

PICK YOUR WIRELESS SOLUTION

Abstract

As Microsoft changed the world of computer applications in the 90s, wireless computer communication is modeling a new landscape in today's 00s. The telecommunications and the computer industries are converging to launch a new revolution: the Wireless Network.

Using a laptop computer equipped with a wireless card is now a reality. You can hook up to either your company's network or a public network (Internet) at work, cafes, hotels, restaurants, airports, and generally speaking, at every place where you are within a few hundred feet of an access point to a wireless local area network (WLAN).

The new concept of the wireless personal area network (WPAN) extends the wireless Internet to a wide range of products, including mobile telephones and handheld devices. Because of the strong expected growth for the wireless network market, many companies are rushing take advantage of the opportunity to introduce one of the new prevalent standards in the wireless world. The current leaders among these standards are Bluetooth and IEEE 802.11b. However, there are other technologies in the market to consider.

This article will explain the features, advantages, and disadvantages of these different technologies compared to a wired network. This report will explore whether these solutions are in competition, or if there is a place for everybody. Whether you are an individual user or a business contemplating a new network, this report will help you to define more clearly which wireless solution you should choose.

PICK YOUR WIRELESS SOLUTION

Wireless poised for growth

Although some still say “people just don’t want their computers to be mobile” (Ferro 5) and conclude that wireless “is not going to revolutionize the world” (Ferro 21), the wireless LAN market is one of the fastest-growing segments of the communications industry. “Cahners-Instat foresees the industry growing from the \$1.1 billion of 2000 to \$5.2 billion by 2005” (Abramovitz 1). “A Microsoft survey late [in 2001] found wireless LANs in 30% of enterprises. And of those that didn’t have them, 70% plan to implement the technology soon” (Phifer 2).

The potential growth of this market is undeniable. But what about the real cost-benefits of this technology?

The wireless LAN paid for itself within 12 months. The cost of installing and maintaining a WLAN over time is lower than a traditional wired LAN. A WLAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. And because WLANs simplify moves, adds, and changes, they reduce the indirect costs of user downtime and administrative overhead (Armenta 6).

Access Points and network interface cards (NICs), the main wireless products currently on the market, are getting cheaper and cheaper. That should help the rapid growth of the industry, and therefore, allow extending the market to a wider range of devices, such as printers, wireless LAN enabled phones, web cameras, MP3 players, handhelds, etc...

Thereby it is time to give a small brush-stroke on what the technologies are and what they offer.

Technologies on the market

Technology	Bandwidth	Frequency	Comments
802.11a	54 Mbps	5.15 – 5.825 GHz	Upcoming
802.11b	11 Mbps	2.4 – 2.4835 GHz	Currently deployed
802.15	-not defined-	2.4 – 2.4835 GHz	In research
802.11g	22 Mbps	2.4 – 2.4835 GHz	Backward compatibility with 802.11b
Bluetooth	1.5 Mbps	2.4 – 2.4835 GHz	Currently deployed
HiperLAN/1	24 Mbps	5.15 – 5.825 GHz	Currently deployed
HiperLAN/2	54 Mbps	5.15 – 5.825 GHz	In research
Home RF	1.6 Mbps	2.4 – 2.4835 GHz	Designed for home market.
IrDa	16 Mbps	Infrared	Currently deployed

The two most popular wireless technologies on the market are IEEE 802.11b and Bluetooth. Nevertheless other options such as IrDa, Home RF and the new 802.15 are or will be in the game.

PICK YOUR WIRELESS SOLUTION

802.11a that is just beginning to appear in the market, features a speed up to 54 Mbps and operates in the 5GHz band. It introduces the possibility of high bandwidth applications over the wireless network, such as video conferencing. Since it is located in a different frequency, it suppresses interference with devices like microwave ovens, cordless phones, and Bluetooth products. This solution looks very attractive for people who wish to set up a new wireless LAN and don't have to address any standard interoperability problem with existing wireless equipment. Companies that already have a broadband wired connection and don't want to change for the lower throughput offered by 802.11b, 802.11a is now an opportunity to consider, or even for ISP that wish to offer the public high speed wireless internet access at home.

