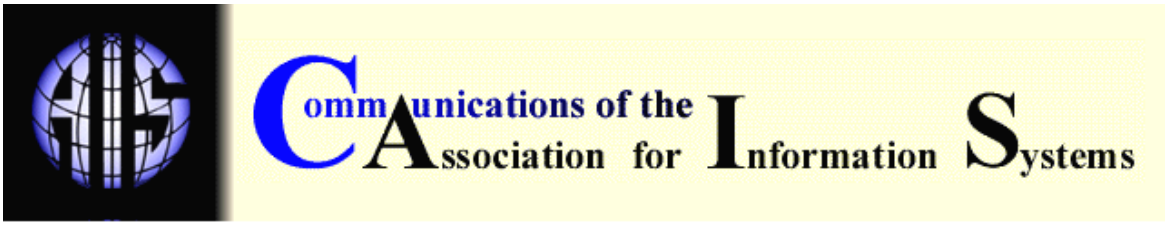
Communications of the Association for Information Systems

Volume 12 Article 11

July 2003

Mobile and Wireless Information Systems: Applications, Networks, and Research Problems

Upkar Varshney
Computer Information Systems, Georgia State University, uvarshney@gsu.edu



WIRELESS I: MOBILE AND WIRELESS INFORMATION SYSTEMS: APPLICATIONS, NETWORKS, AND RESEARCH PROBLEMS

UPKAR VARSHNEY
Department of Computer Information Systems
Georgia State University, Atlanta 30302
uvarshney@gsu.edu

ABSTRACT

Mobile and Wireless Information Systems received considerable interest in research and development communities. As a result, significant advances were made, which will affect our life both as users and researchers of mobile and wireless technologies. In this paper, we discuss both the current state of mobile and wireless information systems and the challenges in the wide-scale deployment and use of these systems. In particular, we address applications, wireless networks, mobile payments, security, challenges and research problems.

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

I. 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 mobile and wireless information systems. For example, faster wireless networks can profoundly affect 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, more than 1.2 billion wireless devices were operational throughout the world. In 2002 wireless devices exceeded the total of all other devices including "wired" telephones, TV, and computers worldwide. Wireless handheld devices are projected to reach 2 billion before the end of year 2007 (or even earlier) [Instat 2003]. This proliferation implies significant 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.

II. MOBILE 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, mobile entertainment services, and wireless data center applications. These applications are likely to be user-centric and highly personalized, context and location aware, and transaction-oriented. Such applications can be supported by storing and analyzing detailed information on user habits, history, and preferences. This analysis, combined with intelligent wireless networks and highly sophisticated and adaptable handheld devices, could make many emerging applications a reality. Also, the progress in context and location-aware infrastructure will benefit the increased personalization of the current and emerging mobile services. With an increasing deployment of diverse wireless networks, applications using multiple devices, networks, or user types could be supported on global scale.

Several new applications are proposed by wireless researchers [Varshney et. al. 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 2003b].

Mobile Financial Applications consist of mobile banking and brokerage services, mobile money transfer, and mobile payments. The number of users making mobile payments are projected to reach over 200 million in Western Europe, Asia and North America by 2005. 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 transmitted. In one scenario, a woman could be informed about various on-going specials in her vicinity or in 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 2002a]. Depending on interests and personality types of individual users, advertisers could decide whether "push" or "pull" form of advertising is more suitable. The 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

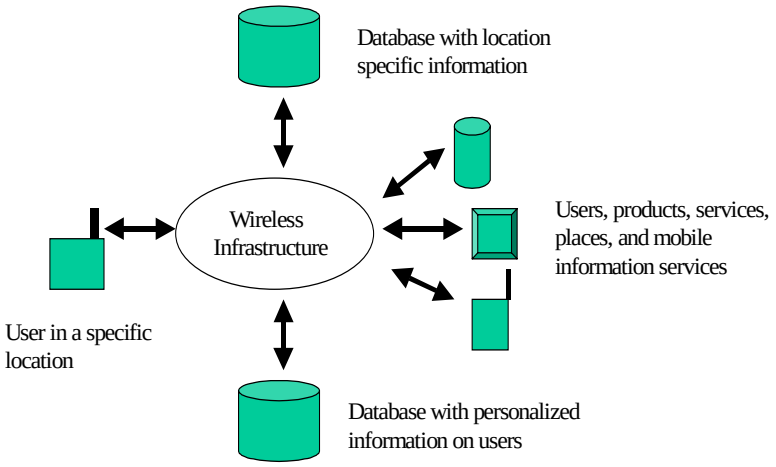


Figure 1. Location-based Services

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 determining location-aware services the user subscribed to or is authorized to access. Currently, only a few examples of location-based services, not necessarily personalized or user-specific exist. These examples include mapping, routing, and lists of places in a users' vicinity [Varshney 2002a].

