Communications of the Association for Information Systems

Volume 13 Article 39

June 2004

Wireless Communications: Myths and Reality

Samuel C. Yang
California State University, Fullerton, syang@fullerton.edu

Samir Chatterjee
Claremont Graduate University, samir.chatterjee@cgu.edu

Charlie C. Chan
Appalachian State University, charlieivy@yahoo.com

Recommended Citation

Yang, Samuel C.; Chatterjee, Samir; and Chan, Charlie C. (2004) "Wireless Communications: Myths and Reality," *Communications of the Association for Information Systems*: Vol. 13 , Article 39.
DOI: 10.17705/1CAIS.01339
Available at: https://aisel.aisnet.org/cais/vol13/iss1/39

Communications of the Association for Information Systems

WIRELESS COMMUNICATIONS: MYTHS AND REALITY

Samuel C. Yang
Department of Information Systems and Decision Sciences
California State University, Fullerton
syang@fullerton.edu

Samir Chatterjee
School of Information Science
Claremont Graduate University

Charlie C. Chen
Department of Information Technology and Operations Management
Appalachian State University

ABSTRACT

The use of wireless communications and computing is growing quickly, and wireless technologies are an active area of research and application. Many myths exist about different aspects of wireless computing. The purpose of this article is to examine the more prominent popular beliefs in this area. We address these beliefs using a framework consisting of three dimensions: technology, business, and society. For technology, wireless' limited bandwidth and its effect on new wireless applications and services are discussed. For business, the anticipated revenue opportunities of Wi-Fi and mobile e-commerce are addressed. For society, issues of wireless security and its effect on wireless adoption are examined. Based on these examinations, we propose research directions along each dimension.

Keywords: wireless communications, wireless computing, myths, mobile computing

I. INTRODUCTION

Although one-way wireless systems such as radio and TV have been in use for most of the last century, it was not until the last 20 years until two-way wireless systems became popular. In some parts of world (notably in northern Europe) cellular subscriber penetrations are now over 70%. The number of cellular phones overtook landline phones at the end of 2002 [ITU, 2003]. The popularity of Wi-Fi increased, with the total number of users exploding from 2.5 million in 2000 to over 18 million in 2003.

With the success of wireless wide area networks (WWAN) (e.g., cellular telephony) and wireless local area networks (WLAN) (e.g., IEEE 802.11x), wireless communication is currently a major ot area of discussion from both business and research perspectives. Contradictory positions entrench most issues, and many debates are suspiciously religious in nature instead of based on solid evidence. As a result, many beliefs have surfaced regarding different aspects of wireless communication. The purpose of this article is to address the more prominent popular beliefs in this area. The goal is not to debunk these belief statements. Rather, our intention is *to* present the belief statements and to discuss the underlying issues, and to direct readers and researchers to fruitful areas of further explorations.

A frank and open discussion of popular beliefs is important because these beliefs, when unchallenged, wrong, and carried to their conclusions, can lead to devastating results. For example, as late as 2000 industry participants were still quoting "Internet traffic doubles once every three to four months" when in reality it actually doubled once every year [Odlyzko, 2000]. Based on the myth of Internet traffic growth, the result was an over-investment in the infrastructure and oversupply of capacity. At this writing, the industry is still painfully adjusting to the imbalance between capacity supply and traffic demand.

Wireless technologies developed rapidly in the last few years. Although technology enabled communicating wirelessly, technology is not the only way to examine this broad area. Before we address the myths, it is useful to present a framework organizing different aspects of wireless communications. Figure 1 shows that the framework consists of three dimensions: technology, business, and society. This framework is presented based on the framework developed by Agres et al. [1998], with its three dimensions akin to the driving forces of virtual societies. Adopting the virtual society framework in our analysis is appropriate because a culture that is increasingly using wireless communications predominantly interacts without the need for face-to-face contact with other people [Brown et al., 2002]. In fact, this paper answers the call made to critically examine the important and relevant issue in their contexts [Agres et al., 1998, p. 80].

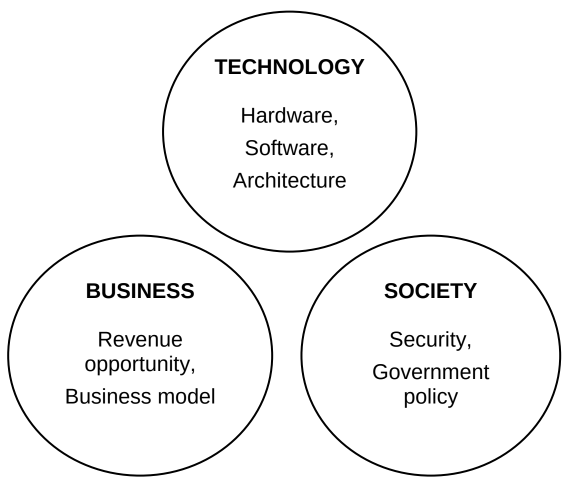

Figure 1. A Framework Addressing the Different Aspects of Wireless Communication

In terms of technology, the literature is dominated by proposals, evaluations, and merits of different technical schemes. While there is no shortage of technical innovations and discussions in the literature on technology, examining wireless communications from the perspectives of business and society are also important. In terms of *business*, the discussion has centered around new ways businesses can make money leveraging wireless. In terms of *society*, it is issues like privacy, security, and government regulations that receive much of the attention. Out of these discussions come many myths regarding either the "best" way of doing things or the de facto current state of affairs. It is our intention to address the more popular myths, which are presented in the subsequent sections in the following order: technology, business, and society, as well as suggest possible future research directions for these areas.