802.11b is a type of WLAN designed for covering a range of up to 100 meters. It is a true multipoint networking technology, similar to a "wireless Ethernet", that provides theoretical bandwidth up to 11 Mbps. Is being adopted chiefly, due to its characteristics, by companies that desires to enhance their service to the customer, providing solutions that wired networks can not handle.

802.11g is an evolution of 802.11b. Operating in the same 2.4 GHz band, it provides a higher data rate and guarantees backward compatibility with 802.11. It could be used as an upgrade of an existing 802.11b network for companies that require a higher data transmission rate.

802.15 is the upcoming and strongest rival of Bluetooth. The IEEE has four task groups dealing with this new standard for the WPAN field. It will be completely compatible with its big brother 802.11, which means it can overthrow Bluetooth from the WPAN market. At the moment it is released in the market and adopted by manufacturers, there will no longer be any more headaches, as both the interference and incompatibility issues will be fixed in a wink.

Bluetooth belongs to the new concept of WPAN and is designed for cable replacement application within a range of 10 meters. This technology provides theoretical bandwidth up to 1 Mbps. Bluetooth works creating 10 meter bubbles that can hold up to 8 devices (1 master and 7 slaves) and supports both voice and data transmission. Additionally it is possible to form a scatternet led by a Bluetooth master device in one piconet and a slave in another piconet.

PICK YOUR WIRELESS SOLUTION

Addressed for the personal use, the Special Interest Group (SIG) works on the design of a full variety of applications that run on devices such as headphones, printers, Pocket PCs, Hand Held devices and mobile phones.

HiperLAN is a European Telecommunications Standards Institute (ETSI) standard ratified in 1996. There exist two version of the standard, HiperLAN /1 and HiperLAN/2

Home RF is a protocol designed for the home market

IrDa is the natural competitor of Bluetooth in the WPAN field. While its counterpart uses radio frequency, IrDa uses optical guidance. The main disadvantage of it is that both devices have to be lined up to communicate. The bandwidth rate is up to 16 Mbps with an efficiency range of 2 meters. Despite of this big disadvantage it still has not fallen into the oblivion by manufacturers of both computer and telecommunication industry, but for users.

802.11b and Bluetooth have often been presented as competitors. "A lot of people talk about how Wi-Fi might be beating Bluetooth, but it's a different market altogether" (RO).

Clearly, terrific growth is imminent and valid technologies are available on the market. Sounds great. However, there is still one point that seems to keep some people from going for wireless: security.

A major wireless challenge: Security

Al Potter, Manager of Network Security Labs at International Computer Security Association (ICSA), has one word for the security exposure he has seen: "Terror." (www.net-security.org). The reason is straightforward, "The inability to physically secure a wireless network is considered to be its Achilles heel" (Colubris White Paper 1).

Going deeper in the problem, "Access Points uses radio signals in the 2.4 GHz range, a range accessible to any computer with a wireless network interface card (NIC) or frequency scanner" (Wavelink White Paper 1). But the problem is also innate to the 802 standard because "it requires that wireless NICs operate in a full promiscuous mode, resulting in continual network broadcasts"(Wavelink white paper 1).

PICK YOUR WIRELESS SOLUTION

Wardriving [scanning the wave radio spectrum to find one open port at an access point] is a lot easier than wardialing [scanning telephone numbers to reach via a dial-up connection access to a company's network] and a lot less intrusive. All you need to play is a laptop, a wireless PC card, and some software. In my case, the software I needed is called Prismstumbler, designed to play nicely with the chipset my D-Link card is based on. (Barr 5)

If you think your company is secure you are wrong. Anyone with technological knowledge base can sniff into your Wireless Network (WN). Eavesdropping in a WN is as simple as to surf the Internet and install programs on your laptop programs like