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” application, 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 mobile services [Varshney and Vetter 2002].

III. WIRELESS NETWORKS

Several different types of wireless and mobile networks are available today. Unfortunately, each type of network involves multiple standards. For Cellular and Personal Communications Systems (PCS) [1], 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 in CDMA, including the one used by DoCoMo in Japan for its iMode service. In addition, multiple proprietary wireless networks are available such as wireless

[1] The wireless field involves many acronyms. A list of the acronyms used in this paper are presented in Appendix I.

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 the 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 wireless and mobile networks, and slow down the development of new features. Although many proposed (such as a worldwide common standard for terrestrial wireless services) exist, interoperability remains a distant dream [Varshney 2002a]. A comparison of several wireless and mobile networks is shown in Figure 2.

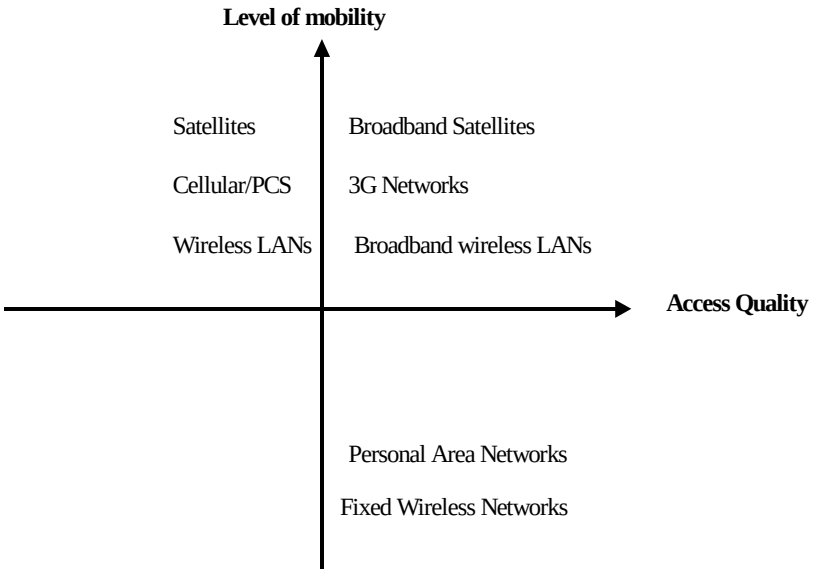


Figure 2. Mobility and Access Quality

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 (see next subsection), and switching among WLANs and cellular networks and broadband access (>=2Mbps) to the Internet [Stallings, p. 434, 2002]. The future uses of standards such as 802.11 (Table 1) would evolve into areas such as wireless digital communities, mobile commerce (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 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 World War 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. The multiple standards for wireless LANs are shown in Table 1 [Varshney 2003a].

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
Maximum 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 the 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 became 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. Wireless LANs are currently being deployed to support users in such areas, primarily airports, downtowns, and busy places. Such deployment of wireless LANs in hotspots (Figure 3) can occur in one of the two ways:

1. 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.
2. 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 service 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.

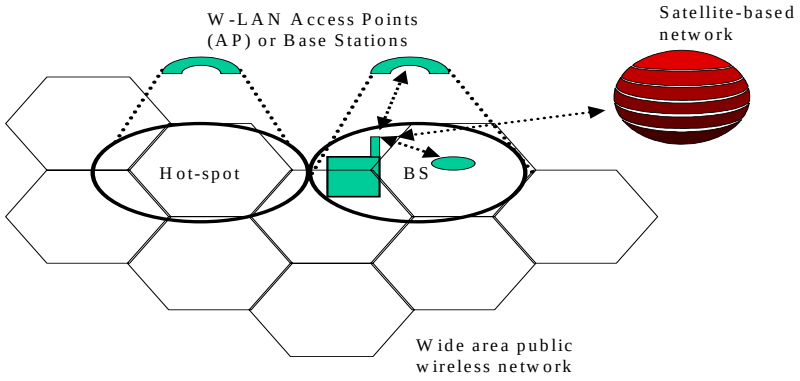


Figure 3. Hot-spots and Multiple Wireless Networks

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. Some progress is reported on switching users in real-time for Internet access from a WLAN to a GPRS system. The wireless carriers are expected to consider this option. Telesea is offering WLAN access on cruise ships to keep vacationers from feeling alone (meaning not connected). Toshiba and Accenture plan 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 verify locations with W-LAN access.

