A Detailed Study on Wireless LAN Technologies

Vijay Chandramouli
Department of Computer Science and Engineering
The University of Texas at Arlington
vmouli@uta.edu

Abstract

Wireless Communication is an application of science and technology that has come to be vital for modern existence. From the early radio and telephone to current devices such as mobile phones and laptops, accessing the global network has become the most essential and indispensable part of our lifestyle. Wireless communication is an ever-developing field, and the future holds many possibilities in this area. One expectation for the future in this field is that, the devices can be developed to support communication with higher data rates and more security. Research in this area suggests that a dominant means of supporting such communication capabilities will be through the use of Wireless LANs. As the deployment of Wireless LAN increases well around the globe, it is increasingly important for us to understand different technologies and select the most appropriate one. This paper provides a detailed study of the available wireless LAN technologies and the concerned issues. This is followed by a discussion evaluating and suggesting a feasible standard for future.

1 Introduction: The increased demands for mobility and flexibility in our daily life are demands that lead the development from wired LANs to wireless LANs (WLANs). Today a wired LAN can offer users high bit rates to meet the requirements of bandwidth consuming services like video conferences, streaming video etc. With this in mind a user of a WLAN will have high demands on the system and will not accept too much degradation in performance to achieve mobility and flexibility. This will in turn put high demands on the design of WLANs of the future. In this paper, we first discuss the various Wireless LAN standards available for deployment. Secondly, a study on the challenging factors of these with a little overview on security issues in wireless LAN is discussed. Finally, an analysis of the available Wireless LAN standards and a feasible solution for future deployment is discussed.

A wireless LAN is based on a cellular architecture where the system is subdivided into cells, where each cell (called Base Service Set or BSS*) is controlled by a Base station (called Access point or AP). Wireless LAN standards that are currently being explored in the field of communications technology are:

1. IEEE 802.11.
   a. 802.11a
   b. 802.11b
   c. 802.11g
2. HiperLAN/2.
3. Bluetooth.
4. HomeRF.

*BSS – Base Service Set; an access point is connected to a wired network and a set of wireless stations.

1.1 Wireless LAN Standards: There are several wireless LAN solutions available today, with varying levels of standardization and interoperability. Two solutions that currently lead the industry are, **HomeRF** and **Wi-Fi*** (IEEE** 802.11b). Of these two, 802.11 technologies enjoy wider industry support and are targeted to solve Enterprise, Home and even public "hot spot" wireless LAN needs.

a. **IEEE 802.11:** The IEEE finalized the initial standard for wireless LANs, IEEE 802.11 [1] in June 1997. This initial standard specifies a 2.4 GHz operating frequency with data rates of 1 and 2 Mbps. With this standard, one could choose to use either frequency-hopping or direct sequence (two non compatible forms of spread spectrum modulation). Because of relatively low data rates (as compared to Ethernet), products based on the initial standard did not flourish as many had hoped.

In late 1999, the IEEE published two supplements to the initial 802.11 standard: **802.11a** and **802.11b (Wi-Fi*)**. The 802.11a [3] standard (High Speed Physical Layer in the 5 GHz Band) specifies operation in the 5 GHz band with data rates up to 54 Mb/s. The advantages of this standard (compared to 802.11b—Higher Speed Physical Layer Extension in the 2.4 GHz Band) include having much higher capacity and less RF (radio frequency) interference with other types of devices (e.g., Bluetooth), and products are just now becoming available throughout 2002. However, 802.11a isn't compatible with 802.11b and 802.11g products. As with the initial standard, 802.11b operates in the 2.4 GHz band, but it includes 5.5 and 11 Mb/s in addition to the initial 1 and 2 Mb/s. The 802.11b standard only specifies direct sequence modulation, but it is backward compatible with the initial direct sequence wireless LANs. The IEEE 802.11b standard is what most companies choose today for deploying wireless LANs.

