AMCIS 2003 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2003

Mobile and Wireless Information Systems: What We Know and What We Need to Know

Upkar Varshney
Georgia State University

Recommended Citation

Varshney, Upkar, "Mobile and Wireless Information Systems: What We Know and What We Need to Know" (2003). *AMCIS 2003 Proceedings*. 425.
http://aisel.aisnet.org/amcis2003/425

MOBILE AND WIRELESS INFORMATION SYSTEMS: WHAT WE KNOW AND WHAT WE NEED TO KNOW

Upak Varshney
Department of Computer Information Systems
Georgia State University
uvarshney@gsu.edu

Abstract

Mobile and wireless information systems received considerable interest in research and development communities. They lead to significant advances, which will affect our life both as users and researchers of mobile and wireless technologies. In this tutorial we discuss both the current state of mobile and wireless information systems and the challenges in the wide-scale deployment and usage of these systems. In particular, we address applications, wireless networks, mobile payments, challenges and research problems.

Keywords: Wireless and mobile networks, applications, mobile payments, research problems

Introduction

Mobile and wireless information systems can be described as systems involving mobile devices, users, wireless and mobile networks, mobile applications, databases, and middleware. Advances in each one of these areas influence all of mobile and wireless information systems. For example, faster wireless networks can have profound effects on mobile applications that could be used by mobile devices. Faster databases could reduce the end-to-end delays (latency) for mobile applications. From many angles, mobile and wireless information systems are likely to experience significant research, development, deployment, and adoption in the next few years. Some of this optimism stems from the current trends and projections for the future. At present, there are more than 1.2 billion wireless devices. In 2002 wireless devices exceeded the total of all other devices including "wired" telephones, TV, and computers worldwide (CTIA, 2002). It is projected that wireless handheld devices will reach 2 billion before the end of year 2007 (or even earlier). This proliferation has profound implications for business, education, users, and governments. All these devices will be networked and many new applications must be designed to work with these devices and networks. Many major issues related to wireless and mobile infrastructure need to be resolved because this infrastructure is likely to play a major role. In this tutorial, we address both the current state of the mobile and wireless information systems and the challenges in the wide-scale deployment and usage of these systems. In particular, we address applications, wireless networks, mobile payments, challenges, and research problems.

Applications

In addition to the current voice and data centric applications, the emerging applications could include mobile financial services (banking, brokerage), mobile advertising (user/location sensitive), proactive service management, location-based services, mobile auction, and mobile entertainment services, and wireless data center applications. These applications are likely to be more user-centric and highly personalized, context and location aware and more transaction-oriented. These applications will also involve multiple devices, networks, or user types and would likely to be more global in nature.

Many of these new applications have been proposed by wireless researchers (Varshney, Vetter, and Kalakota 2000, Varshney and Vetter 2002). However, only few of these (such as mobile financial applications, mobile advertising and location-based services) are beginning to be offered by wireless service providers (Varshney 2002).

Mobile financial applications consist of mobile banking and brokerage services, mobile money transfer, and mobile payments. It is projected that the number of users making mobile payments will reach to a total of 285 million in Western Europe, Asia and North America by 2005 (Report 2002). Many banks in Europe are supporting basic mobile financial applications to reach to a large base of mobile and wireless users.

Location and user-sensitive advertising is another mobile application in progress. By keeping track of user's purchasing habits and current location, very targeted advertising can be performed. In one possible scenario, a woman could be informed about various on-going specials in her close vicinity or a selected area of interest. These messages can be sent to all users who are currently in a certain area (identified by advertisers or even by users) or to certain users in all locations (Varshney 2002). Depending on interests and personality types of individual users, advertisers could decide whether "push" or "pull" form of advertising is more suitable. It should be noted that issues of privacy and sharing of user information with other providers need to be resolved. It is likely that an "opt-in" approach would be implemented where explicit user permission is obtained before "pushing" any advertising contents.

Location-based services utilize location information to provide specialized contents to mobile users. The contents could include information on desired restaurants, devices, users, and products (Figure 1). One user could be interested in knowing availability and waiting time at one or more restaurants close to his current location (pull). Another user would like to be alerted when one of her friends is in the same general area (push). Location information of fixed entities can be kept in separate databases for each area, while location tracking of mobile and portable entities could be performed as and when needed (on-demand). When a user enters a designated area, user information from previous networks and locations are accessed to allow a determination of location-aware services the user has subscribed to or is authorized to access. Currently, there are a few examples of location-based services, not necessarily personalized or user-specific. These include mapping, routing, and lists of places in a users' vicinity (Varshney 2002).

