may involve multiple trucks carrying a large amount of inventory while on move. Whenever a store needs certain goods/items, it can locate a truck (preferably in nearby area) and just-in-time delivery of goods can be performed. The rolling inventory and delivery application can reduce the amount of inventory space and cost for both vendors and stores and may reduce the time between when an order is placed and the goods are delivered (shown in figure 5.3 above) (cf. [13]).

Location tracking of components can be broken into two components: indoor and outdoor. Indoor tracking can be performed by a chipset (TX/RX) and location information may be transmitted over a satellite or cellular/PCS system to the component supplier where such information is needed.

5.4 Product Location and Search (PLS)

![Diagram of Product Location & Search](image)

Figure 5.4: *Product Location & Search*

This class of application includes locating an item in a particular area or location. This is concerned with finding an item with certain specifications and whether it is available in a specified area or not. Potentially, there could be multiple places where such an item or items of similar attributes are located. Currently many people are going to several stores to find an item (certain brand/size of TV, VCR or an automobile) and compare prices and features. Using a mobile device and centralized/distributed database containing information on products, a user should be able to find the exact location of the store where a certain item is located. After that the user can buy online using a browser on his/her mobile devise. In the case of multiple stores/vendors carrying an item desired by a user, they could compete to get customer by real time manipulation of prices or by offering instant discounts. From the technological point of view, a mobile user can send a query message to a centralized location (shown in figure 5.4 above), which in turn can interface several different stores/dealers and decide if the item is available or not (cf. [10]).
5.5 Proactive Service Management

This class of application is based on collecting pertinent information about current or near future user needs and providing services to users proactively. One such application may involve collecting information about the aging components of an automobile (shown in figure 5.5 below).

Figure 5.5: *Information Transmission on aging Automobile components to dealers*

This would help reduce anxiety levels of owners and improve the general conditions of automobiles on the road leading to the reduced number of traffic jams, accidents and even fatalities. From the technological point of view, automobiles can be equipped with smart sensors that keep track of how much wear and tear a car component has gone through. This information can then be transmitted using a radio/microwave/satellite system to a specified service center or other location. Some implications of such applications are privacy, security, reliability and cost of deployment.
Chapter 6

M-PAYMENT

This section gives an introduction to payment mechanisms for m-commerce. First, we will motivate the heterogeneity of payment system solutions, before categorizing e-payment and m-payment systems respectively. Figure 6.1 below shows the different Payment Mechanisms for Mobile Services.

Table 6.1: Different Payment Mechanisms

6.1 Background on payment systems

E-payment systems provide means for payment of goods or services over the Internet. In contrast to conventional payment systems, the customer sends all payment-related data to the merchant over the Internet; no further external interaction between customer and merchant is required (e.g. sending an invoice by mail or confirmation by fax). To date, there exist more than 100 different e-payment systems.
6.2 Distinctive features of payment systems

There exist a large number of payment systems for E- and M-payments. The following distinctive features of payment systems motivate this diversity (cf. [12]).

- Time of payment
- Payment amount
- Anonymity issues
- Security requirements
- Online or offline validation

Time of payment denotes the relation between the initiation of a payment transaction and the actual payment. In pre-paid payment systems, the customers account is debited before the payment and the amount is stored, for example, on smart cards, in specific customer accounts or as electronic cash. In pay-now payment systems, the customers account is debited at the time of payment and in post-payment systems, payment can be regarded as a 'payment promise' where the merchants account is credited before the customers account is debited (for example, credit card systems). The payment amount has an influence on the design of electronic payment protocols.