- NetStumbler - tells you the access point name, whether encryption is enabled, and much other information
- Kismet - network sniffer for Linux that includes many of the same features as its twin NetStumbler
- AirSnort - a Linux based tool that tries to recover encryption keys, it claims that given the right number of packets it can crack the first line of defense of 802.1x networks, Wireless Equivalent Privacy (WEP)

Fortunately, secure solutions are available. "Most of the enterprise solutions involve existing Virtual Private Network (VPN) technologies that can be built into or on top of wireless LAN products. Smaller wireless LAN implementations find the Wireless Equivalent Privacy (WEP) standard or the common 128-bit extension of WEP sufficient" (Abramowitz 3). VPN offers a tight way to protect sensitive data communications providing "three levels of security: user authentication, encryption and data authentication" (Colubris White Paper 2).

At this time, the safest solution seems to set up your wireless network as follows: "You put it outside the corporate firewall and use a VPN to tunnel in. Clients who are not allowed to get on the network don't ever make it through the firewall. The VPN will also encrypt all the data coming out of the wireless client" (Cohn 16). The disadvantage of this solution is the burden of installing a VPN-client in all wireless devices you want to enable to access to your network.

PICK YOUR WIRELESS SOLUTION

Once, whether you are an individual or a company, connects a private network to the public network, all of a sudden thousands of new potential `users` pop up, prompting them to gain access of your resources.

Wireless networks are prone to `play` with, via Network Packet Sniffers, IP spoofing, Password challenging, Denial of Service (DoF), Jamming Frequency (JF), Fluhrer Mantin Shamir (FMS) attack and Man-in-the-middle attack (MITM), nevertheless the aim of this paper is not to focus in this issue but to explain how both the data and security breaches in WN takes place.

Security Breach	Gaining access to the Access Point (AP)	
	Reaching control over the network (NT) resources	
Data Breach	Data Privacy (DP)	
	Data Authentication (DA)	
	Data Integrity (DI)	
Solutions	P R O T O C O L S	Light Extension Protocol (LEAP)
		IPSec through a VPN
		Static WEP
		Secure Socket Layer (SSL)
	A D D	Access Control List (ACL)
		Service Set ID (SSID)
		Virtual LAN (VLAN)
	S W	Netmotion from NetMotion Wireless
		Mobile Manager from WaveLink
	H W	Bluesocket
		Reef Edge
Vernier Networks		
Major Problem	Key distribution	

Modeling a situation of how a WN works we come up with the following picture:

Whenever a wireless device (WD) receives the broadcast signal from an AP it has to identify itself if the AP is functioning in a closed mode, opposite to the open mode that immediately associates the WD to the

PICK YOUR WIRELESS SOLUTION

AP enabling access to the resources. The way to tackle with this is via authentication logons, SSID Control and ACL.

“Access points also send out periodic management frames known as beacons. Beacons contain access-point information such as the service set identifier, supported data rates, whether the access point supports frequency hopping or direct sequencing, and capacity. Beacon frames are broadcast from the AP at regular intervals, adjustable by the administrator” (Cisco - SAFE: WLAN Security in Depth 45)

Authentication Logons permit to verify either the WD is who it claims to be or conversely if the AP is who claims to be. Verifying the user via a password and a username we control what WD can 'link' to the AP. Checking the AP avoids the Rogue AP attack. The Rogue AP consists of an AP installed by a hacker in the range of other trusted APs as with the objective of deceiving the WC that tries to link that AP, whereby regarding sensitive information that the user provides.

SSID permits only to associate a WD to an AP if the client of the WN knows the ID number of that AP, and thereby gaining access to the wireless service. Many of the actual APs broadcast this information, making it easy to get the SSID.

ACL is similar to the SSID, but in this case the AP maintains a list of Media Access Control (MAC) addresses that can associate it. The shortcoming of this approach is that MAC addresses can be spoofed, an AP has a limited number of entries and for a multiple environment it creates more woes than joys. Reducing the scalability of the system and increasing the maintainability headaches.

If a hacker bypasses this phase then he/she gains access to whatever is beyond the AP depending upon the security level he has reached. At this moment is when the other three major issues turn up.