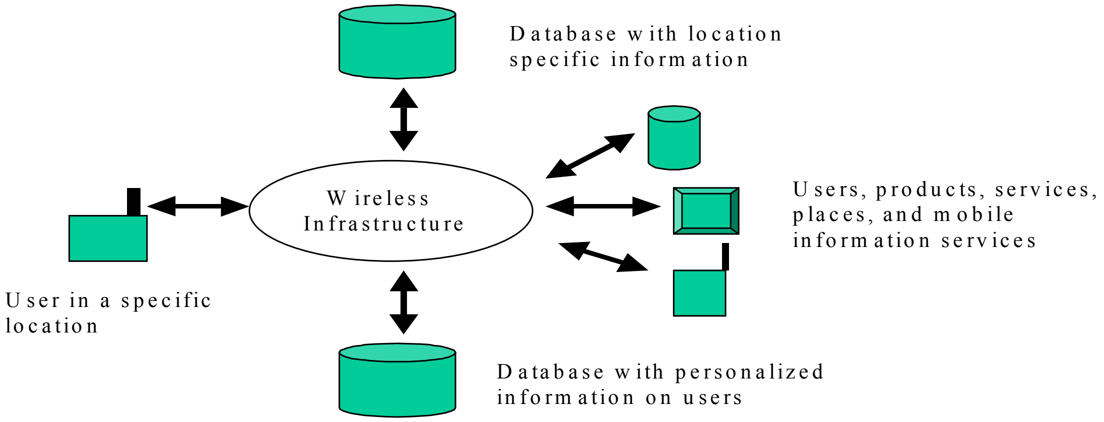
Database with location specific information
Wireless Infrastructure
Users, products, services, places, and mobile information services
User in a specific location
Database with personalized information on users

Figure 1. Location-Based Services

In addition to the basic versions of these applications, more sophisticated applications involving increased user personalization and context awareness must be offered. Although it is difficult to suggest a "killer" applications, we believe that mobile games, personalized contents, entertainment services, mobile auction and trading, and product recommendation systems could give a boost to mobile and wireless systems. Mobile and multiparty games could become major drivers. Entertainment contents will attract some users especially if the contents can be tailored to different user groups and interests. Other applications such as mobile office, mobile distance education, and wireless data center (applications where a large amount of stored data to be made available to mobile users for making "intelligent" decisions) could add value to m-commerce services (Varshney and Vetter 2002).

Wireless Networks

Several different types of wireless and mobile networks are available today. Unfortunately, there are multiple standards for each type. For Cellular and Personal Communications Systems, the US standards include analog cellular, digital cellular, two versions of PCS based on time and code division multiple access, and GSM, the common European standard for wide area cellular service.

One attraction behind GSM is General Packet Radio Service (GPRS), a packet data service for up to 160 Kbps. GPRS is currently being deployed in many US cities as some major carriers introduce GSM/GPRS for high-speed data transmission. Another technology is Enhanced Data rate for GSM Evolution (EDGE), a 2.5 generation technology being used as a transition technology to the emerging 3rd generation wireless systems. It can support up to 384 Kbps by using link quality control, which adapts the error control technique to the current channel quality. Multiple standards also exist among CDMA, including the one used by DoCoMo in Japan for its iMode service. In addition, there are multiple proprietary wireless networks such as wireless WANs (28.8-128 Kbps), Satellites (9.6-400 Kbps, possibly higher), Wireless Local Loops (1-10 Mbps or even higher). Multiple standards also exist for wireless LANs, multiple IEEE 802.11 standards in 1 to 54 Mbps range and HIPERLAN2 at 54 Mbps. These multiple standards also differ in coverage and access protocols. The multiple standards in wireless and mobile networks make interoperability much more difficult, limit roaming between networks, and slow down the development of new features. Although many proposed solutions (such as a worldwide common standard for terrestrial wireless services) exist, interoperability remains a distant dream (Varshney 2002). A comparison of several wireless and mobile networks is shown in Figure 2.