The 802.11 working group is currently working to extend the data rates in the 2.4 GHz band to 54 Mb/s using OFDM (orthogonal frequency division multiplexing), which is the **802.11g** [7] standard. This standard will hopefully be ratified by the end of 2002. Companies should be able to easily scale their existing 802.11b products to become 802.11g-compliant through firmware upgrades. This enables companies having existing 802.11b infrastructures to scale up their network via relatively simple cost-effective changes.

b. **HiperLAN 1/2:** European Telecommunications Standards Institute, ETSI, ratified in 1996 with High Performance Radio LAN (**HiperLAN 1**) [4] standard to provide high-speed communications (20Mbps) between portable devices in the 5GHz range. Similarly to IEEE802.11, HiperLAN/1 adopts carrier sense multiple access protocol to connect end user devices together. On top of that, HiperLAN/1 supports isochronous traffic for different type of data such as video, voice, text, etc. Later, ETSI, rolled out in June 2000, a flexible Radio LAN standard called **HiperLAN 2**, designed to provide high speed access (up to 54 Mbps at PHY layer) to a variety of networks including 3G mobile core networks, ATM networks and IP based networks, and also for private use as a wireless LAN system. Basic applications include data, voice and video, with specific QoS***

* Wi-Fi: Wireless Fidelity; a term usually referred to 802.11b

** IEEE – Institute of Electrical and Electronic Engineers; best known for developing standards for the computer and electronic industry. ; ***QoS – Quality o f Service.

parameters taken into account. HIPERLAN/2 [5] has a very high transmission rate up to 54 Mbps. This is achieved by making use of a modularization method called Orthogonal Frequency Digital Multiplexing (OFDM). OFDM is particularly efficient in time-dispersive environments, i.e. where the radio signals are reflected from many points, e.g. in offices.

c. **Bluetooth:** Bluetooth is an industry specification for short-range RF-based connectivity for portable personal devices with its functional specification released out in 1999 by Bluetooth Special Interest Group [6]. Bluetooth communicates on a frequency of **2.45 gigahertz**, which has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM). One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of 1 milliwatt. The low power limits the range of a Bluetooth device to about **10 meters**, cutting the chances of interference between a computer system and a portable telephone or television. Bluetooth makes use of a technique called spread-spectrum frequency hopping. In this technique, a device will use 79 individual, randomly chosen frequencies within a designated range, changing from one to another on a regular basis. Bluetooth devices essentially come in two classes, both using point-to-point communication to speak. Class 3 devices operate at 0 dBm range and are capable of transmitting 30 feet, through walls or other objects and the other class is termed as class 1 products. These devices operate at 20 dBm, which allows for the signal to travel about 300 feet through walls or other solid objects. Both Bluetooth classes are rated at traveling at about 1 Mbps, with next generation products allowing anywhere from 2 to 12 Mbps, to be determined at a later date.

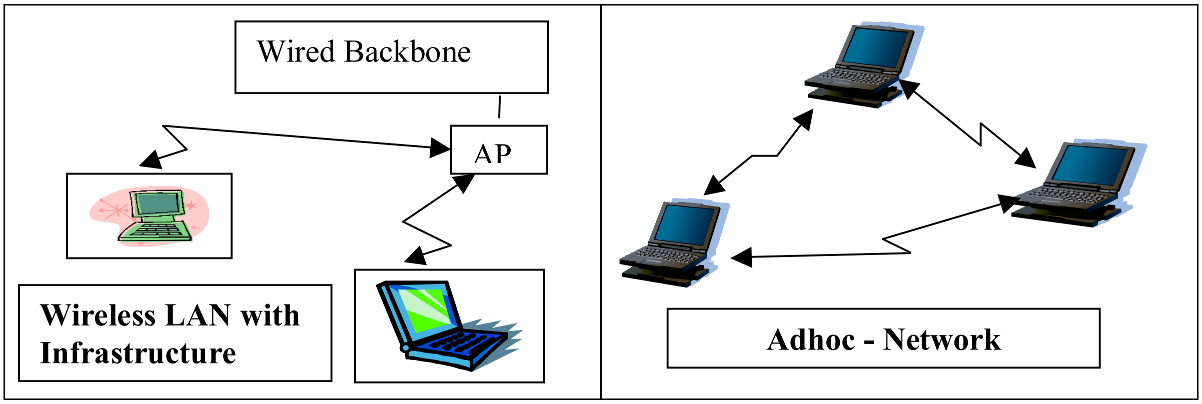
Standard	IEEE 802.11	802.11a/802.11b	HiperLAN/2	Bluetooth	HomeRF
Mobile Freq. Range (GHz)	N.A/Europe 2.4 – 2.483 Japan 2.47 – 2.499	**a** Aimed at 5.15 – 5.25 5.25 – 5.35 5.725 – 5.825 **b** NA/Europe 2.4 – 2.483 Japan 2.47 – 2.499	Aimed at 5.15 – 5.35 5.47 – 5.725	NA/Europe 2.4 – 2.483 Japan 2.47 – 2.499	NA/Europe 2.4 – 2.483 Japan 2.47 – 2.499
Multiple Access Method	CSMA/CA	CSMA/CA	TDMA	TDMA	TDMA/CSMA
Duplex Method	TDD	TDD	TDD	FDD	TDD
Number of Independent Channels	FHSS*: 79 DSSS*: 3-5	**a** 12 **b** 3 to 5	12	FHSS*: 79	FHSS*: 79

