WIRELESS NETWORKING

Edward Garza, Texas A&M University – Kingsville
Dr. Charles Alworth, Texas A&M University – Kingsville, c-alworth@tamuk.edu
Dr. Jack D. Shorter, Texas A&M University – Kingsville, j-shorter@tamuk.edu

ABSTRACT

The purpose of this paper is to inform the reader about the basic terms and definitions of wireless networks and applications. Subjects addressed are current standards in wireless networks and security. We also list some of the benefits of implementing wireless local area networks for both corporate and home users. The future aspects of wireless local area networking technology and how they compare to the technology that is currently implemented are also discussed. Such technology includes IEEE 802.11, HiperLAN, HomeRF, and Ultra-Wideband.

Keywords: WLAN,Wi-Fi, IEEE802.11B, OFDM, Wireless

INTRODUCTION

Wireless networking applications continue to proliferate at an incredible pace as wireless features, functions, security, and throughput improve (9). Wireless local area networking is not a recent development; in fact, it's been around almost a decade. However, it is just now reaching critical mass, with WLAN technologies that operate at speeds comparable to wired local area networks. Both corporate users and home users alike are choosing WLANs for their ease of installation, as well as for their flexibility. 802.11 is the standard on which wireless networking exists today (9). Products that use the technology support a broad range of uses for enterprises and home users.

THE WIRELESS ADVANTAGE

To stay competitive in today's business world, many organizations are strategically focusing their efforts on improving productivity, as well as producing better customer service (10). In an effort to achieve these goals, organizations are developing wireless applications, enabling employees to access critical information while away from their desks. At the same time, wireless networks make it easier for organizations to keep up with the rapid pace of technology by making network upgrades easier. Wireless is, in a sense, a response to the way we do business today.

COMBINING COMPUTERS AND COMMUNICATIONS

WLAN is at the center of two different trends taking place in the worlds of computers and communications (4). First, voice communications is migrating to Internet-like networks that turn voice communications into data for greater efficiency. Secondly, broadband is entering the home and workplace.

A converged voice and data network would provide more enhanced computing and communications applications. WLAN makes administration and expansion of such a network at its end-points easier and more flexible.

WIRELESS LOCAL AREA NETWORKING

Wireless local area networks (WLANs) are the same as the traditional LAN but they have a wireless interface (2). WLANs were designed to replace traditional "wired" local area networks. With the introduction of small portable devices such as PDAs (personal digital assistants), the WLAN technology is becoming very popular. WLANs provide high-speed data communication in small areas such as a building or an office. It allows users to move around in a confined area while they are still connected to the network.

BENEFITS OF WIRELESS LOCAL AREA NETWORKING

One of the most attractive aspects of a WLAN is its ease of installation. There is a minimal amount of configuration necessary that is essentially no different than setting up a wired network (4). However, there is less overall work involved when installing a WLAN, as there are no cables to install. In some cases, the Wi-Fi base station, or access point, is simply a Wi-Fi transceiver that lets you connect Wi-Fi computers together.

WLANs are also more easily upgraded compared to wired networks. The ease comes from the independence of devices on a WLAN in that only the object being upgraded is affected by the change (11). The network remains operational, and no new wires need to be installed, tested, or terminated.

WLANs can be, in the long run, lower cost solutions than wired networks (11). While wireless components, such and network cards and transmitters, may cost more than wired components, the absence of cable installation and testing often offsets these expenses. There is also the elimination of the cost of setting up cabling and services for companies that wish to connect their current LANs to remote locations.

Another compelling feature of Wi-Fi is its ability to support ad hoc networks. These are impermanent networks set up on the fly, such as a few laptops with Wi-Fi capability and a Wi-Fi access point. Some of these machines are sold pre-configured so setting up the network is as simple as plugging in the machine and turning on the power.

WLANs are growing in popularity and thus have a head start defining high performance wireless data in the marketplace (5). Users also are attracted to a wireless service that, according to Garber, “will look like Ethernet and act like a corporate network.” It is also noted that although WLANs are currently private networks, they could eventually become public networks.

SECURITY

As we become more reliant on WLAN technology, the security issue will become that much more important (4). Traditionally, the physical attachment of network nodes behind a firewall, with one access point to the outside world, made it easy to block illicit entry (4). The main security concern with WLANs is all that’s needed to gain entry onto the network is physical proximity.

There are some serious security issues with Wi-Fi. All Wi-Fi products have built-in security provisions, but many products require activation by the user, who may be unaware that activating security tools is their responsibility. There is also the possibility that the built-in security is not as secure as possible.