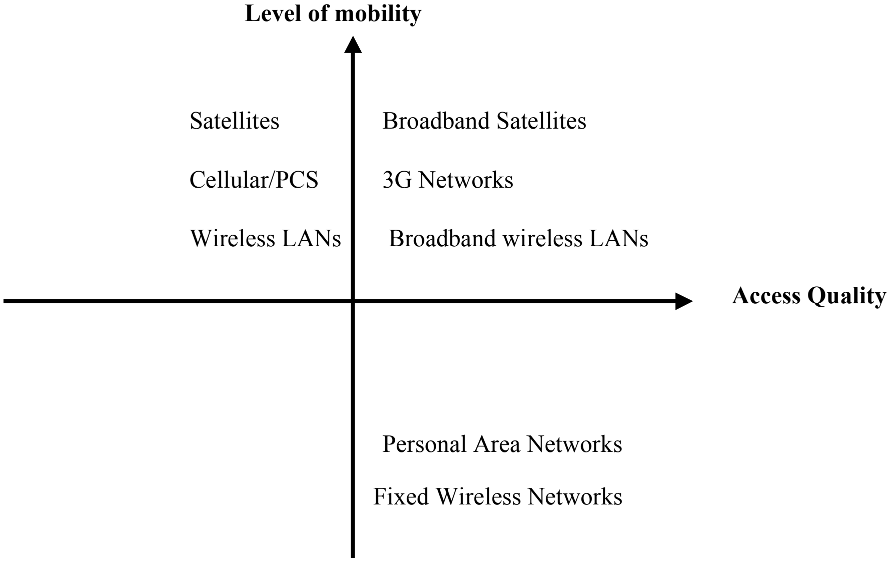

Figure 2. Mobility and Access Quality

Wireless LANs

Wireless Local Area Networks are designed to provide support for mobile computing in a small area, such as a building, hallway, park, or office complex. They can extend or replace wired LANs (such as Ethernet) and can be designed for both infrastructure and ad-hoc configurations. The primary uses of WLANs are LAN extension, nomadic access by deploying in hot-spots, and switching among WLANs and cellular networks and broadband access (>=2Mbps) to the Internet (Stallings, p. 434). The future uses of standards such as 802.11 (see Table 1) would evolve into areas such as wireless digital communities, m-commerce transactions and financial services, and location-based services.

Wireless LAN requirements are throughput, number of nodes, connection to backbone LANs, service area (100-300meters), battery power consumption, interference, security, co-located network operation (multiple WLANs), license-free operation, handoff/roaming (from one cell to the other) and dynamic configuration (Stallings, p. 437, 2002). Unlike cellular networks where a frequency (channel) is allocated, users in WLANs share frequencies. Because many simultaneous users may cause packet collisions (and hence waste of channel bandwidth), it is important that packet collisions be avoided. The choice of frequency depends on whether microwave, spread spectrum, or infrared type communication will be used. Since infrared cannot penetrate walls, it does not require licensing from the FCC. Microwave or spread-spectrum does require FCC license. However, some exceptions do exist, including the Industrial, Scientific and Medical (ISM) bands (902-928 MHz (U.S.), 2400-2483.5 MHz

(Worldwide), and 5725-5850 MHz (U.S.)) respectively. The ISM bands are designated for unlicensed commercial use and are widely used by ambulances, police cars, taxicabs, and Citizen Band (CB) radios.

Interference and security depend on the type of communications method used in the WLAN. Because infrared cannot penetrate walls, it encounters very little interference from external sources but is limited in its coverage. Spread-spectrum was designed during WW-II to avoid frequency jamming by enemies by spreading the signal over a wide frequency range. For security, some form of encryption may be used. If the ISM band is used, some interference is likely to occur because the band is open to other users/agencies. Security problems in general are caused by increased vulnerability due to open-air transmission, difficulty in encryption with smaller devices with somewhat limited abilities and weaknesses in many wireless standards (such as IEEE 802.11). In addition, the unlimited mobility in ad hoc wireless networks makes the security functions even harder. There are multiple standards for wireless LANs as shown in Table 1.