Source: Lucent Technology Labs; NA – North America

*FHSS, DSSS – two forms of spread spectrum radio; Frequency Hopping Spread Spectrum; Direct Sequence Spread Spectrum

d. **HomeRF:** HomeRF is an open industry specification developed by Home Radio Frequency Working Group [2] that defines how electronic devices such as PCs, cordless phones and other peripherals share and communicate voice, data and streaming media in and around the home. HomeRF-compliant products operate in the license-free 2.4 GHz frequency band and utilize frequency-hopping spread spectrum RF technology for secure and robust wireless communications with data rates of up to 1 Mbps (HomeRF 1). Unlike Wi-Fi, HomeRF already has quality-of-service support for streaming media and is the only wireless LAN to integrate voice. HomeRF may become the worldwide standard for cordless phones. In the year 2001, the Working group unveiled HomeRF 2.0 that supports 10 Mbps (HomeRF 2.0) or more.

1.2 Classification of Wireless LAN: Wireless LANs can be broadly classified into two categories: ***ad hoc wireless LANs*** and ***wireless LANs with infrastructure***. In ad hoc networks, several wireless nodes join together to establish a peer-to-peer communication. Each client communicates directly with the other clients within the network. Ad-hoc mode is designed such that only the clients within transmission range (within the same cell) of each other can communicate. If a client in an ad-hoc network wishes to communicate outside of the cell, a member of the cell MUST operate as a gateway and perform routing. They typically require no administration. Networked nodes share their resources without a central server.



In wireless LANs with infrastructure, there is a high-speed wired or wireless backbone. Wireless nodes access the wired backbone through access points. These access points allow the wireless nodes to share the available network resources efficiently. Prior to communicating data, wireless clients and access points must establish a relationship, or an association. Only after an association is established can the two wireless stations exchange data.

2 Issues over Wireless LAN: Since wireless devices need to be small and wireless networks are bandwidths limited, some of the key challenges in wireless networks are:

a. Data Rate Enhancements.
b. Low power networking.
c. Security.
d. Radio Signal Interference.
e. System Interoperability.

a. Enhancing Data Rate: Improving the current data rates to support future high speed applications is essential, especially, if multimedia service are to be provided. Data rate is a function of various factors such as the data compression algorithm, interference mitigation through error-resilient coding, power control, and the data transfer protocol. Therefore, it is imperative that manufacturers implement a well thought out design that considers these factors in order to achieve higher data rates.

b. Low Power Design: The size and battery power limitation of wireless mobile devices place a limit on the range and throughput that can be supported by a wireless LAN. The complexity and hence the power consumption of wireless devices vary significantly depending on the kind of spread spectrum technology being used to implement the wireless LAN. Normally, direct sequence spread spectrum (DSSS) based implementations require large and power-hungry hardware compared to frequency hopped spread spectrum (FHSS). They tend to consume about two to three times the power of an equivalent FHSS system. But, the complex circuitry provides better error recovery capability to DSSS systems compared to FHSS. The right time has come for researchers and developers to approach these issues in wireless LAN technologies together and from a global perspective.

c. Security: Security [10] is a big concern in wireless networking, especially in m-commerce and e-commerce applications. Mobility of users increases the security concerns in a wireless network. Current wireless networks employ authentication and data encryption techniques on the air interface to provide security to its users. The IEEE 802.11 standard describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN access point. In large enterprises, an IP network level security solution could ensure that the corporate network and proprietary data are safe. Virtual private network (VPN) is an option to make access to fixed access networks reliable. Since hackers are getting smarter, it is imperative that wireless security features must be updated constantly.