WEAKNESSES OF WIRELESS LANS

Currently wireless LANs suffer from many limitations, including 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. Three options are:

1. per transaction,

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 use of wireless LANs. 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, franchisers, 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 [Varshney 2003a].

IV. MOBILE PAYMENTS

Many of the emerging mobile and wireless applications would be significantly benefited, 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). Applications like mobile advertising could evolve into mobile “paying-for-your attention” service. They would 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.

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 [Varshney, 2002b].

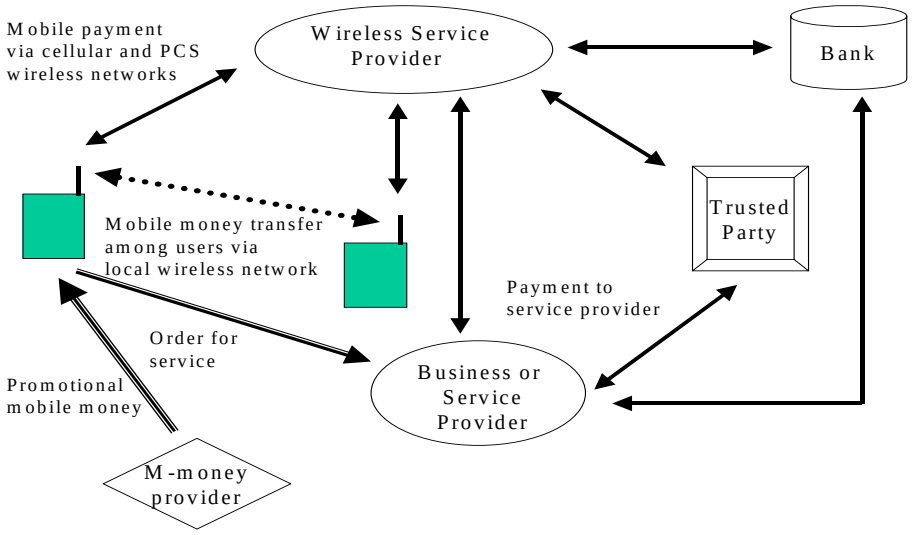


Figure 4. Mobile Payments

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 prove to be better candidates. However, much more effort would be required because many significant challenges, including end-to-end security, must be addressed by financial institutions, which traditionally lack wireless expertise and cannot access mobile users directly.

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 the United States. 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. PayCircle 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.

V. SECURITY

The security issues in m-payments are confidentiality, authentication, integrity, authorization, and non-repudiation.

- *Confidentiality*: In m-payments no-one-else should find out what was purchased and how it was paid.

- *Authentication*: Merchants and mobile customers must be able to trust the identity claimed.
- *Integrity*: the value of transactions should not be modified by others, knowingly or unknowingly.
- *Authorization*: parties involved must be able to verify if everyone involved in a transactions is allowed to make payments.
- *Non-repudiation*: No one should be able to claim that the financial transaction on his/her behalf was made without their knowledge.

Other, non-security issues include accessibility, convenience, speed, ease-of-use, and standardization.

In addition to security and privacy risks, new vulnerabilities arise in mobile financial applications because wireless devices are used. 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 United States wireless networks do not authenticate a particular user to a particular device.

Some support for security is provided by 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 the WAP gateway). The translation between Secure Sockets Layer (SSL) and WTSL occurs at the WAP gateway. These gateways are vulnerable to Denial of Service (DoS) attacks because malicious WML Script may run on a device, thereby making other existing security techniques (signing, authentication and encryption) less effective. Several United States-based financial companies and associated vendors in the Financial Services Technology Corporation (FSTC)[2] 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 at present is that end-to-end encryption that is not widely available; however, such encryption 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. I-appli service provided by DoCoMO in Japan using iMode phones supports few financial services. To provide security for these services, Secure Socket Layer (SSL) protocol is used at either 40 or 128 bit versions.

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 wireless network that is currently being used to make m-payment could also be a factor in limiting the amount of money that can be transferred by its permanently registered users and roaming users.

[2] The Financial Services Technology Consortium (FSTC) is a consortium of North American-based financial institutions, technology vendors, independent research organizations, and government agencies. Its aim is to bring forward interoperable, open-standard technologies that provide critical infrastructures for the financial services industry.

SECURITY ISSUES IN 802.11

Wireless security used in IEEE 802.11 was compromised and several weaknesses were 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). A key management protocol is not defined. Therefore, it is hard to re-key if a device is stolen or the key becomes public [Winget et. al 2003].

A short-term and a long-term solution are available for 802.11 security problems. 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.