Table 1. Multiple Versions of 802.11

Wireless LANs → **Characteristics**	802.11	802.11b	802.11a	802.11g
Spectrum	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz
Max. physical rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps
Layer 3 data rate	1.2 Mbps	6-7 Mbps	32 Mbps	32 Mbps
Frequency selection	Frequency Hopping or Direct Sequence	Direct Sequence only	Orthogonal Frequency Division Multiplexing	OFDM
Compatible with	None	802.11	None	802.11 and 802.11b
Major advantage	Higher range	Widely deployed High range	Higher bit rate in a less crowded spectrum Smaller range	Higher bit rate in 2.4 GHz spectrum Higher range than 802.11a

802.11a uses OFDM (orthogonal frequency division multiplexing), a multi-carrier technique, where up to 52 carriers are used to transmit data from a single source to achieve a 54 Mbps channel bit rate. The problem with 802.11a is that it uses a different spectrum and is not backward compatible to 802.11b (although dual-band adapters allowing access to both 80211.a and 802.11b could address this problem). 802.11a signals travel less distance with same power, thus requiring more access points to cover the same area. 802.11g is a standard under consideration and will be backward compatible with 802.11b because it uses the same ISM band and provides the higher bit rates of 802.11a. Apple is already offering products with 802.11g support. Dual band adapters combining 802.11a and 802.11b are available. 802.11g will become a standard in mid 2003 and adapters covering 802.11a, b, and g together are available now.

Wireless LANs and Hot-Spots

Hot-spots are areas where either the current or expected network traffic exceeds the wireless capacity available. To support users in such areas, primarily airports, down towns, and busy places, wireless LANs are currently being deployed. Such deployment of wireless LANs in hotspots (Figure 3) can occur in one of the two ways. Wireless LANs can be backboned by fiber or wireless links to the Internet without going through cellular and PCS providers. This approach is termed a pure WLAN to Internet architecture. In this architecture, two possible choices are interconnecting all wireless LANs to a central point or direct lines joining a group of co-located wireless LANs to lots of other wireless LANs. If location management is necessary, then the location management accuracy is equal to one access point coverage. In the second architecture, wireless LANs support handoffs to other wireless networks and then all networks connect to the Internet. In this architecture, location management accuracy is higher due to E911 and other precise location schemes that could be deployed in this environment. It will be possible to design network architectures that will allow switching to the overlapping wireless networks based on the multiple requirements. For example, applications with m-commerce transactions needing better Quality of Service or real-time could be handed off to cellular/PCS/3G networks. Similarly, those requiring broadcast or multicast can be linked to satellites with some outdoor restrictions, also if overload occurs. This handoff could be implemented to support atomic (all or none steps) transactions. One big issue is how to support context-awareness in such an architecture.

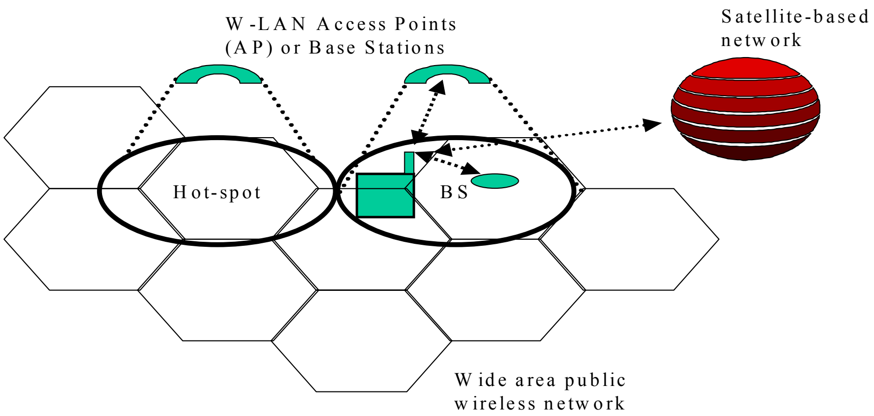

Figure 3. Hot Spots and Multiple Wireless Networks

Deployment of Wireless LANs in Hot-Spots

T-mobile USA, a wireless company, offers 802.11 access for more than half of the hot-spots in the US. The company is experiencing steady growth as tens of thousands of users access the Internet from its 802.11 networks from many places including Starbucks Coffee shops. The prices are reduced to $30/month and $6/day for a 1-day pass. The company plans to offer service packages and plans with a common bill for access to WLAN and traditional wireless networks. McDonalds and Intel announced plans to offer wireless LAN access free with the purchase of certain combo meals. Many cities including Portland, Oregon are planning to offer free WLAN access as a potential economic development tool for the city businesses and users. There has been some progress on switching users in real-time for Internet access from a WLAN to a GPRS system. The wireless carriers are expected to consider this an option. Telesea is offering WLAN access at cruise ships to keep vacationers from feeling alone (meaning not connected). Toshiba and accenture plans to deploy more than 10,000 wireless LANs using hardware from the former and billing and technical support from the latter. Wi-Fi Alliance (www.wi-fizone.org) started a Wi-Fi ZONE seal of approval for hot-spots where WLAN access is available for a fee. This seal could help set-up a minimum quality of service standard and would also allow users to figure out locations with W-LAN access.