d. Radio Signal Interference: Interference can take on an inward or outward direction. A radio-based LAN, for example, can experience *inward interference* either from the harmonics of transmitting systems or from other products using similar radio frequencies in the local area. Microwave ovens operate in the S band (2.4GHz) that many wireless LANs use to transmit and receive. These signals result in delays to the user by either blocking transmissions from stations on the LAN or causing bit errors to occur in data being sent. Newer products that utilize Bluetooth radio technology also operate in the 2.4GHz band and can cause interference with wireless LANs, especially in fringe areas not well covered by a particular wireless LAN access point. The other issue, *outward interference,* occurs when a wireless network's signal disrupts other systems, such as adjacent wireless LANs and navigation equipment on aircraft.

e. System Interoperability: With wireless LANs, interoperability is taken as a serious issue. There are still pre-802.11 (proprietary) wireless LANs, both frequency-hopping and direct sequence 802.11 versions, and vendor-specific enhancements to 802.11-compliant products that make interoperability questionable. To ensure interoperability with wireless LANs, it is best to implement radio cards and access points from the same vendor, if possible.

Handoff: Handoff is the mechanism by which an ongoing connection between a Mobile host (MH) and a corresponding Access point (AP) is transferred from one access point to the other. Handoff occurs during cell boundary crossing, weak signal reception and while a QoS deterioration occurs in the current cell. Present handoff mechanisms are based only on signal strength and do not take into account the load of the new cell. There is no negotiation of QoS characteristics with the new AP to ensure smooth carryover from the old AP to new AP. Now, several methods are proposed by researchers to have a seamless handoff between access points.

3 Security Issues in 802.11:

During the beginning of the commercialization of the Internet, organizations and individuals connected without concern for the security of their system or network. Overtime, they realized that some form of security was required to prevent others from exploiting the connected resources. Deployment of Wireless LAN as a medium of communication to connect mobile devices with the wired infrastructure has paved a new path in the networking technology. Security should also be taken as an important factor while considering this way of communication. In contrary to their wired counterparts, a wireless network is more difficult to secure, since the transmission medium is open to anyone within the geographical range of a transmitter. Data privacy is usually accomplished over a radio medium using encryption. While encryption of wireless traffic can be achieved, it is usually at the expense of increased cost and decreased performance. Organizations are rapidly deploying 802.11 standard based wireless infrastructures. For most WLAN users, there are three basic issues:

a) **Data Compromise** is any form of disclosure to unintended parties of information. Data compromise can be inappropriate access to payroll records by company employees, or industrial espionage whereby marketing plans are disclosed to a competitor.
b) **Denial of Service** is an operation designed to block or disrupt normal activities of a network or facility. This can take the form of false requests for login to a server, whereby the server is too distracted to accommodate proper login requests.
c) **Unauthorized access** is any means by which an unauthorized party is allowed access to network resources or facilities. Unauthorized access can lead to compromise, for example, if access is gained to a server with unencrypted information, or destruction in the case that critical files, although encrypted on the server, may be destroyed.

The 802.11 standard provides several security mechanisms intended to provide a secure operating environment. In this section, we summarize each of these mechanisms with a major emphasis on the widely acknowledged Wired Equivalent Privacy (WEP) protocol.

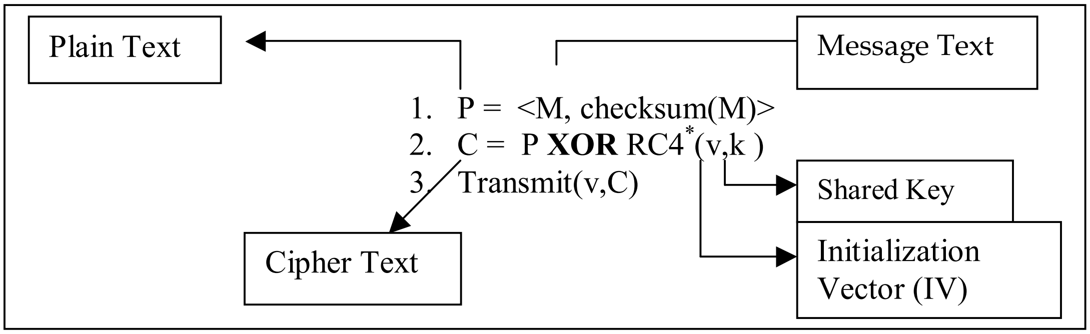
1. **Open System Authentication**: As the name implies, open system authentication authenticates anyone who requests authentication. Essentially, it provides a NULL authentication process. After the mobile gets associated, its data frames would be encrypted, if WEP was required in the WLAN. If WEP was not being used, the data frames would all be sent in the clear, i.e., although there is no initial authentication, data is encrypted.