Electronic payment systems often originate with conventional payment systems. As such, cash-like payment systems should provide anonymity to the customer. Generally, integrity, authentication, authorization, confidentiality, availability, and reliability issues need to be considered, depending on the specific requirements of an electronic payment system. Offline payment validation means that no third party is involved during the payment procedure, whereas Online payment validation involves some kind of background payment server as a trusted third party. The latter causes an additional communication overhead, but reduces certain risks, e.g. double spending. The above discussion summarizes some distinctive features of payment systems. There are other issues such as

- Overhead imposed on customers and merchants (e.g. installation of software, registration)
- Performance (e.g. response times)
- Cost incurred per payment transaction
- Fulfilment of the ACID (Atomicity, Consistency, Isolation, Durability) principle for payment transactions (i.e. transactions have to be executed all or nothing, leaving the system in a consistent state, and their effect should be durable)
- National or international deployment

The above list of distinctive features gives an idea of the complexity and variety of payment systems.
6.3 Categorization of M-payment systems

Most e-payment systems are not suitable for use in a mobile context, i.e., using a mobile device and communicating over a mobile telecommunication network (cf. [1]). This is due to the special characteristics of mobile devices and mobile telecommunications. Consumers can use many forms of payment in mobile commerce, including:

- Premium-rate telephone numbers- which apply charges to the consumer’s long-distance bill
- Charges added to the consumer’s mobile telephone bill, including deductions to pre-paid calling plans
- Credit cards - Some providers allow credit cards to be linked to a phone’s SIM card
- Micropayment services
- Stored-value cards, often used with mobile-device application stores or music stores.

In the following, we categorize m-payment systems according to the whereabouts of the customers money:

1. Software electronic coins - electronic money stored on the mobile device in file format.
2. Hardware electronic coins - electronic money stored on the mobile device on a smart card.
3. Background account - electronic money stored in a remote account at a trusted third party.

6.3.1 Software electronic coins

In this case, monetary value is stored on the mobile device and the customer has full control of his/her money wherever he/she goes and whatever he/she does. An electronic coin is represented as a file containing, among other information, a value, a serial number, a validity period, and the signature of the issuing bank. Since software electronic coins are easy to copy, the validity of an electronic coin depends on its uniqueness in terms of its serial number. The customer transfers electronic coins to the merchant, who forwards them to the issuing bank for the 'double spending test'. In this test, it is checked whether the electronic coin has been spent beforehand. If yes, it is rejected. Otherwise, its serial number is entered into the double spending database and the money is credited to the merchants account. Due to the limitations of mobile devices, electronic coins may have to be generated and stored externally, until they are downloaded onto the mobile device.
6.3.2 Hardware electronic coins

In this case, monetary value is stored on a secure hardware token, typically a smart card, in the mobile device. The presentation of electronic money is not important, as long as it is stored securely on the smart card. Electronic money could be represented as a simple numeric counter. In order to get to the money, the customer’s smart card and the merchant’s payment server authenticate each other and a secure channel is set up between them. Then, electronic money can be transferred from one to the other. This approach is quite attractive because smart cards provide an additional level of mobility. That means the payment smart card can also be used in POS transactions.

6.3.3 Background account

Here, the money is stored remotely on an account at a trusted third party. Depending on the specific payment system, the account could be a credit card account, a bank account, or an account held at the network operator. Common to all scenarios is that, on receipt of an invoice, the customer sends an authentication and authorization message to the merchant that allows the trusted third party (that holds the account) to identify the customer and to verify the payment authorization. The accounts can then be settled. There are numerous payment systems that fall into this category. The differences are regarding the nature of the trusted third party and the procedure to send authentication and authorization data. For example, in some cases this data is sent in the clear (e.g. a credit card authorization) not providing any security against eavesdropping and in some cases this information is encrypted and digitally signed, providing anonymity to the customer (e.g. SET - Secure Electronic Transactions).

6.4 Standardization and forums

One important aspect of m-commerce is standardization. Due to the heterogeneity of technologies for mobile devices, and the need for transmission and payment over the air interface, it is essential to find common approaches, both at a national and an international level. The following list summarizes standardization bodies and forums dealing with issues relating to m-commerce:

- PayCircle® (www.paycircle.org) - is a vendor-independent non-profit organization. Its main focus is to accelerate the use of payment technology and develop or adopt open payment APIs (uniform Application Programming Interfaces) based on XML, SOAP, Java and other Internet languages.