Weaknesses of Wireless LANs

Currently wireless LANs suffer from many limitations. These limitations deal with security weaknesses and lack of multicast and locations management. More work is also necessary to address and evaluate the scalability of wireless LANs in terms of users, distance, and transactions. Before public WLANs become widely adopted, many restrictions must be overcome. The future of wireless LANs would depend on how both technology and business issues are addressed. One major issue would be pricing of services: (1) per transactions, (2) location-based pricing, or (3) monthly flat rate. The merger (or alliance) of wireless LANs in hotspots with wide area wireless networks would be another critical factor in the deployment and usage of wireless LANs. An increased user personalization could also lead to a higher adoption rate of wireless LANs and related services. The other issues that could influence the future of wireless LANs are economic incentives for access and security (Wireless ISP, farnchisors, WiFI carriers, and WiFI aggregators), ease of use (e.g., easy registration at hot-spots, easier setup) and new network management tools for enhanced performance (access, interference, and security management functions) (Henry and Luo, 2002).

To address the demands of future wireless LANs, IEEE High Throughput Task Force (soon to become 802.11n) is considering ways to increase bit rates to 108 Mbps and possibly 320 Mbps. These capabilities could be available in 2005.

Mobile Payments

Many of the emerging mobile and wireless applications would be significantly benefitted, especially those with monetary value, by mobile payment support from the underlying wireless infrastructure. Besides banking and financial applications, paying for items, parking, tickets, and food items would require mobile payments (Figure 4). As applications like mobile advertising could evolve into mobile “paying-for-your attention” service, it could involve a small payment to mobile users for reading and using “targeted” advertisements. Mobile payment trends are expected to become more prominent in the near future as many research firms project that the number of users willing to pay for mobile contents to reach several hundred millions in 2005.