Tighter security for Wi-Fi networks is forthcoming (and already built into Windows XP) in the form of IEEE-802.1x authentication (4). This is a security specification that brings user authentication to a network's access point, thus preventing any exchange of data between a network's server and an unauthorized user.

Nevertheless, the greatest network security problem facing many wireless users is their own failure to use, or properly configure, the wireless security mechanisms now available (11). VanDerSchuur recommends that in order to achieve security to that of traditional wired LANs, users should seek the services of reputable security consultants and wireless installers.

IEEE 802.11B

The wireless local area networking market is home to a wide variety of technologies, but products that use the IEEE 802.11b technology, also known as Wi-Fi, are recommended for installing a wireless network in either a home or office. Wi-Fi products are the best networking options for several reasons, one of which is that it is targeted towards business, which means that you can use the same technology at work and home (4).

IEEE 802.11b products are tested for interoperability by an organization known as the Wireless Ethernet Compatibility Alliance (WECA). Products that meet WECA's criteria for interoperability receive Wi-Fi certification. Devices that are Wi-Fi certified should be compatible directly from the box, even if they are from different manufacturers. In a press release in January 2002, WECA announced that 232 Wi-Fi certifications had been awarded to 61 WECA member companies' products since March of 2000 (12). Products include access points, WLAN-to-Internet gateways, print servers, and laptops with built in Wi-Fi connectivity (4). This continued growth in certifications indicates that Wi-Fi is the world's dominant wireless LAN technology.

INTRODUCING THE ALTERNATIVES

Although Wi-Fi is currently the best choice for WLAN installations, it is hardly the only choice (4). Faster IEEE-802.11 networks are coming soon. HomeRF is one of IEEE 802.11's top competitors. In Europe, there are HiperLAN (high-performance radio LAN) and HiperLAN/2 installations. There are also technologies such as Symphony and RangeLAN that were popular before the IEEE standardized the 802.11 series technologies.

Most of theses technologies operate in the 2.4-Ghz Industrial, Scientific, and Medical (ISM) band (4). These technologies sometimes suffer with interference with other products that use 2.4-Ghz, such as microwaves and cordless phones. IEEE 802.11a and HiperLAN/2 operate in the 5-Ghz Unlicensed National Information Infrastructure band (UNII). WLAN technologies that operate in different frequency ranges can overlap without creating interference with one another. For example, an 802.11a and 802.11b network can be installed in the same air space without having a negative impact on the performance of either network.

IEEE 802.11A

Wireless networks based on the IEEE 802.11a (Wi-Fi5) specification promise throughput of up to 54 Megabits per second (1). IEEE 802.11b, or Wi-Fi, has a limit of only 11 Mbps. Much of the increase comes from use of the orthogonal frequency division multiplexing (OFDM) modulation technique (9). While the high throughput may be a good reason for corporate users to switch to Wi-Fi5, it really isn't worthwhile for home users who want to wirelessly share Internet connections because of its premium price. Home users may also not want to use it because it is still limited in what products it has to offer, especially in terms of an installed user base (4). It is also incompatible with IEEE 802.11b. Instead it is more suitable for businesses that transfer large data files (i.e. graphics, videos, and databases) or need to accommodate more users per access point.

There are several reasons to consider using 802.11a (6). One reason is because there's need for much higher performance. By far the top driver for choosing 802.11a is the need to support higher end applications involving video, voice, and the transmission of large images and files. For these applications, 802.11b probably won't be able to keep up.

Another reason is because significant RF interference is present within the 2.4 GHz band (6). The growing use of 2.4 GHz wireless phones and related devices could crowd the radio spectrum within your facility and significantly decrease the performance of 802.11b wireless LANs. The use of 802.11a operating in the 5 GHz band will avoid this interference.

Another reason to choose IEEE 802.11a is because end users are densely populated (6). Places such as computer labs, airports, and convention centers need to support lots of end users in a common area competing for the same access point, with each user sharing the total throughput. The use of 802.11a will handle a higher concentration of end users by offering greater total throughput.

Something to keep in mind is that the interoperability among 802.11a and 802.11b will considerably improve over the next year (6). For example, some companies dealing in wireless technology are working towards the development of a dual 802.11a/b chipset. This will enable product developers to deliver wireless LAN radios that talk both 802.11a and 802.11b.