- MoSign (www.mosign.de) - banks, technology partners and end-device manufacturers have joined forces in the MoSign (Mobile Signature) project to create a platform for secure, legally binding mobile transactions based on existing standards.
• Mobile Payment Forum (www.mobilepaymentforum.org) - is a global, cross-industry organization dedicated to developing a framework for standardized, secure, and authenticated mobile commerce using payment card accounts.

• mSign (www.msign.org) - the Mobile Electronic Signature Consortium is an association of companies and organizations from the mobile phone and Internet sectors. The objective is to establish and develop a secure cross-application infrastructure for the deployment of mobile digital signatures.

• mwif (www.mwif.org) - the Mobile Wireless Internet Forum (MWIF) is an international non-profit industry association. Its mission is to drive acceptance and adoption of a single open mobile wireless and internet architecture that is independent of the access technology.

• Radicchio (www.radicchio.org) - As a non-profit organisation, Radicchio brings together market leaders to establish a common foundation for secure m-commerce by reaching a consensus on important inter-operability issues.

• Encorus (www.encorus.com) - Encorus Technologies is focused on building a flexible and open infrastructure and efficient payment processing services to drive the acceptance and usage of mobile payments worldwide.
Chapter 7

CONCLUSIONS AND FURTHER RESEARCH

7.1 Harnessing M-Commerce potential

In India, m-commerce is in its initial stages and its advantages will soon be realized. M-commerce revolution will take the country by storm since statistics are on our side. Another encouraging trend is that the Indian consumer is fast maturing and is open to new ideas.

Some key points:

• About 2 percent of Indians, which is 20 million people, have a per capita income exceeding 13,000 dollars - a number greater than the populations of Malaysia and Singapore put together.

• Customers surfing the Internet through their mobile phones will have to pay an access charge of only Rs 0.42 per minute. These trends suggest that a fertile ground for m-commerce already exists in India and its revolution seems inevitable.

7.2 Interesting Research Areas in M-Commerce

There are many interesting research problems in mobile commerce. Some of these are unique due to the limitations of mobile devices and wireless networks and some are similar to research problems that are currently being addressed by e-commerce research developers. The problems that are unique to m-commerce are:

• Novel applications and services made possible due to the wireless networks and mobile devices.

• Security and privacy problems that is unique to wireless networks and mobile devices.

• Middle-ware issues that are unique due to device, network and protocol limitations
• Role of different wireless networking standards
• Adoption factors of mobile devices that are significantly different in different parts of the world
• Context and location awareness in unique to mobile commerce as many of the applications are sensitive to the context and the location of a user.

The research problems that can be addressed by the existing e-commerce research with some modifications and extensions are:

• Strategy of new service offering
• Role of m-commerce providers
• Trust building
• Adoption of new services
• Pricing models and sensitivity analysis.

Mobile commerce is an interesting and challenging area of research and development. It presents many issues that cover many disciplines and may best be addressed by an active participation of computer and telecommunications experts, social scientists, economists and business strategists.

M-commerce introduced several new classes of applications, reviewed networking requirements, and discussed application development support. Since the area of mobile commerce is very new and still emerging, several interesting research problems are currently being addressed or should be addressed by the research and development community. It is believed that user trust will play a crucial role in acceptance and widespread deployment of mobile commerce applications. Regarding m-payment, some systems are under development or already operational. One of the main future challenges will be to unify payment solutions, providing the highest possible level of security.
Bibliography


[7] GSM 03.48 version 8.3.0 release 1999. Digital cellular telecommunication system (Phase 2+); Security Mechanisms for the SIM application toolkit.


[10] UNDERSTANDING USABILITY in Mobile Commerce, by Viswanath Venkatesh, V. Ramesh, and Anne P. Massey