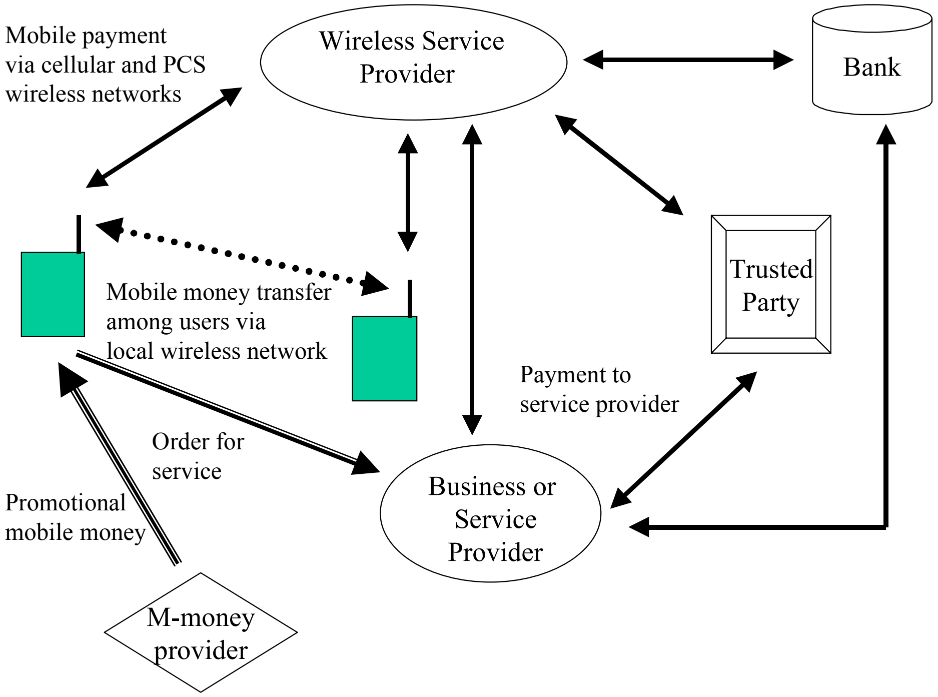

Figure 4. Mobile Payments

It is likely that wireless carriers will play an active role in mobile payments, especially payments with smaller value (micro payments), as mobile users access their networks to perform all transactions. It is possible that one common bill (bundled services) for voice, data, and mobile commerce services would be of some interest to mobile users. Issues, such as the real cost of mobile micro-payments, and how to make any profit on mobile micro-payments, need to be resolved. The possible solutions are (1) pre-payments, (2) reduced cost with an increased numbers of transactions, and (3) the use of micro payment aggregators to reduce payment processing and network traffic caused by a large number of payments with small monetary value. In any case, wireless service providers are likely to be more suitable for providing micro-payment services due to their customer base, technical know-how, and billing experience. For large payments, it is likely that the level of risk involved would deter wireless phone companies from offering this service. Banks and financial institutions could evolve as better candidates. However, much more effort would be required because many significant challenges, including the end-to-end security, must be addressed by financial institutions, which traditionally lack wireless expertise and have no direct access to mobile users.

The current mobile payment offerings include wireless service providers such as Vodafone's mobile payment service in England, Germany, and Italy. Vodaphone is expected to reach to 50 million customers in the near future. US Sprint and eONE made some progress in this area by establishing a mobile payment network in US. The nationwide network would allow people to make mobile payments by multiple ways including e-wallet. The network would allow international payments because it uses PaymentWorks, the same software used by several providers in many European countries. In this joint effort, eOne will supply technologies for multiple channel access, authentication, routing, and settlement of transactions. The payment network would initially support micro-payments and is likely to venture into macro-payments over time. Among the consortia and companies working on mobile payments, is PayCircle, established by HP, Lucent, Oracle, Sun, and Siemens. It will provide APIs to allow vendors to incorporate payment technology in devices. Many of the proposed and current m-payment services would benefit significantly if interoperability of payment systems could be achieved where people using a variety of devices in different countries with different wireless networks can make m-payments in multiple currencies.

Security

The security issues in m-payments are confidentiality, authentication, integrity, authorization, non-repudiation, and accessibility. In m-payments no-one-else should find out what was purchased and how it was paid (confidentiality), merchants and mobile customers must be able to trust the claimed identities (authentication), the value of transactions should not be modified by others, knowingly or unknowingly (integrity), parties involved must be able to verify if everyone involved in such transactions is allowed to make such payments (authorization), and no one should be able to claim that the financial transaction on his/her behalf was made without their knowledge (non-repudiation). Other, non-security issues include convenience, speed, ease-of-use, and standardization.

In addition to security and privacy risks, new vulnerabilities arise in mobile financial applications due to the use of wireless devices. These transactions may involve multiple wireless networks with different levels of security. These networks could lead to possible change/deletion of information, and denial of service. In such an environment, tracing hackers is a difficult job as devices move in and out of multiple wireless networks and many US wireless networks do not authenticate a particular user to a particular device.

There is some support for security in mobile middleware. For example, WAP provides security using Wireless Transport Security Layer (WTSL), but it does not result in the end-to-end security (only between device and WAP gateway). The translation between Secure Sockets Layer (SSL) and WTSL occurs at WAP gateway. These gateways are vulnerable to Denial of Service (DoS) attacks because malicious WML Script may run on a device making other existing security techniques (signing, authentication and encryption) less effective. Several US-based financial companies and associated vendors in Financial Services Technology Corporation (FSTC) are working on implementing end-to-end transaction support for financial applications involving mobile devices, wireless networks, and financial institutions. One of the major hurdles is the end-to-end encryption that is not widely available, but will become possible with widespread deployment and use of WAP 2.0.

It is possible to add some security features for financial services. GSM supports both user (PIN) and device authentication (SSL). Finnish wireless provider Sonera is offering PKI on a SIM card. Another possibility is wireless PKI, a system to manage keys and certificates and requires the user to enter 2 PINs (authentication and digital signature). The WPKI is used in WTSL to support 2-way authentication (anonymous: class 1, server: class 2, user: class 3).

Financial services are supported in I-appli service for iMode phones using a version of Java designed for small devices. This supports both 40 and 128 bit versions of SSL.

Security will dominate any discussions of m-payments, especially, macro payments. Certainly more work is needed in addressing specific security requirements of m-payments and new ways to support m-payment security. It is also possible to introduce location as a constraint in deciding the limit on the monetary value of m-payments, in addition to other traditional constraints such as type of user, past history of payments, and credit availability. The other possible constraints could be the type of wireless network currently used by the people who want to make an m-payment.