II. TECHNOLOGY

MYTH 1: THE LIMITED BANDWIDTH IN WIRELESS COMMUNICATIONS WILL HINDER THE GROWTH OF NEXT-GENERATION MULTIMEDIA SERVICES TO MOBILE USERS

The belief that wireless communications bandwidth is limited compared to wired communications is widespread. Wireless communications certainly encounters more challenges than wired communications because the surrounding environment interacts with the signal, blocking signal paths and introducing noise and echoes [Foreman and Zahorjan, 1994]. As a result, wireless communication is characterized by lower bandwidths, higher error rates, and more frequent disconnects. These factors in turn produce longer delays, less reliability which can hinder new multimedia services (voice, video, and data) over hand-held devices.

To understand why this belief continues to exist or even if it is valid today, it is important to revisit some basic fundamental concepts in communications. Bandwidth is a measure of the width of a range of frequencies and not the frequencies themselves. For example, if the lowest frequency that can be used in a frequency band is f_1 and the highest frequency is f_2, then the bandwidth available is $f_2 - f_1$. While many wireless applications operate at a precise frequency, that frequency is the center frequency around which voice (or data) is modulated and can change as a subscriber travels from one cell to another. The range of allowable frequencies then represents the bandwidth supported by the particular application.

Data rate (at a given Quality of Service or QoS) is the metric of concern in wireless communications, and data rate is not solely determined by bandwidth. Signal-to-noise (S/N) ratio of the medium also plays a critical role. Signal loses power with distance, and in all communications systems there is noise (due to movement of electrons, induction, cross-modulation, thermal and impulse) which affects the sensitivity of a receiver. In general, data rate is proportional to bandwidth. In addition, for a fixed bandwidth, designers can increase data rates using clever modulation techniques (admittedly at higher S/N ratios). Ultimately, Shannon's Theorem [Shannon, 1948] determines the limits of data rate as a function of bandwidth and S/N ratio.

Furthermore, in wireless communications, one can increase bandwidth by adopting frequency reuse, a method used by a system to provide more usable bandwidth to service a user population. In frequency reuse, either cells of different frequencies overlap or power of transmission is reduced so that more cells of identical frequencies can fit in a given area.

Several advances make this myth less valid today. With more spectrum being released by governments worldwide and advances made in hardware, signal processing, access mechanisms, and software management [Stable and Werbach, 2004], the available data rates to mobile devices are higher today than what were available a decade earlier. In local areas, Wi-Fi (IEEE 802.11) provides higher data rates today. IEEE 802.11b provides 11 Mbps while 802.11a can provide up to 54 Mbps. IEEE 802.11g can potentially achieve up to 54 Mbps. In wide areas, IMT-2000 (3G) is a radio and network access specification that aims to provide the following high-speed packet data rates:

- 2 Mbps for fixed environment
- 384 Kbps for pedestrian
- 144 Kbps for vehicular traffic

Table 1 shows the bandwidths of popular wireless standards.

Table 1. Bandwidth Comparison of Various Wireless Standards

Standard	Bandwidth/Bit-rates	Modulation Technique	Applications
IEEE 802.11b	11 Mbps	DSSS	Network access, home area networks
IEEE 802.11a	54 Mbps	Orthogonal FDM (OFDM)	Wireless campus
3G	Up to 2 Mbps	MQAM, MPSK, turbo codes	Mobile web surfing, transactions, video
Bluetooth	Up to 1Mbps	Gaussian FSK	Peripheral connectivity
LMDS/MMDS	500 MHz, up to 1 Gbps	64-QAM	Wireless cable, multipoint video

In terms of WLAN, Wi-Fi standards are becoming popular in the market. It mostly uses two radio techniques at the physical layer:

- *Direct-sequence spread spectrum (DSSS)* – 2.4 GHz radio that uses complementary code keying (CCK) modulation, and
- *Frequency-hopping spread spectrum (FHSS)* – 2.4 GHz radio that also uses CCK.

As an example, early 802.11b implementations used the FHSS physical layer because it provided superior multi-path resistance [Kapp, 2002]. Allocating a relatively small bandwidth and a high number of channels (79 in total) and moving quickly from frequency to frequency (once every 0.4 seconds) virtually eliminated multi-path. But since FHSS was limited in bandwidth (1-Mbps effective full duplex throughput), it could not keep up with performance demands. As a result vendors have now focused on DSSS. In the U.S., DSSS allocates 11 overlapping channels of 22 MHz bandwidth each. This allocation created three non-overlapping channels that provide 11 Mbps of throughput apiece (5.5 Mbps full duplex) [Kapp, 2002]. Applications are proliferating and industry wide efforts are underway to link up wireless base stations to create large Wi-Fi WLANs.

Therefore, while it is true that we are still several years away from seeing very high bandwidths (like fiber optics) on the wireless side, technological advances made the belief statement less valid. Service providers are rolling out new generations of local and wide area wireless services, which is an indication that consumers can expect more wireless multimedia services in the coming years.

MYTH 2: UMTS PROVIDES THE TRUE THIRD-GENERATION (3G) WIRELESS SERVICE, WHILE CDMA2000 DOES NOT

The terms third-generation (3G) wireless service and Universal Mobile Telephone Service (UMTS) are often used interchangeably in the popular literature. But in actuality whereas 3G is used to describe wireless services that consists of voice and high-speed multimedia data, UMTS refers to one particular standard used to provide 3G services. UMTS is sometimes known as the Wideband Code Division Multiple Access (W-CDMA) which was endorsed by the European Union (E.U.) as the de facto 3G technology.