As a result, an 802.11a/b radio within an end user device will automatically sense whether the access point is 802.11a or 802.11b and then communicate accordingly (6). Likewise, an access point can also deploy the dual 802.11a/b solution; enabling interoperability with end user devices equipped with either an 802.11a or 802.11b radio. With this in mind, companies will be able to use both 802.11a and 802.11b.

IEEE 802.11E

The 802.11e committee is working to establish Ethernet quality of service characteristics within 802.11 wireless LANs (9). The standard applies to all 802.11 implementations and is expected to link the wired Ethernet QoS and the wireless world.

The goal of 802.11e is to help wireless LANs handle interference--by moving away from it--and to provide better support for those big streaming multimedia files by using error-correction and better bandwidth management (3).

IEEE 802.11G

The 802.11g standard, which is also known as 802.11b-extended, seeks to increase the data throughput of the 2.4-Ghz ISM frequency band (9). 802.11g would provide initial throughput of 32 Mbps with the potential to grow to 54 Mbps and beyond. IEEE 802.11g will be slower than "a," but faster than "b". It is also expected to be backward compatible, which means that it will work with 802.11b.

IEEE 802.11a and 802.11g now share a common high-rate waveform (OFDM) and offer complementary advantages to consumers (14). IEEE 802.11a systems enjoy more spectrums at 5 GHz, thus allowing for more channels and, by extension, more users. On the other hand, 802.11g systems provide backward compatibility with existing Wi-Fi devices and offer a range advantage relative to systems operating at 5 GHz.

IEEE 802.11I

Originally focused on 802.11b systems, the 802.11i committee is developing new data security protocols for use in all 802.11 systems (9). The original standard included a wired equivalency protocol (WEP) with two key structures, 40 and 128 bits long. WEP is essentially an encryption technique that incorporates none of the more advanced security techniques known to the networking industry.

The most significant development has come from 802.1x. It establishes a lightweight version of the extended authentication protocol (EAP) applicable to 802.11. EAP uses Radius for authentication, authorization, and access to the wireless system, and it serves to derive the WEP encryption key on request by a client device for a session association.

HOMERF 2.0

Home Radio Frequency (HomeRF) is a wireless personal area network technology from the HomeRF Working Group that uses the Shared Wireless Access Protocol (SWAP) and provides an open standard for short-range transmission of digital voice and data between desktop devices and mobile devices such as laptops, PDAs, and phones (8). Transmitting in the unlicensed 2.4GHz range, up to 127 devices can be addressed within a range of 150 feet at a data rate of 1 or 2 Mbps.

HomeRF 2.0 has had a major improvement in its transfer speed from its previous version, bringing the bandwidth up to 10 Mbps, the same speed as standard wired Ethernet (8). This is a vast improvement since HomeRF 1.0, which had speeds of only 1.6 Mbps.

HomeRF 2.0's security model is relatively transparent to the end user and very secure (8). HomeRF 2.0 uses a technology called frequency hopping. This keeps the 'data channel' shifting from one frequency to another many times a second, which makes it very hard for someone to eavesdrop on your network. Also, HomeRF 2.0 has introduced the concept of a 'network password' needed to join your network. Without knowing the password, peripherals will be unable to communicate with the network. Lastly, the HomeRF 2.0 standard includes support for 128-bit encryption so all the data traveling across the radio waves is scrambled.

HomeRF 2.0 is also much more resistant to interference than IEEE 802.11b. HomeRF also uses 2.4GHz but will track the particular kinds of interference in your home and work

around them (8). It does this by figuring out what 'data channel' the interference is on, and then telling the frequency hopper to not use that channel.

HIPERLAN/2

When compared to HiperLAN/2, other WLAN products are often found to be less efficient with regard to throughput, do not offer Quality of Service, and are not flexible but restricted to a single core network type (7). HiperLAN/2 can also be used in a variety of networks due to its convergence layer concept. This makes it future proof, too, since, once you have bought a piece of hardware, your device can be upgraded by software with additional convergence layers for operation in different network types.

HiperLAN/2 is a centrally controlled system where the central controller has full knowledge of all buffer states in the terminals (7). The central control leads to a much higher efficiency with regard to throughput compared to IEEE 802.11, and the ability to fully support quality of service. Moreover, it can be used in various core network environments, whereas IEEE 802.11 is only suited for application in Ethernets.

HiperLAN/2 can also be used at home (7). There, an ad hoc capability can be added and the network serves as the connection between all kinds of devices, such as video cameras, TVs and Hi-Fi sets.

HiperLAN/2 can also be applied as public networks (7). Due to the low transmission power allowed, the range will be restricted to approx. 50 m per access point. Therefore HiperLAN may be used to cover hot spot areas, such as airports, train stations or fair grounds, where a critical requirement for high-speed data communication is met. One can even imagine having access to an Internet Service Provider in some areas.