DP deals with the scrambling of the data to be only understandable by those parties that own the correct key to encrypt/decipher sensitive data. A key can be either symmetric or asymmetric, with an added shortcoming, how do I spread the supposed secret key?

Another issue is how do I know if the information that the AP is sending to me is not being bypassed by a hacker that has installed a Rogue AP. DA is also a major concern.

PICK YOUR WIRELESS SOLUTION

In the same way the hacker is able to get the packets from the spectrum wave he/she is also able to change the data that those frames contain. DI is solved with different mechanisms such as Cyclic Redundancy Checking (CRC), Message Integrity Check (MIC), Message Digest 5 – Hash-based Message Authentication (MD5-HMAC) and SHA-HMAC.

Because of the shortcomings detected in the 802.11b standard, many vendors have devised its own solution, what means to depend on proprietary HW, nevertheless solutions other than this have been designed if the product buyer does not want to stick to a manufacturer.

- Cisco has developed LEAP, a method that enables mutual authentication and encryption via RC4 algorithm but requires a Cisco secure Access Control Server (ACS) or a compatible Remote Access Dial-up Server (RADIUS).
- Agere also provides mutual authentication and encryption with its Advanced Mobile Security Architecture (AMSA) that uses Diffie-Helman algorithm for the key-exchange. The last enhancement is the rekeying every 5 minutes and authentication via Extended Authentication Protocol – Triangle Layer Security (EAP-TLS).
- Symbol Technologies uses the Kerberos algorithm for key exchange, mutual authentication and dynamic key definition per-client per-session.

From other parties it is possible to find solutions such as Netmotion and Wavelink in software, and from Bluesocket, Reefedge and Vernier Networks in hardware. These solutions are aimed to individuals or companies that stick to the static WEP standard defined by the IEEE. The SSL protocol, used in today's secure web transaction is a solution available for WN. "SSL is a security transport protocol that sits right below the application layer in the TCP/IP stack. It was built to stream data securely". (Getgen 3)

In the other hand, each Bluetooth device has a 48 bit fixed public address that is unique for each, combined with a 128 bits private user authentication key, a 8-128 bits private user encryption key and a 128 bit random number generated for each transaction between the Bluetooth devices. These four pillars give Bluetooth a strong mechanism to stop eavesdroppers from getting into the information in the wireless bubble.

PICK YOUR WIRELESS SOLUTION

Security solutions exist for wireless products. The IEEE Task Group I is currently working on extensions, to incorporate in a short future enhancement algorithms and authentication steps. The biggest security threat is that many companies fail to use security features, either because they don't think it is worth it or because they don't know how.

Although these two technologies, Bluetooth and 802.11b seem to be complementary rather than competing, their coexistence is not necessarily simple because their collocation in the frequency band results in the potential for interference.

The crowded 2.4 GHz band: Interference

Another major challenge faced by wireless LANs/PANs is Interference. All the different technologies can deal relatively well with the interference caused by microwaves, cordless phones, etc. But mutual interference between the wireless LAN and the wireless PAN, is altogether a different problem.

Since 802.11b and Bluetooth share the same band frequency, which extends from 2.4 to 2.4835 GHz, they can potentially interfere with each other. Neither technology was designed with the capability to combat interference created by the other.

Recent studies show that if the separation between a Bluetooth device and a Wi-Fi device is more than three meters, the performances of both systems are good. Between three meters and about a half-meter, the degradation becomes significant. "For the most reliable data transfer rates, it is necessary to keep IEEE 802.11b DSSS and Bluetooth radios at least three meters apart" (Chandrashekhar D-75). When the radios are brought into close proximity, interoperability is impossible. "We can clearly see that it is unfeasible at this time for the IEEE 802.11b DSSS and Bluetooth radios to reliably operate simultaneously in the same computer. More specifically, they will completely cancel or 'kill' each other" (Chandrashekhar D-75).