Security Issues in 802.11

Wireless security used in IEEE 802.11 has been compromised and several weaknesses have been exposed including breaking of a key in a few minutes by eavesdropping and analyzing the wireless network traffic. Although 802.11 WLANs use WEP (Wired Equivalent Privacy) to provide data integrity and authentication, most 802.11 LANs do not even turn it on. WEP is based on the use of single shared key (common to all users and kept in a software-accessible location). It does not have a key management protocol defined so it is hard to re-key if a device is stolen or the key becomes public. There are two solutions for 802.11 security problems, one short-term and one long term. The short term solution involves adding a patch while the long term solution is based on major changes in the protocol. Another solution (Henry and Luo, 2002) is to use Virtual Private Networks (VPN) with an IPsec (Secure IP) tunnel. This alternative would allow secure and continued access, but because all traffic must be processed by a VPN gateway, scalability (in terms of number of possible users that could be supported) becomes an issue.

Challenges and Research Problems

As discussed in this paper, several challenges must be overcome before mobile and wireless information systems become widely deployed. These challenges include applications and services, security and privacy concerns, support for mobile payments, and wireless infrastructure. Mobile and wireless information systems have attracted a significant attention among research and development communities. Many exciting research problems are being addressed and some that are yet to be addressed. These studies include mobile applications and services, wireless and mobile infrastructure, security and mobile payments. The infrastructure issues and problems of access, coverage, roaming, reliability, location management and multicast communications must be addressed. Mobile applications and services present many challenges. Lack of killer applications has always been a problem with many technologies. Among the many research problems that must be addressed are:

- Design of mobile applications and services
- Personalization, context and location-awareness
- Support for group communications (multicast)
- Reliable communications (dependable infrastructure)
- Inter-working and integration of different wireless technologies
- Introduction of mobile technologies in business and organizations
- Specific infrastructure requirements and the role of local wireless networks (wireless LANs, "3G and beyond" and location-aware infrastructure)
- Design of seamless wireless solutions to work across multiple access protocols, devices, bandwidth, and dependability and quality of service
- Wireless access and security issues
- Mobile payments and pricing issues
- Device and user interface issues

On a positive note, some of these problems are being addressed in the research community and we hope that our paper inspires others to address some of these challenges.

References

CTIA Background on CTIA's Semi-Annual Wireless Industry Survey, **http://www.wow-com.com/**, 2002.

Ghosh, K. A., and Swaminatha, T. N. "Software Security and Privacy Risks in Mobile E-Commerce," *Communications of the ACM* (44:2), February 2001, pp. 51-57.

Henry, P., and Luo, H. "WiFi: What's Next," *IEEE Communications Magazine* (40:12), December 2002, pp. 66-72.

Report on Users of Mobile Payments, **www.allnetdevices.com/wireless/news/2002/02/07/study_mobile.html**, 2002.

Stallings, W. *Wireless Communications and Networks*, Upper Saddle River, NJ: Prentice Hall, 2002.

Varshney, U. "M-commerce Tutorial," ACM Mobicom 2002.

Varshney, U. "Mobile Payments," *IEEE Computer* (35:12), December 2002, pp. 120-121.

Varshney, U., and Vetter R. "Framework, Applications, and Networking Support for M-commerce," *ACM/Kluwer Journal on Mobile Network and Applications (MONET)* (7:3), June 2002, pp. 185-198.

Varshney, U., Vetter. R., and Kalakota, R. "M-commerce: A New Frontier," *IEEE Computer* (33:10), October 2000, pp. 32-38.

Winget, N., Housley, R., Wagner, D., and Walker, J. "Security of 802.11 Data Link Protocols," *Communications of the ACM*, forthcoming.

Appendix: Acronyms

CDMA	Code Division Multiple Access
CTIA	Cellular Telephony and Internet Association
DoS	Denial of Service
EDGE	Enhanced Datarate for GSM Evolution
FSTC	Financial Services Technology Corporation
GSM	Global System for Mobile communications
GPRS	Generalized Packet Radio Service
HIPERLAN	High Performance Radio Local Area Networks
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical
OFDM	Orthogonal Frequency Division Multiplexing
PCS	Personal Communications Systems
PKI	Public Key Infrastructure
SSL	Secure Socket Layer
VPN	Virtual Private Network
WAP	Wireless Applications Protocol
WEP	Wired Equivalency Protection
WLAN	Wireless Local Area Network
WML	Wireless Markup Language
WTSL	Wireless Transport Security Layer