On the other hand, supporters of cdma2000 also claim it to be a legitimate 3G technology. Although cdma2000 is not officially endorsed by any government entities, it is deployed in North America, South Korea, and Japan to provide voice and high-speed data services. cdma2000 is a natural evolution of the 2G IS-95 CDMA technology that was pioneered by Qualcomm, a San Diego based American company. While Qualcomm does have intellectual claims to the CDMA technology used in both UMTS and cdma2000, it actively lobbies for the adoption of cdma2000 as the implementation of 3G.

In mid 1990s, the International Telecommunication Union (ITU) initiated an effort to develop a framework of standards and systems that will provide wireless and ubiquitous telecommunications services to users anywhere at anytime. This initiative was originally called Future Public Land Mobile Telecommunications Systems (FPLMTS) but subsequently renamed as International Mobile Telecommunications-2000 (IMT-2000). As a result, IMT-2000 published a set of performance requirements that a 3G system must meet. They are (for both packet-switched and circuit-switched data)

- 144 kbps in the vehicular environment,
- 384 kbps in the pedestrian environment, and
- 2 Mbps in the fixed indoor and pico-cell environment.

In addition, in all environments the system must support the same data rates for both forward and reverse links (symmetric data rates), as well as support different data rates for both forward and reverse links (asymmetric data rates) [ITU, 1997].

Although IMT-2000 specified a set of requirements of 3G wireless services, it is silent on exactly how these services are to be implemented. By 1999, several technology proposals (sponsored by different consortia from different regions of the world) existed. UMTS and cdma2000 were two such proposals. UMTS is the 3G evolution from the existing Global System Mobile (GSM) networks, while, as noted above, cdma2000 is the 3G evolution from the existing IS-95 CDMA networks. Although UMTS and cdma2000 are currently vying for dominance, both these standards fully meet the 3G requirements set forth by IMT-2000. Hence, both qualify as bona fide 3G technologies.

The origin of the belief statement lies not in the standards themselves but in the migration path from 2G to 3G. From the perspectives of migrating to cdma2000, current deployments of cdma2000 strictly do not meet all of the 3G requirements. cdma2000 is implemented in two ways: 1xRTT and 3xRTT. Initially, cellular companies will deploy cdma2000 1xRTT using 1.25 MHz of bandwidth that can provide a peak data rate of 614 kbps. cdma2000 3xRTT requires 5 MHz of bandwidth and will be able to provide higher data rates. However, many cellular companies now consider deploying 1xEV-DO instead of 3xRTT for high-data rates. 1xEV-DO, which stands for “1x Evolution-Data Optimized,” will be able to provide data rates of up to 2 Mbps. One reason why cellular companies are considering 1xEV-DO is that it only requires 1.25 MHz of bandwidth and at the same time can provide a data rate of up to 2 Mbps.

From the perspectives of UMTS migration path, GSM service providers mostly chose General Radio Packet Service (GPRS) as the intermediary step toward 3G. GPRS uses the same 200 kHz of bandwidth as GSM. In standard GSM, each 200 kHz of bandwidth is divided into eight time slots, and each voice user occupies one time slot. By using more than one time slot and more efficient channel coding schemes, GPRS can provide a peak data rate of 171 kbps. To meet all 3G requirements fully, GSM service providers do need to deploy UMTS.

What is more important than the definition and qualification of 3G is the acceptance and adoption of the technologies in the marketplace. In the beginning of the 3G race, it appeared that cdma2000 gained more market share. For example, in Japan, NTT DoCoMo launched the world’s first commercial UMTS network in 2001, and it signed up 135,000 subscribers by the end of 3Q02. On the other hand, KDDI launched service using cdma2000 1xRTT in early 2002, and signed up 2.3 million users at the end of 3Q02 [Economist, 2002]. Worldwide, since South Korea launched the world's first cdma2000 1xRTT network in 2001, there are now over 40 million users of cdma2000..

One reason for the different rates of adoption between cdma2000 (1xRTT) and UMTS is that it is comparatively easier to migrate to cdma2000 given that the technology is a natural evolution of IS-95 CDMA. cdma2000 uses the same bandwidth as IS-95 CDMA (i.e., 1.25 MHz), hence the nomenclature "1x." A cellular company can choose to either deploy cdma2000 in the same carrier that currently serves IS-95 CDMA customers, or deploy a new cdma2000 carrier. Either way, the cdma2000 deployment experience thus far shows that cdma2000 is a technology that works reliably. UMTS, on the other hand, is known to incur problem with its handsets. These issues include the interoperability of handsets and base stations made by different vendors, handset battery life, and handset availability.

Despite the growing pains, service providers deployed UMTS networks. Mobilkom (Austria), Hutchison 3G (U.K.), and NTT DoCoMo (Japan) are operating commercial UMTS networks in mid-2004. More UMTS networks will come online by the end of 2004. The current problems encountered by UMTS are not unlike those encountered in the mid 1990s when American cellular companies first tried to deploy 2G IS-95 CDMA. Eventually, the problems were solved one by one. If history is a guide, UMTS may very well replicate the success of GSM when a group of countries (i.e., E.U.) adopt a single standard and exploits the advantage of scale.

In conclusion, although both UMTS and cdma2000 qualify as 3G technologies, many issues lie behind the belief about 3G wireless technologies. The situation is exacerbated because the popular literature is filled with opinions aired by different stakeholders such as cellular companies, equipment manufacturers, intellectual property owners, investors, and government entities. Although many entities clearly have technology preferences, ultimately the marketplace will determine the distribution of adoption of different 3G technologies, which will be a lot more important than the definition and qualification of 3G.

RESEARCH DIRECTION

Based on the discussions of these two beliefs, it is clear that industry participants heavily emphasize the raw deliverable data rates of different wireless technologies. Work is ongoing in technologies, (such as orthogonal frequency division multiplexing (OFDM), intelligent antennas, and ultra-wideband (UWB) [Staple and Werbach, 2004]), which can achieve much higher spectral efficiency and are expected to underpin the next-generation wireless wide-area and local-area networks.