Because one may want to surf the Internet using an 802.11b type of connection, and at the same time have a laptop communicating with another device using a Bluetooth type of connection, this problem needs to be addressed. One approach is to develop technical solutions (either software or hardware). Those possibilities must be balanced carefully, since they may affect system performance. Another

PICK YOUR WIRELESS SOLUTION

approach is to move to an alternate frequency band. It is the solution retained by 802.11a that operates in the 5 GHz band, where you don't have to worry about mutual interference. But moving to a higher band frequency also involves smaller range, higher cost, and the need to meet international requirements.

WLAN 802.11 provides a link layer acknowledgement function which goal is to provide notifications to the transmitter that the receiver has received the appropriate frame.

Conclusion

Wireless networks are poised for terrific growth. They offer lower costs and greater convenience than wired networks. Security is a real concern, but solutions are available and effective if they are applied properly. Vendors of wireless products are making a big effort to devise the right method to avoid eavesdroppers from gaining access to your wireless network. It is possible to choose among different technologies upon your needs and budget.

Since Bluetooth and 802.11b are complementary rather than competing, they are expected to coexist. However, concern over interference arises when they operate in the same environment. Maybe is a good solution to move out of the packed Industrial Scientific Medical (ISM) band and pick some different.

As we mentioned at the beginning whether you are a company or an individual you have to be aware of the benefits of going for wireless. We have shown the benefits and shortcomings of a huge range of technologies, focusing mainly on the pace of the market.

Inevitably going for wireless is an important step in terms of money, both for maintenance and locations that have a difficult wired access. But, at what price?? Without the boundaries of the wired network the number of intended recipients of information blows up. In spite of this shortcoming we have shown means to control security threats. We also have talked about the compatibility issues between some of them.

Individuals have a enormous variety of products with both Bluetooth and 802.11b technologies built in. But, the answer to the question, what is the best option, only has reply on oneself. The reason in

PICK YOUR WIRELESS SOLUTION

that many are the variables that influence the resolution of the equation, and the different combinations are optimal should you outline the `picture` needed.

An important question comes from an examination of these two technologies: why pay for both technologies when the next evolution of 802.11b could do what Bluetooth does?

PICK YOUR WIRELESS SOLUTION

Works Cited

Abramovitz, Jeff. Wireless LANs – Poised for Untethered Growth. Wireless LAN Association web.

October 2001. <http://wlana.org/pdf/wlana_industry.pdf>

Armenta, Anthony. “QetA: Wireless LAN Association a WLAN resource”. Interview with Jack

Pickell. *SearchNetworking*. 16 Jan. 2002.

Bluetooth. “Bluetooth Security White Paper”. Apr. 2002.

<www.bluetooth.com/upload/24Security_Paper.PDF>

Bluetooth. “Security comparison: Bluetooth Communications vs. 802.11”.

<www.bluetooth.com/upload/14Bluetooth_Wifi_Security.pdf>

Chandrashekar et al. Evaluation of Interference between IEEE 802.11b and Bluetooth in a Typical Office Environment.

Cisco Systems. “Wireless LAN Security”. Nov. 2001.

<www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.pdf>

Cisco Systems. “Security Technologies”. 2002.

<www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/security.pdf>

Cisco Systems. White Paper. “SAFE: *Wireless LAN Security in Depth*”. Jan. 2002.

<www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf>

Cisco Systems Product Bulletin No. 1515. “*Cisco Wireless LAN Security Bulletin*”. Nov. 2001.

<www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.pdf>

Colubris Networks. White Paper. “Building Secure Wireless Local Area Networks”. 2001.

<www.colubris.com/en/support/whitepapers/whitepapers/WP-010712-EN-01-00.pdf>

Compaq White Paper. “Bluetooth Technology Overview”. Nov 2000.

Ericsson Research. “Bluetooth – an Enabler for Personal Area Networking”. Per Johansson.

Ferro, Greg. “Wireless Ethernet: Just another (yawn) tool in my toolbox”. *searchNetworking* 07

Feb. 2002.

