A World Without Wires: The Future of Wireless Networking

Heather Nodler
Knowledge Management Systems
Dr. Don Turnbull
May 3, 2005
Introduction

A New York Times article (Scheisel, 2005) recently reported that more than 10 million homes in the United States employ a wireless router to access the Internet, up from virtually none in the year 2000. Legislative battles rage over the right of municipalities to provide free or inexpensive wireless Internet access to citizens. The technology to support wireless networking continues to evolve at a rapid pace, promising that faster, cheaper, more pervasive wireless computing solutions will be available to businesses and consumers who will require always-on, seamless, wireless computing experiences. Wireless networks clearly offer an array of advantages over traditional wired networking solutions to users in all types of networks and industries. These advantages include mobility, ease of installation, reduced cost of ownership and scalability, which in turn lead to increased productivity and interpersonal communication. This paper will outline the history of wireless networking, the types of wireless networking currently in use and some of its possible future applications. It will also discuss the social and political issues surrounding this important technology.

WLAN

At this point in time, wireless connectivity solutions can be grouped into three main categories. All three use Radio Frequency (RF) technology to transmit data through the air. The first category, wireless local area networking (WLAN), transmits data between a wired network and a mobile user or users (Types, 2005). Its origins lie in the encrypted radio signals sent by allied operatives across enemy lines during World War II. Referred to as “spread spectrum technology,” the wartime messages paved the way for the first computational wireless network, which was created in 1971 at the University of
Hawaii. The project, called ALOHNET, had seven computers set up on four islands communicating with one central computer on Oahu, none of them using phone lines (Bautts, 2005). In a modern-day example of WLAN technology, businesses commonly issue network-connected laptops with wireless cards to their employees to replace desktop computers. This allows their employees to be productive anywhere within the bounds of the corporate network. It also encourages collaboration by giving them the ability to form ad hoc work groups. In certain situations, it can provide employees with incentives to use their computers at home or in coffee shops, where they may do work outside of traditional work hours. In this case, because the employees’ work time seeps into their leisure time, a perceived benefit for the employee (the use of a computer with wireless capabilities) becomes a very real benefit for the employer.

Wireless LANs operate using a transceiver device to send and receive data. This device, also referred to as an “access point,” connects the computers on the wireless network to a wired network. The computers are equipped with wireless networking devices, which come standard on many laptop and handheld computers now. Each access point ensures connection to the network within a radius of anywhere from 100 to several hundred feet. Access points are strategically placed across a network area so that connection areas overlap, and users can travel between them without interruption of service, a process called “roaming.” (Proxim, 1998)

Several different protocols exist for wireless local area networking, all approved by the Institute of Electrical and Electronics Engineers (IEEE). Together, LAN protocols have been assigned the numerical grouping 802. They are then broken down into further groupings. 802.11b (Wireless Fidelity - commonly referred to as “WiFi”) is the standard
used by most WLANs today. A new standard 802.16 (WiMax) is currently being
developed to provide connectivity with a 30-mile radius around each access point.

**WPAN**

The second category of wireless solutions, wireless personal area networking
(WPAN) establishes connectivity between devices that manage personal information or
information shared between a small group of individuals. Currently, this type of
connectivity is achieved using the Bluetooth protocol. Originally designed to provide a
way to connect portable and/or fixed peripherals, e.g., mice, keyboards, headsets,
headsets and other devices, to computers without using cables, Bluetooth operates using
low-power, short-range radio links. (Bluetooth, 2005) This technology is commonly used
to establish a wireless connection between an individual’s PDA or mobile phone and a
desktop computer.