While technology results should continue to increase the raw deliverable data rate over wireless, an equally important research question is *ho*w can a system best appropriate resources to optimize a wireless user's experience? In addition to depending on the data rate, a wireless user's experience also depends on other factors, such as types of services requested. If not careful, an unaware application could send a 4.7-GB MPEG-2 file over a 14.4-Kbps 2G cellular link [Wood and Chatterjee, 2002]. Thus, in addition to focusing on the raw data rate, research should also emphasize wireless applications and devices that are sensitive to a user's environment and device capabilities and accordingly deliver an optimized experience to that user.

For example, when a wireless user requests a video conferencing session, the system should locate the wireless user (e.g., is it in a dense urban area where there is a high-speed WLAN hot spot nearby), determine the capability of the user's wireless device (e.g., software version and what kind of compression it can handle), and regulate the (video) data flow between the wireless user and the network (i.e., as not to overwhelm the limited storage space at the wireless user). Thus, the user's overall experience of wireless video conferencing depends on more than the raw data rate; it also depends on location management [March et al., 2000], system adaptability [Welling and Badrinath, 1998], and data administration [Jing et al., 1999]. This research direction is also echoed by Fano and Gershman [2002] who call for devices and applications to possess context-sensing capabilities and to be "responsive to the specific needs of the customer and take advantage of the resources available at the customer's location." [Fano and Gershman, 2002, p. 85]

III. BUSINESS

MYTH 3: WI-FI CREATES UNPRECEDENTED REVENUE OPPORTUNITIES

This statement is almost a hyperbole of what's happening in the Wi-Fi space. Wi-Fi, an implementation of WLAN, allows devices to acquire network connection wirelessly at high speeds. Wi-Fi communication cards for devices such as laptops are selling at a rate of approximately 1 million per month [Kaczman, 2002]. Hundreds of start-up companies are working on some aspects of Wi-Fi, ranging from Wi-Fi services to Wi-Fi security to voice over Wi-Fi to roaming between Wi-Fi and other networks.

Wi-Fi, or Wireless Fidelity, is actually a commercial name of the IEEE 802.11 standard trademarked by the Wireless Ethernet Compatibility Alliance (WECA). The most popular version today is the IEEE 802.11b standard, which operates in the unlicensed Industrial, Scientific, and Medical (ISM) band at 2.4 GHz and provides a peak data rate of 11 Mbps. A higher data-rate version is the IEEE 802.11a, which operates in the Unlicensed National Information Infrastructure (UNII) band at 5 GHz and provides a peak data rate of 54 Mbps. The latest version is the IEEE 802.11g, which is really an extension to 802.11b and also provides a peak data rate of 54 Mbps.

A better question to ask is: for whom does Wi-Fi represent unprecedented revenue opportunities? Clearly equipment manufacturers will continue to make money by selling Wi-Fi gear ranging from Wi-Fi PCMCIA cards to wireless routers. The picture is less clear, however, from the perspective of service providers. In general, three types of entities provide Wi-Fi services:

1. nonprofit and volunteer groups,
2. companies that provide and sell Wi-Fi services, and
3. traditional cellular companies.

Non-Profits and Volunteer grous

The nonprofit groups began as a grassroots movement to share broadband connections. Because a Wi-Fi network is relatively easy and inexpensive to set up, many groups set up Wi-Fi networks in communities and public places. For example, the nonprofit group NYCWireless sets up wireless "hot spots" in public places in New York City. While many of these groups sought to provide free Wi-Fi service, some found it necessary to start charging for their services in order to pay their expenses [Kharif, 2002].

Wi-Fi Service Companies

The Wi-Fi service companies either built their own wireless hot spots at hotels and airports, or "aggregate" smaller Wi-Fi networks and resell the service. One well known example is Boingo, which provides Wi-Fi services at over 1200 hot spots in North America. One way Wi-Fi service companies can increase the scale and reach of their networks is either to build more networks or combine with other operators. Another way is to sign up or acquire the independent nonprofit networks.

Traditional Cellular Companies

The traditional cellular companies are moving into the Wi-Fi market. For example, T-Mobile announced in early 2002 that it will integrate Wi-Fi into its existing networks. Many cellular companies already invested a lot of capital to deploy 3G technologies. But, thus far, data connections routed through the traditional cellular networks still hover below 100 kbps. Worse yet, when a user is inside a building (e.g., hotel or airport), cellular signals deteriorate and connection speeds slow down further (if there is no “in-building” base station at that location). Therefore, cellular companies potentially can gain much by expanding their service offerings to include Wi-Fi, especially for serving selected locations where high-speed demands may be particularly high. In doing so, cellular companies can provide ubiquitous wireless data services: at high speeds using Wi-Fi at high-demand locations, and at nominal speeds using traditional cellular networks everywhere else. Cellular companies are moving in this direction. T-Mobile purchased MobileStar Network, and Sprint provided some of Boingo’s startup capital.

The conclusion, then, is that Wi-Fi does seem to present revenue opportunities for the for-profits such as Wi-Fi service providers and traditional cellular companies. In particular, the cellular companies should be able to charge a premium for their cellular/Wi-Fi hybrid service because the service is ubiquitous, whereas pure Wi-Fi service providers do not provide contiguous network coverage.