ULTRA-WIDEBAND

Ultra-wideband (UWB) -- a breakthrough wireless technology with applications for public safety, home networking and high-speed data transmission, has only recently been given the nod by the U.S. Federal Communications Commission (FCC) (13).

In a nutshell, UWB is revolutionary because it delivers broadband wireless communications without using radio waves on specific spectrum bands (13). Instead, data is transmitted using time and amplitude modulated pulses of energy, less than one nanosecond in duration, across a wide swath of frequencies.

UWB can coexist with carrier frequency users without interference (13). By reusing RF spectrum, it ushers in a wide array of communications options to ease the growing bandwidth crunch.

The technology currently can deliver hundreds of megabits of wireless data, with an eventual capacity in the gigabit range, the agency said (13). And the broad spectral nature of UWB pulses enables wireless communications to penetrate walls and obstacles better than existing technologies. It also delivers positional accuracy on UWB devices to within one-centimeter resolution, the FCC said.

WLANS GOING LONG DISTANCE

One of the more interesting developments in the WLAN world is the extent to which WLAN technology has been adapted for wide-area use (4). Using local-area technology for a wide-area wireless network involves the use of microcellular architecture. Fundamentally, it's the same as a cellular network, except the cells are so small that a moving device will pass from one access point to another more frequently. To create a microcell network, access points must be installed virtually everywhere so that the area of the WLAN is covered. Unfortunately, it is very costly and companies are at risk of being shut down if they don't have the financial means to fund such a project.

CONCLUSIONS

Wireless local area networks (WLANs) are the same as the traditional LAN but they have a wireless interface. One of the most attractive aspects of a WLAN is its ease of installation. As we become more reliant on WLAN technology, the security issues will become that much more important. Although Wi-Fi is currently the best choice for WLAN installations, it is hardly the only choice. Something to keep in mind is that the interoperability among 802.11a and 802.11b will considerably improve over the next year.

Current and future technologies for WLAN include IEEE 802.11, HiperLAN, HomeRF, and Ultra-Wideband. These and newer wireless technologies will be in use in the office, home, and educational centers of the future.

References

1. Arar, Yardena (2002, February). Wireless Nets Hit 54 MBPS. PC World, 20.
2. Ciampa, Mark (2001, August). Soon To Be a Wireless World. Retrieved February 23, 2002 from http://www.course.com/techtrends/wlan_082001.cfm
3. Coursey, David (2002, November 6). A, B, E, and G--What 802.11 means to me (and you, too). Retrieved February 26, 2002 from http://www.zdnet.com/anchordesk/stories/story/0,10738,2822686,00.html
4. Forman, David (2002, April). All About Wireless Networking. PC Upgrade, Vol. 11, No. 2, 60-66.
5. Garber, Lee (2002, January). Will 3G Really Be the Next Big Wireless Technology? Computer, 26-32.
6. Geier, Jim (2002, January 24). The BIG Question: 802.11a or 802.11b? Retrieved February 25, 2002 from http://www.80211-planet.com/columns/article/0,4000,1781_961181,00.html
7. HiperLAN/2 (2001). Retrieved February 26, 2002 from http://www.kbs.uni-hannover.de/~allert/hiperLAN/link5.html
8. Kaminski, Chris (2001). Technology Overview of HomeRF 2.0. Retrieved February 23, 2002, from http://www.homenethelp.com/web/explain/about-homerf-2.asp
9. Kapp, Steve (2002, January/ February). 802.11: Leaving the Wire Behind. IEEE Internet Computing, 82-85.

10. Toenjes, Paul G. (2002, February). Increase Productivity With Wireless. .Net Magazine, 31-36.
11. VanDerSchuur, Leo (2001, November). Wireless adds flexibility to high-speed Ethernet. Control Solutions, 28-33.
12. Wi-Fi Wireless LANs Continue to Grow at an Amazing Pace. (2002, January 7). Retrieved February 26, 2002, from http://www.weca.net/pr/industryreleases.asp
13. Wrolstad, Jay (2002, February 15). U.S. Approves Ultra-Wideband Technology. Retrieved February 26, 2002, from http://www.wirelessnewsfactor.com/perl/story/16374.html
14. Zyren, Jim (2002, February 1). 802.11g spec: Covering the basics. Retrieved February 26, 2002 from http://www.commsdesign.com/design_corner/OEG20020201S0035