**WWAN**

The third category of wireless solutions, wireless wide area networking
(WWAN), is similar to WLAN but is designed to allow people to connect to the Internet
or another network outside of the bounds of a LAN. For example, a businessman who
wants to stay connected during a course of travel can use a PC card cellular modem or his
cellular phone to connect his laptop to the Internet or his company’s intranet, as long as
he is within reach of a cellular phone tower. (Types, 2005)

**Connectivity and Bandwidth**

In 1985, the FCC made segments of the bandwidth spectrum available for use by
certain telecommunications devices without a license. The unregulated spectrum was
known as the ISM (Industrial, Scientific and Medical) bands, and the FCC recently added
to the unregulated a spectrum 300 MHz of additional bandwidth. This dedicated free bandwidth ensures that anyone adhering to pre-set standards of power and technologies applied can reap the benefits of wireless connectivity without having to obtain a license or pay fees.

**Future WLAN Applications**

Wireless connectivity has to a great extent changed the way we live, and it promises to do so increasingly. Currently, WLANs allow employees in organizations to carry out their duties and remain constantly connected to a network, where they can retrieve, exchange and store information. Doctors and nurses in hospitals frequently carry handheld devices connected to the hospital’s WLAN to record and download vital patient information to and from the network. (Proxim, 1998) Students on college campuses tote laptop computers from class to class, remaining constantly connected to the Internet, and supplementing their classroom educations.

WLANs are also increasingly employed to establish voice connections between users with Voice-over Internet Protocol (VoIP), which transmits voice data across the Internet in data packets. The appeal of VoIP is that since most providers charge a flat monthly rate, calls can be connected without incurring long-distance fees. This can provide a very cost-effective solution to users who routinely make international calls.

Voice-over WiFi (VoWiFi) combines VoIP with wireless networking technology. Using a PDA or a laptop computer equipped with a wireless card and Internet telephony software, a user can make a telephone call over a wireless network. One advantage of this technology over traditional cellular phone technology is improved connection quality indoors or underground. Some cellular phone companies have developed hybrid
telephones that operate using VoWiFi most of the time but can switch to a regular cellular connection if the user happens to move out of the LAN area. (Beal, 2005)

**Future WPAN Applications**

The possibilities of WPAN extend beyond the ability to sync one’s Palm Pilot to a desktop without wires. Currently, the Bluetooth protocol is being applied in the development of pervasive computing solutions for the home. In the very near future, the majority of people may use a Bluetooth-enabled wireless connection and a personal controller to access or remotely control many “intelligent” devices, such as handheld computers, mobile telephones, cars, kitchen appliances, home lighting systems, etc., which can detect users’ changing locations and respond to their needs accordingly (WPAN, 2005)

Developers are working on a generation of wearable devices that will perform functions such as allowing the wearer to input data without using a keyboard or mouse, or monitoring the wearer’s vital statistics. These applications, together with home and office pervasive computing, could save time and be of tremendous help to people with illnesses or disabilities.

**Societal Implications of Wireless Connectivity**

As a rule, technological innovations force a society to reevaluate its core principles and sometimes make significant, often irreversible, cultural adjustments to accommodate the new technology. Wireless networking is uniquely poised to change the world in a relatively short period of time, insofar as it engenders an unprecedented cultural situation in which users are constantly connected to each other with mobile devices through the Internet or ad hoc peer-to-peer networks.
In *Smart Mobs* (2002), Howard Rheingold considers many of the implications of such a situation envisioning a “wireless commons” in which every person, object and place is connected to the Web and assigned a unique URL, transmitting and receiving information constantly across the network. In this dense (and mostly invisible) web of data, roaming human nodes in the network will be able to retrieve and share information about *everything*, everywhere, effortlessly.

On the positive side, Rheingold views such a network as a means of dissolving barriers between people and fostering the formation of communities, both of divergent segments of the population who stand to benefit from each other’s knowledge, and of like-minded individuals who choose to convene for social purposes or for spur-of-the-moment, cooperative political action. Both functions are critical for effective knowledge management. Rheingold cites several feats of political coordination enabled by wireless computer connectivity, including the 1999 World Trade Organization protests in Seattle and the ongoing demonstrations by bicycling “Critical Mass” protesters. On a more mundane level, the process of arranging one’s social or business calendar is streamlined when friends and colleagues can keep tabs on each other’s whereabouts, and communicate across the network instantly.