Although Wi-Fi does present revenue opportunities for many entities, one potential problem exist with the technology down the road, Ironically, the problem is what enables Wi-Fi to be so successful in the first place: the spectrum in which Wi-Fi operates is unlicensed and free. Therefore,potential conflicts could exist in the future. These conflicts take two forms:

1. signal interference between Wi-Fi and other devices (e.g., industrial, scientific, and medical) in close proximity, and

2. signal interference between two nearby Wi-Fi networks.

Interference may become a serious issue when, say, two Wi-Fi operators would like to serve the same high-demand location (e.g., a popular food court at a busy airport). Since the spectrum is unlicensed, no single operator can claim an exclusive right to use the spectgurm at that location. Although it is possible for two Wi-Fi networks to coexist at the same location, the data rate for each network must necessarily be lowered to minimize interference.

Unlike the issue of Wi-Fi security, which can be solved by the vigilant use of authentication and encryption before and during every session, the interference issue has not received much attention up to now. Part of the reason is that across the country, Wi-Fi coverage is still sparse and does not overlap much. The FCC currently does not plan to regulate Wi-Fi spectrum use, but FCC Chairman Michael Powell did warn that Wi-Fi could eventually cause a “meltdown” in the spectrum [Crockett et al., 2002]. To ensure the continued success of Wi-Fi and the continued revenue stream from it, the industry needs to start addressing the interference issue, sooner rather than later.

MYTH 4: MOBILE E-COMMERCE IS THE NIRVANA OF NEW USERS AND SERVICE PROVIDERS

In addition to the specific technologies of 3G and Wi-Fi, the larger issue of mobile e-commerce, or m-commerce needs to be resolved. Advances in wireless technologies drew business and IT manager attention to profitable m-commerce applications [Kalakota and Robinson, 2001; Deklava, 2004]. Convergence of wireless and wired networks further presents users and service providers with abundant m-commerce opportunities [Chatterjee and Byun, 2002]. Business-to-business (B2B) and business-to-customer (B2C) mobile applications include financial service, inventory management, proactive service, product locating and shopping, auction and reverse auction, entertainment services and games, mobile office environment, distance education, and data center [Varshney and Vetter, 2000].

The Strategy Analyst and Gartner Group estimate that by year 2004 there will be over one billion wireless device users and 600 million wireless Internet subscribers [Fitzharris, 2000].These potential users will be important to the estimated $200 billion m-commerce market. Finland is the first country to obtain revenues from wireless communication that exceed those of wired counterparts. Other countries like the U.S. and Japan may soon catch up with Finland. Given these growths, many service providers and users of mobile applications believe that m-commerce is their nirvana to harvest unique mobile business opportunity.

Before accepting the belief that "m-commerce is the nirvana of new users and service providers", issues such as mobile client, m-commerce applications, and global standards [Tarasewich et al., 2002] need to be examined carefully.

Mobile Clients

Current wireless device technologies range from smart phone, web-enabled phone, and SMS-enabled phone to personal message pager, laptop computers, and wireless-enabled handheld computers (e.g., pocket PC, personal digital assistant or PDA, and tablet PC). These devices possess both strengths and weaknesses for running m-commerce applications. For example, in the U.S. in 2004, the smart phone market is small. Therefore, only limited service is being offered to users. Without security measures (such as storing private keys and nonrepudiation supports), smart phones are often not suitable for sophisticated m-commerce applications. The market for Short Message Service (SMS) phones caters to a large customer base in the U.S. But SMS phone's low-bandwidth, high-latency network prevents the use of audio- and video-applications. This market penetration limited SMS phone primarily to one-way and information-push m-commerce applications [Gonzalez, 2002].

Wireless devices using higher-throughput 3G (up to 2Mbps) and 4G (up to 100 Mbps) networks are emerging. These devices can offer high-speed and multimedia-based m-commerce applications. But technological issues (such as interoperability of radio interfaces and short battery life) and service issues (such as convergence between wired and wireless Internet) remain. Ultimately, incompatible wireless devices will require additional investments to empower m-commerce applications to serve different mobile clients.

M-Commerce Applications Issues

M-commerce applications differ from their wired counterparts because they are contextual [Worthen, 2001] and dynamic, lack users' attention, are perceived vulnerable [Ghosh and Swaminatha, 2001], and are location-based [Kalakota and Robinson, 2001]. These characteristics must be supported with the appropriate m-commerce business models, privacy-protection, and security measures, and integrity of synchronized data among multiple devices.

M-commerce companies propose an array of business models to increase their revenues. NTT DoCoMo obtains its revenue from traffic usage of end-users and portal usage, advertising fees, and proxy collection charges from ISPs (1,500 official i-Mode websites and unofficial websites). Cingular introduced small wireless payments and e-wallet service to increase its revenue. 4thpass Inc. offers a Java-based debit service. Despite of these attempts, even NTT DoCoMo (perceived as the only profitable m-commerce business model in one of the most affluent Internet-enabled wireless societies) is struggling with many challenges. These challenges include low usage rates of few websites and low percentage of heavy i-Mode teenage users [Beck, 2001].

M-commerce applications are exposed not only to existing e-commerce security threats (due to convergence), but also to m-commerce specific threats such as software risks, platforms risks, software application risks and security risks of wireless language scripts [Ghosh and Swaminatha, 2001]. M-commerce vendors may need to formulate a more careful security design to combat these threats.

Global Standards

M-commerce applications vary across different countries because of legal, cultural, social, political and technical differences. For example, in Japan and Europe SMS messages dominate wireless network traffic, while in the U.S. wireless networks are mostly used to conduct live conversations. In terms of 2G technology, Europe uses GSM, North America uses CDMA and GSM, and Asia uses CDMA, GSM, and TDMA. In terms of 3G, early visionaries hoped for a single global standard, but currently more than one 3G standard emerged, including UMTS and cdma2000. All in all, the success of any m-commerce business model depends on taking these national differences into account.