2. **Shared Key Authentication:** Shared key authentication uses a standard challenge and response along with a shared secret key to provide authentication. In this, the access point sends string of unencrypted data to client and client encrypts with WEP key and sends back. This way of authentication is also insecure as a user sniffing the traffic would see the unencrypted and encrypted traffic.

3. **Wired Equivalent Privacy** (WEP) **Protocol**:

The IEEE 802.11 standard for wireless LAN communications introduced the WEP protocol in order to address the security problems discussed above and attempted to bring the security of the wireless systems closer to that of wired ones. The main goal of WEP algorithm is to protect wireless communication from eavesdropping. Although unauthorized access to a wireless network is not an explicit goal in the 802.11 standard for wireless communication, it is frequently considered to be a feature of WEP. Unfortunately, the 802.11 provides only limited support for wireless confidentiality through the Wired Equivalent Privacy (WEP) protocol [11]. Difficult security issues such as key management and a robust authentication mechanism are left as open problems by the standards committee. In this section, we first describe the features of WEP and then discuss about the pitfalls in WEP.

3.1 WEP Protocol Review:



The goal of WEP is to provide an equivalent level of privacy as is ordinarily present in an unsecured wired LAN by encrypting transmitted data. WEP has never intended to be an end-to-end security solution. WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The 802.11 standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks described above but no commercial systems that we are aware of has mechanisms to support such techniques.

WEP uses the RC4 encryption algorithm [8], which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce cipher text. The receiver has a copy of the same key, and uses it to generate identical key stream. The original plaintext is obtained by XORing the key stream with the cipher text. The original implementations of WEP used so-called "40-bit" encryption that implements a key of length 40 bits and 24 additional bits of system-generated data (64 bits total). Research has showed that 40-bit WEP contains security flaws, and consequently most product vendors today employ so-called "128-bit" encryption (key length of 104 bits, not 128 bits).

3.2 Flaws with WEP Protocol:

Risks of Key Stream Reuse: WEP provides security using a stream cipher called RC4. Stream ciphers operate by expanding a secret key (if WEP, a public IV and a secret key) into an arbitrarily long key stream of pseudorandom bits. A well known pitfall of stream ciphers is that encrypting two messages under the same IV and key can reveal information about both messages. WEP [8] needs an IV avoidance algorithm, to prevent one node from reusing an IV already used by another. WEP defines no such algorithm, and it is unclear how to even begin to design one.

Message Integrity: WEP uses an integrity [9] checksum field, implemented as a CRC-32 checksum, which is part of the encrypted payload of the packet to ensure that packets do not get modified in transit. However, CRC-32 is *linear*, which means that it is possible to compute the bit difference of two CRCs based on the bit difference of the messages over which they are taken. In other words, flipping bit n in the message results in a deterministic set of bits in the CRC that must be flipped to produce a correct checksum on the modified message. Because flipping bits carries through after an RC4 decryption, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid.

3.3 Alternatives to WEP:

Since WEP does not provide strong link-level security however it may accomplish its goal. Later, a revised version of WEP, known as WEP2 scaling the length of the key to 128 bits is proposed with mandatory Kerberos support. Although WEP2 increase the IV key space to 128 bits, it fails to prevent exploits and still permits IV key reuse. Also, the inclusion of Kerberos support merely opens WEP2 to new dictionary-based attacks. Analysis shows that although that security has been improved, there are additional problems associated with these.

In addition to WEP2, the 802.11i standard will likely include the **Advanced Encryption Standard** (AES) protocol. AES offers much stronger encryption. An issue, however, is that AES requires a coprocessor (additional hardware) to operate. This means that companies need to replace existing access points and client NICs to implement AES. Apart from this, the standard body would likely to propose an **Enhanced Security Network** which includes WEP, WEP2 and AES. It would make use of Kerberos for authentication mechanism and also provide dynamic association of key values.

3.4 Security in IEEE 802.11b vs HomeRF:

Data Compromise: 802.11b Encryption is done using WEP explained above. HomeRF standard defines 128-bit key encryption but with a 32-bit IV; compared to the 24-bit IV used in 802.11. The time scale for repeated IV is half a year instead of half a day. Unlike 802.11, a brute force attack on HomeRF encryption is inconceivable for organizations without the resources of a government security agency.