VI. CHALLENGES AND RESEARCH PROBLEMS

Mobile and wireless information systems attracted a significant attention among research and development communities. Many exciting research problems are being addressed and some 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. Among the many research problems that must be addressed are:

- **Design of mobile applications and services**: So far only simple versions of mobile services including location-based services, mobile entertainment, and mobile games are currently offered by wireless service providers. More work is also needed to identify new and useful mobile applications and services, including those dealing with personalization of mobile contents. Also new avenues of mobile and wireless applications must be explored such as mobile telemedicine and patient monitoring using wireless infrastructure.
- **Context and location-awareness:** For mobile applications to become more useful, some work is also necessary to include context and location-awareness in both applications and mobile devices.
- **Device and user interface issues:** To increase the usability of mobile services and systems, some work is necessary in designing dynamic, adaptable and smart user interfaces that learn from and with users. The devices should have the ability to accept user input in many forms including voice and be able to display rich and usable contents. The mobile devices could also be designed to include multi network interfaces for an increased and reliable wireless access.
- **Support for group communications:** As many of the mobile applications are likely to involve groups with more than two entities, it would be helpful to support multicast in the network, application and/or middleware protocols to reduce the network traffic that could result from several one to one communications among group members.
- **Reliable communications**: More efforts are necessary towards ensuring that mobile and wireless infrastructure works as expected and does not add errors of its own. Increased reliability would be helpful for several mobile applications such as mobile financial services.
- **Inter-working and integration of different wireless technologies**: Due to the existence of multiple and diverse mobile and wireless technologies, more efforts are needed towards the inter-working and integration of these technologies. Some integration can be made in physical and data link layers. However middleware and application

layers must also be designed to adapt to changing time and location-dependent performance and quality obtained in different mobile and wireless networks.

- **Introduction of mobile technologies in business and organizations:** The introduction of mobile and wireless technologies to businesses and organizations is somewhat slowed due to the difficulty in putting "mission-critical" or other important information on wireless networks that are either not very secure or "perceived" to have weak security. The potential lack of accessibility of wireless networks for continued business operation is also seen as an obstacle. These challenges must be addressed in the organizational context before large-scale deployment of mobile and wireless technologies in businesses become a reality.

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

Editor's Note: This article is based on a tutorial given by the author at the 2003 AMCIS meeting in Tampa Florida. It was received on August 7, 2003 and was published on August __, 2003

REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Ghosh, K.A. and T. N. Swaminatha (2001) "Software security and privacy risks in mobile e-commerce", *Communications of the ACM*, (44:2), February, pp. 51-57.

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

Instat (2003) *Wireless Subscribers to Reach Two Billion by 2007 - CDMA to See Dramatic Growth.* Instat MDR Market Alerts, Reed Electronics Group, *August 6, 2003* http://www.instat.com/newmk.asp?ID=714 (last consulted August 16, 2003)

Stallings, W. (2002) *Wireless Communications and Networks*, Upper Saddle River, N.J. Prentice Hall

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

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

Varshney, U. (2002a) M-commerce Tutorial, ACM Mobicom 2002 (slides available via e-mail: uvarshney@gsu.edu)

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

Varshney, U., (2003a) The Status and Future of 802.11-based WLANs, *IEEE Computer*, (36)6, June, pp.90-93.

Varshney, U. (2003b) Location Management for Mobile Commerce Applications in the Wireless Internet, *ACM Transactions on Internet Technology*, (3)3, August 2003, pp. 236-255.

Winget, N., R. Housley, D. Wagner, and J. Walker (2003) Security Flaws in 802.11 Data Link Protocols, *Communications of the ACM*, (46)5, May, pp. 35-39.

APPENDIX I. LIST OF 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

ABOUT THE AUTHOR

Upkar Varshney is Associate Professor of Computer Information Systems at Georgia State University. He received a B.E. in electrical engineering from the University of Roorkee, India (now Indian Institute of Technology-Roorkee), an M.S in computer science and a Ph.D. in telecommunications and computer networking both from University of Missouri-Kansas City. He is the author of over 70 papers on wireless networks, mobile commerce, wireless multicast, and other topics in major journals and international conferences. Several of his papers are among the most widely cited publications in mobile commerce. He presented more than 50 tutorials, workshops and keynote speeches at major international conferences including ACM Mobicom, IEEE WCNC, IFIP HPN, HICSS and AT&T technology conference. Upkar was awarded the Myron T. Greene Outstanding Teaching Award and the RCB College Outstanding Teaching Award at Georgia State University. He is the guest co-editor of three special issues in mobile computing in computer science journals. He is on the editorial boards of *IEEE Computer, International Journal on Mobile Communications, and the Communications of the AIS*.

Communications of the Association for Information Systems

ISSN: 1529-3181