Conclusion

M-commerce still suffers from incompatible mobile clients, limited applications, and differing wireless standards. M-commerce may proliferate and become profitable when these and other issues are adequately addressed by vendors and standards bodies. Before then, the statement of “m-commerce is the nirvana for users and service providers” is not an accurate one of the current state of m-commerce.

RESEARCH DIRECTION

For wireless business, research should go beyond Wi-Fi and m-commerce and focus on the larger issue of the relationship between wireless technologies and businesses. Many businesses are beginning to recognize the benefits provided by wireless technologies and are deploying appropriate applications. A majority (64%) of companies in a 2003 survey consider wireless technology important to their business goals [Johnson, 2003], and 75% of respondents in another survey are undertaking a wireless project [Worthen, 2004]. These results are not surprising considering that the cost of deploying wireless continues to fall. Collett et al. [2003] suggest that companies and organizations will deploy wireless technology when a compelling economic benefit (e.g., return on investment) can be demonstrated. Given that the cost of deploying wireless continues to fall, ROI is becoming justifiable for wireless for more organizations.

One alternative of reaching businesses and consumers is WiMAX, which is based on the IEEE 802.16 series of standards for broadband wireless systems. The WiMAX Forum [Kozup, 2004] was formed to increase public awareness of the broadband wireless potential and accelerate adoption by driving vendor interoperability. In the same way that the Wi-Fi Alliance spawned the growth of 802.11, WiMAX could become the industry standard for broadband wireless access. Although WiMAX does not create a new market (broadband wireless currently exists in various forms), it enables the standardization of technology required for volume economics that reduces costs and enables broader market growth.

Given that businesses are beginning to adopt wireless technologies, the research question more appropriate at this point is: how can organizations best utilize wireless technologies to their advantage*?* The current literature consist mostly of anecdotal evidence claiming that wireless technology contributes to benefits (e.g., [Kanell, 2003]), and most of the benefits are articulated by the adopting organizations and wireless project managers. Clearly more work is needed, particularly on documenting the quantitative benefits of using wireless technologies across different industries and businesses.

IV. SOCIETY

MYTH 5: WIRELESS COMMUNICATION IS NOT SECURE

This myth comes about partly because wireless devices typically operate at lower processing power and bandwidth and less memory than wired devices [Radding, 2001]. Reduced processing power could limit the range of encryption schemes that can be used. Bandwidth limitations can increase the expense of storing packet overhead and of using complex handshaking. Limited memory could constrain the placement of security measures. These characteristics of wireless devices mean that they are susceptible to security risks such as:

1. target (not attackers-initiated) threats (e.g., information stolen),
2. software risks (time gap between decryption and encryption),
3. platform risks (failure to provide sandboxes for untrusted codes), and
4. software application risks (low-level languages) [Ghosh and Swaminatha, 2001].

Despite these weaknesses, examining security features of wireless local and wide area networks is important in addressing the belief statement.

Wireless Local Area Networks (WLAN)

Wi-Fi and Bluetooth WLANs adopted the Wired Equivalent Privacy (WEP) 40-bit encryption mechanism. To achieve higher security levels, the WEP2 128-bit encryption mechanism is proposed but is not yet fully adopted. Before WEP2 is adopted, WECA suggests changing password, SSID, and the table of MAC addresses of WLAN to ensure higher security levels.

The IEEE defines 802.11x authentication standards for WLANs. The Extensive Authentication Protocol (EAP) information (e.g., passwords, token cards, Kerberos, digital certificates and public- and private-key) can be encapsulated in data frames that are sent within the WLANs. Authentication can also be executed at the MAC layer. At multiple access points, a table of MAC addresses and SSID can be used to manage the security of WLANs. Rather than maintaining a static encryption key for WLAN, IEEE 802.X LANs can provide centralized user authentication and automated key distribution. Cisco, Lucent, and Agere are solution providers.

Wireless Wide Area Network (WWAN)

The Wireless Transport Layer Security (WTLS) protocol supports security on mobile devices running Wireless Application Protocol (WAP). WTLS protocol is based on the Secure Sockets Layer modified to support user datagram and TCP transport protocols. The existing WAP 1.1 standard is vulnerable to hacking at the WAP gateway server where the encryption/decryption takes place. The new WAP 2.0 standard can provide end-to-end encryption/decryption and will eliminate this weakness. In addition, WAP will adopt the Wireless Identity Module (WIM) to store a digital certificate and its associated private key for secured authentication.

In addition, WWAN operators can also authenticate their users' devices. For example, GSM phones rely on the Subscriber Identify Module (SIM) card to hold all security information. The SIM card uses onboard cryptography to improve security levels. CDMA phones can also support SIM cards. In this case, WWAN operators serve as gatekeepers to secure customer data and keep them from being abused by entities with vested business interests.

Fee collection and financial service demand different levels of security. To ensure higher authentication such as non-repudiation, wireless public key infrastructure (PKI) are required. Wireless PKI standards are instituted by many organizations like European Telecommunications Standards Institute and Internet Engineering Task Force. Currently, third parties that issue and validate digital certificates include Certicom, RSA Security, Entrust Technologies Inc., Baltimore Technologies PLC, and VeriSign Inc.

Roaming between WLAN and WWAN

Security holes can exist when roaming between WLAN and WWAN. TCP/IP assumes that each connection session is established with a fixed IP address after a user is authenticated. To prevent users from being re-authenticated every time their IP address or network attachment point changes (during roaming), a software solution can be deployed at all access points of a single subsets (physically or virtually via a VLAN).