As Rheingold points out, however, this omniscience comes with a price. Being permanently tied into a network requires one to relinquish a privilege that people in this country have traditionally held very dear: privacy. If information flows freely across the network, it has the potential to be seen by anyone. Information can be intercepted over networks, whether by a nosy family member, a malevolent thief, or a government authority. Already, the prevalence of personal data theft has created calls for
governmental regulation of data brokers and massive network security initiatives (Zetter, 2005). Many people are wary of any technology that has the ability to make our private lives public. With that in mind, Rheingold suggests that more powerful encryption technology, along the lines of the Wireless Encryption Protocol (WEP), may be the only way that users will be able to maintain any semblance of privacy in the new wireless world.

Philip Agre in his essay “Welcome to the Always On World,” (2001) presents a few more social discomforts that can, and have, resulted from ubiquitous human networking. Among them are: 1) constant interruptions – the “always on” mentality can distract people from their tasks; 2) divided attention – when people are constantly paying attention to maintaining their social networks and communications devices, they have little attention to devote to individual personal relationships; 3) addiction – some people become addicted to information in a networked environment, constantly checking their e-mail, blogs, message boards, etc., because they fear they might miss out on something important; 4) boundaries – when people give each other tacit permission to keep track of each others affairs, social boundaries collapse, causing what can be perceived as an invasion of each other’s privacy (Agre, 2001). These concerns have been manifested in use of wireless technology, and as wireless computing becomes more ubiquitous, they will only grow more intense.

Therefore, it is incumbent upon people in this age to approach the use of new technology with a critical eye. People should be able to ask, “What are the implications of using this technology? Does it make my life more manageable or more complicated? Are its benefits worth its consequences?” Certainly, wireless networking will change the
very fabric of our society, but we as societal participants have the opportunity to make
decisions regarding just how this change will take place.

The Politics of Wireless Networking

The adoption of wireless networking technology comes with many political
considerations as well. One concern is how it affects the so-called “digital divide.” Some
people view wireless networks as opening up new opportunities for learning and
participation in society for people who are at a disadvantage either through lack of
material resources or information illiteracy. A counterargument posits, however, that
building a wireless network into our society’s core will only serve to alienate those
without access to Internet service, laptops, PDAs, or wearable devices. According to
Metcalfe’s Law, the addition of people to the network will increase the network’s value,
while Reed’s Law suggests that adding a new group of people will increase its value even
more. In short, a wireless society stands to benefit from the inclusion of all citizens,
especially those who would otherwise be excluded.

One response to this issue has been the creation of low-cost or free public wireless
networks to ensure that all citizens have access to the Internet. Sponsored by libraries,
philanthropists and city or state governments, these projects have created much
controversy and a series of territorial disputes, in part because broadband Internet service
providers feel they should be able to charge people for wireless service without fear of
competition from the government. Due to their strong lobbying power in Congress, the
broadband companies have posed a formidable challenge to municipalities, and several
states are considering bills to outlaw municipal wireless projects. (Tanner, 2005)
While corporations think that they should control the networks, others think that networks should remain uncontrolled and subject to the will of the people. Still others argue for more government involvement. Rheingold (2002) discusses the case of government projects, like California’s Center for Information Technology Research in the Interest of Society (CITRIS) that use wireless networks as a security infrastructure in case of a catastrophic event. In part because wireless networks lack the physical constraints of wired networks, the question of who has the right to exercise control over them is a difficult one that will need to be decided in the near future.

**Conclusion**

We live in exciting times, when hosts of emerging wireless technologies promise radical change in our modes of perception, interaction, democratic participation, and time and information management. As new technology is developed, we will witness even greater change, which hopefully will benefit society, rather than harm it. In the meantime, we have an obligation to approach that technology with a certain degree of criticality.
References


http://www.stylusinc.net/technology/pervasive_computing/WPAN.shtml