Getgen, Kim. “Securing the air: Security in the Palm of your Hand”. Feb. 2002.

<[www.ibm.com http://www-106.ibm.com/developerworks/wireless/library/wi-sec3.html](http://www.ibm.com/http://www-106.ibm.com/developerworks/wireless/library/wi-sec3.html)>

PICK YOUR WIRELESS SOLUTION

Getgen, Kim. "Securing the air: In code we trust". Mar. 2002.

<[www.ibm.com http://www-106.ibm.com/developerworks/wireless/library/wi-sec4.html](http://www.ibm.com/http://www-106.ibm.com/developerworks/wireless/library/wi-sec4.html)>

Getgen, Kim. "Securing the air: Don't let your wireless LAN be a moving target". Nov. 2001.

<www-106.ibm.com/developerworks/library/wi-sec1/index.html>

Heath, Robert W. Interview about Wireless LANs. Electrical Engineering Department,
The University of Texas at Austin. 27 Feb. 2002.

IBM. "Wireless Security Auditor (WSA)".

<www.research.ibm.com/gsal/wsa/>

IBM. "A security strategy for mobile e-business". Jul. 2001.

<www-3.ibm.com/pvc/tech/pdf/gsoee213.pdf>

IEEE. "Interference between Bluetooth networks – Upper bound on the packet error rate". Jun 2001

IEEE. "Link performance of an embedded Bluetooth Personal Area Network". 2001

Lorson, Joe. "Bluetooth". Motorola Lecture. Electrical Engineering Department,
The University of Texas at Austin. 29 Mar. 2002.

Microsoft. "Making IEEE 802.11 Networks Enterprise-Ready". Mar. 2001.

<www.microsoft.com/windows2000/docs/wirelessec.doc>

Mankle, Chris. Interview about Wireless LANs. McCombs School of Business,
The University of Texas at Austin. 4 Mar. 2002.

Matthews, Tim. Interview on the Wireless Network of the McCombs School.

McCombs School of Business, The University of Texas at Austin. 19 Feb. 2002.

Molta, Dave. "WLAN Security on the rise". *Network Computing*. Feb. 2002.

<www.networkcomputing.com/1303/1303ws2.html>

ORiNOCO. "Wireless LAN Security". 7 Mar. 2002.

<ftp://ftp.orinocowireless.com/pub/docs/ORINOCO/BULLETIN/TECH/March_7_02_ORINOCO_Wireless_LAN%20Security_Response.pdf>

Phifer, Lisa. "How secure is the WLAN today? Tomorrow?" Interview with Jack Pickell.

SearchNetworking. 08 Feb. 2002.

PICK YOUR WIRELESS SOLUTION

Rappaport, Ted. "The Wireless Internet Future." ECE Distinguished Lecture.

The University of Texas at Austin. 2 Apr. 2002.

Stark, Tom. "Something in the air: Through a scanner, darkly". Oct. 2001.

<www-106.ibm.com/developerworks/library/wi-sky4.html>

Symbol Technologies. "Technology for a secure Mobile Wireless LAN Environment: Evolution, Requirements, Options". Dec. 2001.

<[ftp://symstore.longisland.com/Symstore/pdf/SecurityWhitePaperFinal.pdf](http://symstore.longisland.com/Symstore/pdf/SecurityWhitePaperFinal.pdf)>

Symbol Technologies. "Wireless For Beginners". 2001

<[ftp://symstore.longisland.com/Symstore/pdf/WirelessForBeginners_110901.pdf](http://symstore.longisland.com/Symstore/pdf/WirelessForBeginners_110901.pdf)>

Symbol Technologies. "RF site survey and antenna selection for optimum wireless LAN Performance". <[ftp://symstore.longisland.com/Symstore/pdf/RFsitesurvey.pdf](http://symstore.longisland.com/Symstore/pdf/RFsitesurvey.pdf)>

Wavelink. White Paper "Wireless Network Security." 2001.

<www.wavelink.com/downloads/whitepapers/Wireless_network.pdf>