Another alternative to securing the roaming of WLAN and WWAN is to adopt Java mobile agent technology. The technology creates agents, each with a unique identity. When an agent roams the Internet (over wired and wireless networks), its identity is verified with a list of system's valid users with respect to their permission to access corresponding resources. This agent technology offers another layer of security in addition to keeping track of an agent's stops [Wong et al., 1999].

Conclusion

Admittedly, the adoption of wireless security technologies is slow. For example, micropayments may not drive the adoption of wireless PKI because many merchants express no interest in exercising such a high level of security in small fee collections. In addition, customers do not feel as confident when conducting transactions wirelessly [Siau and Shen, 2003]. The challenge is having enough merchants, buyers, and transactions to justify investments in security infrastructure by these stakeholders [Herzberg, 2003]. This lack of both supply and demand of PKI technologies slowed the diffusion of micropayments in B2C m-commerce. However, not all m-commerce applications need stringent security technologies. For example, information-push advertisements do not need to be encrypted using a 128-bit encryption algorithm, but it is necessary for financial institutions to deploy PKI standards to avoid possible repudiation disputes.

Although the perceived security level for wireless networks is low, wireless networks can technically exercise as much security as wired networks. Wireless devices possess more processing power and memory and can communicate at higher data rates now than previously. Thus from a technical perspective, the statement "wireless communication is not secure" is not accurate. Industry technologists agree that for most organizations' security is no longer a reason not to adopt [Brewin, 2003].

RESEARCH DIRECTION

Given that for most organizations security should no longer be a reason not to adopt wireless technologies, a more appropriate research question at this point is how can organizations best secure their wireless networks? Research applicable here would include case studies of:

1. organizations that are addressing their wireless security concerns,
2. processes used to secure their wireless infrastructure, and
3. methods used to match countermeasures to threats.

Case studies of how companies develop security plans that recognize risks, eliminate vulnerable points in the infrastructure, and ensure that users are trained about the threats should also be fruitful areas of research.

In addition, given that solutions now exist to ensure secured communications and transactions over WWANs (most m-commerce transactions occur over WWANs) and communications over WLANs, another important question is not whether security technology exists to ensure secured communications and transactions [Siau et al., 2001], but how can one facilitate the adoption of wireless security measures? Even though security solutions exist, a host of issues underlies whether or not individuals and organizations adopt adequate security measures. An individual may not turn on the over-the-air encryption feature in his or her home WLAN because he or she does not know how (i.e., lacks requisite knowledge). A small business may not be interested in adopting wireless PKI and thus will not become an m-commerce seller because the cost of adoption is too high (i.e., low ROI) [Herzberg, 2003]. Thus, studies of contributions of independent variables to the adoption of security measures are worthy areas of continued research.

V. CONCLUSION

Considering the past and future of wireless communications, it seems clear that this field will continue to grow as people become more mobile and demand that they no longer be tethered to a fixed location. Undoubtedly, as the field grows more (erroneous) belief statements will surface. Although many such statements about wireless communications at first seem reasonable, it is important to consider them critically. In this paper, we considered some of the more popular misconceptions and presented a framework for examining them. We also proposed relevant research questions for future investigations. We hope that this article and its framework will serve not only as a tool for researchers to identify future myths in wireless communications, but also as a model for studying the technological, organizational, and societal aspects of wireless communications.

Editor's Note: This article was received on March 25, 2004. It was with the authors for seven weeks for one revision. It was published on June 29, 2004.

REFERENCES

Agres, C., D. Edberg, and M. Igbaria (1998) "Transformation to Virtual Societies: Forces and Issues", *The Information Society*, (14), pp. 71-82

Beck, J. C. (2001) "Seven Myths about Japanese M-Commerce", New York: Accenture.

Brewin, B. (May 5, 2003) "Working-Class Wireless", *Computerworld*, pp. 38-39

Brown, B., N. Green, and R. Harper, eds. (2002) *Wireless World: Social and Interactional Aspects of Wireless Technology*: London: Springer-Verlag.

Chatterjee, S., and J. Byun (2002) "Network Convergence: Where is the Value?", *Communications of the AIS*, (9)27

Collett, S., B. Brewin, and T. Hoffman (May 5, 2003) "Wireless Gets Down to Business", *Computerworld*, pp. 30-36

Crockett, R. O. et al. (April 29, 2002) "All Net, All the Time", *Business Week*, pp. 100-104

Deklava, S. (2004) "M-Business: Economy Driver or a Mess?" Communications of AIS, (14)14, pp. 111-134, February

Economist (Sept. 28-Oct. 4, 2002) "Mobile Telecoms: Time for Plan B", *Economist*, pp. 57-58

Fano, A., and A. Gershman (2002) "The Future of Business Services in the Age of Ubiquitous Computing", *Communications of the ACM*, (45)12, pp. 83-87

Foreman, G. H., and J. Zahorjan (April, 1994) "The Challenges of Mobile Computing", *IEEE Computer*, pp. 38-47

Fitzharris, M.A. (2000) "StatCenter: The Wireless Market", TechRepublic, January 27 http://www.techrepublic.com/article.jhtml?id=/article/r00620000127maf02.htm (Current July 23, 2001)

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

Gonzalez, J. D. (2002) "A Roadmap to Wireless: The state of the Technology", Atlanta, GA: Air2Web, Inc.

Herzberg, A. (2003) "Payments and Banking with Mobile Personal Devices", *Communications of the ACM*, (46)5, pp. 53-58

International Telecommunication Union (ITU), (1997) *ITU-R Recommendation M.1225: Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000*, Geneva: International Telecommunication Union.

International Telecommunication Union (ITU) (2003) *World Telecommunication Indicators Database 2003*, Geneva: International Telecommunication Union.

Jing, J., A. Helal, and A. Elmagarmid (1999) "Client-Server Computing in Mobile Environments", *ACM Computing Surveys*, (31)2, pp. 117-157

Johnson, M. (May 5, 2003) “Worthy of Wireless”, *Computerworld*, p. 22
Kaczman, J. (September 2002) “Wi-Fi Hotspot Networks Sprout like Mushrooms”, *IEEE Spectrum*, pp. 18-20
Kalakota, R., and M. Robinson (2001) *Mobile Business: The Race to Mobility*: New York: McGraw-Hill Professional.
Kanell, M. E. (November 15, 2003) “No Frills Wireless”, *CIO*, pp. 104-106
Kapp, S. (Jan./Feb. 2002) “802.11: Leaving the Wire Behind”, *IEEE Internet Computing*, pp. 82-85
Kharif, O. (September 17, 2002) “Footing the Bill for Free Wi-Fi”, *Business Week*.
Kozup, C. (May 13, 2004) “The What, Where, and Why of WiMAX”, *ZDNet Tech Update*,http://techupdate.zdnet.com/techupdate/stories/main/What_Where_Why_WiMAX.html?tag=tu.arch.link (Current May 21, 2004)
March, S., A. Hevner, and S. Ram (2000) "Research Commentary: An Agenda for Information Technology Research in Heterogeneous and Distributed Environments", *Information Systems Research*, (11)4, pp. 327-341
Odlyzko, A. M. (November 2000) “Internet Growth: Myth and Reality, Use and Abuse”, *iMP: Information Impacts Magazine*, http://www.cisp.org/imp/november_2000/11_00contents.htm (Current May 12, 2003)
Radding, A. (January 1, 2001) “Technology: Crossing the Wireless Security Gap”, *Computerworld*, pp. 52-53.
Shannon, C. (1948) “A Mathematical Theory of Communication”, *Bell System Technical Journal*, 27, pp. 379-423
Siau, K., E. Lim, and Z. Shen (2001) " Mobile Commerce: Promises, Challenges, and Research Agenda", *Journal of Database Management*, (12)3, pp. 4-13
Siau, K., and Z. Shen (2003) "Building Customer Trust in Mobile Commerce", *Communications of the ACM*, (46)4, pp. 91-94
Staple, G., and K. Werbach (March 2004) “The End of Spectrum Scarcity: New Technologies and Regulatory Reform will Bring a Bandwidth Bonanza”, *IEEE Spectrum*, pp. 49-52
Tarasewich, P., R. Nickerson, and M. Warkentin (2002) "Issues in Mobile E-Commerce", *Communications of the AIS*, 8, pp. 41-64
Varshney, U., and R. Vetter (2000) "Emerging Mobile and Wireless Networks", *Communications of the ACM*, (43)6, pp. 73-81
Welling, G., and B. Badrinath (1998) "An Architecture for Exporting Environment Awareness to Mobile Computing Applications", *IEEE Transactions on Software Engineering*, (24)5, pp. 391-400
Wong, D., N. Paciorek, and D. Moore (1999) "Java-Based Mobile Agents", *Communications of the ACM*, 42, pp. 92-102
Wood, S., and S. Chatterjee (2002) "Network Quality of Service for the Enterprise: A Broad Overview", *Information Systems Frontiers*, (4)1, pp. 63-84
Worthen, B. (May 1, 2001) "Wireless Technology: Location, Location, Location", *CIO*, pp. 107-113
Worthen, B. (February 1, 2004) “Wireless Finally Connects”, *CIO*, pp. 62-68

ABOUT THE AUTHORS

Samir Chatterjee is Associate Professor in the School of Information Science and Founding Director of the Network Convergence Laboratory at Claremont Graduate University. Prior to that, he taught at Georgia State University. His previous research examined ATM scheduling systems, efficient routing protocols, TCP/IP performance over HFC cable networks, QOS and all-optical networking. Currently he is exploring fundamental challenges in Voice/Video over IP, real-time protocols and secured PKI infrastructures.His publications appear in *Communication of the ACM*, *Computer Networks & ISDN Systems*, *Computer Communications*, *Communications of the AIS*, *Information System Frontiers*, *ACM Computer Communication Review* and others. He is a core member of Internet2 Middleware working group on videoconferencing and served as an expert on the Computer Science and Technology Board panel under National Research Council. He is principal investigator on several NSF grants and has received funding from many private corporations.. He is the secretary of EntNet Technical Committee for IEEE Communications Society. He also co-founded a startup, VoiceCore Technologies Inc. in 2000. His PhD is from the University of Central Florida.

Charlie Chen teaches electronic commerce and advanced database concept at the Department of Information Technology and Operations Management, Appalachian State University. He joined ASU in August of 2003 after completing his PhD in Management of Information Systems from the School of Information Science, Claremont Graduate University. He taught previously at California State University, Northridge. Dr. Chen likes to view the field of Management Information Systems from infrastructural, managerial and operational perspectives. He is working on improving information system solutions in each of these three areas.

Samuel Yang is Associate Professor of Information Systems and Decision Sciences at California State University, Fullerton. He holds a Ph.D. in information science from Claremont Graduate University. Samuel Yang's experience in the wireless and telecommunications industries spans 15 years. . He was a manager of network planning at Verizon Wireless, where he led the strategic planning and design of its 2G and 3G wireless networks in the western United States. Prior to Verizon Wireless, he was with Hughes Space and Communications (now Boeing Satellite Systems), where he served as a technical lead on several international communication satellite programs. His publications appear in refereed journal and conference papers. He is also the author of two books about wireless communications. He currently conducts research and consults in the area of wireless networking,

Communications of the Association for Information Systems

ISSN: 1529-3181