Unauthorized Access: 802.11b access control occurs by way of an exchange of management frames. The default protocol in the 802.11 standard is known as "Open System Authentication" [2] which means that the most systems will authenticate any user that makes the request. A more robust, but proprietary access control protocol, known as "Closed Network" has been implemented by Lucent in its products based on the 802.11b standard. The protocol is based on shared knowledge of a network name, or SSID*. Only those clients with knowledge of the network name can join. In HomeRF, all devices make use of a "shared secret" network ID (NWID) without which compliant devices will not be permitted to communicate. Because HomeRF uses a frequency hopping physical layer (as opposed to the frequency static and code static 802.11b physical layer) a client device must synchronize its hopping sequence with the access point in order to receive the data. In order to synchronize, the client must have the identical security NWID.

Denial of Service: The 802.11b DSSS is static in frequency and also uses a single DS "spreading code" for all time and all users, as specified in the standard. Anyone desiring to do so can generate valid 802.11b control packets which must be accepted by all 802.11-compliant equipment; alternatively, anyone can listen to all 802.11b control frames transmitted and this has proved vulnerable by hackers. On the contrary, HomeRF employs legitimate frequency hopping, which must be overcome in order to inject or detect control frames. It is extremely difficult to determine where in the frequency regime an access point is going to be at that moment.

4 Analyses:

In this section, a complete qualitative and comparative analysis of each of the existing wireless LAN technologies in the section is carried out.
a. Bluetooth: Bluetooth is proposed as a cable replacement technology and does not provide a complete wireless LAN solution. The advantages of Bluetooth technology are its very low power requirements and cost. Initial Bluetooth-based applications include file and data synchronization between devices, wireless headsets for mobile phones and

* SSID – Service Set Identifier, a 32- character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the base service station. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

computers, and connections to local peripheral devices. Hence, the Bluetooth technology [12] is far from ready for mass adoption. Systems using 802.11 wireless LAN technologies are designed with encryption choices and formal authentication through access port hubs, giving them the edge over Bluetooth, which is used for instant, inter-device communications in small groups with as little overhead as possible and limited security. It lacks the capability to simultaneously support multi-line telephony, Broadband speed data access and multiple streaming sessions.

b. 802.11b: At present, 802.11b is the clear winner in business wireless networking as it has a great advantage in that it is accepted worldwide. One of the more significant disadvantages of 802.11b is that the frequency band is crowded, and subject to interference from other networking technologies, microwave ovens, 2.4GHz cordless phones (a huge market), and Bluetooth. There are drawbacks to 802.11b, including lack of interoperability with voice devices, and no QoS provisions for multimedia content. Interference and other limitations aside, 802.11b is the clear leader in business and institutional wireless networking and is gaining share for home applications as well.

c. 802.11a: 802.11a, which has just started to ship into the market, is much faster than 802.11b. An added advantage to 802.11a keeping aside its high data rates is that it isn't subject to interference from Bluetooth or any of the other 2.4GHz frequency users. One big disadvantage is that it is not directly compatible with 802.11b, and requires new bridging products that can support both types of networks. Other clear disadvantages are that 802.11a is only available in half the bandwidth in Japan (for a maximum of four channels), and it isn't approved for use in Europe, where HiperLAN2 is the standard.

d. 802.11g: An obvious advantage of 802.11g [7] is that it offers faster data rates comparable with 802.11a (at least on paper, since working silicon isn't available) and maintains compatibility with 802.11b (and 802.11b's worldwide acceptance). The standard operates entirely in the 2.4GHz frequency, but uses a minimum of two modes (both mandatory) with two optional modes. The mandatory modulation/access modes are the same CCK (Complementary Code Keying) mode used by 802.11b (hence the compatibility with Wi-Fi) and the OFDM (Orthogonal Frequency Division Multiplexing) mode used by 802.11a (but in this case in the 2.4GHz frequency band). Another disadvantage of 802.11g is that the 2.4GHz frequency will get even more crowded.

At first look 802.11g, which operates in the 2.4GHz frequency with mandatory compatibility with 802.11b but with a maximum data rate of 54Mbps, would be an obvious step in the race to improve wireless networking performance while maintaining compatibility with Wi-Fi, but there's more to the story. 802.11g also gives up roughly one year to 802.11a--products for the latter are already beginning to reach the market, although many products (those based on chipsets from companies other than Atheros) won't be out until mid year.

OFDM – Orthogonal Frequency Division Multiplexing, an FDM modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions.

5 Conclusion: "Is Winner Emerging?"

A number of Wireless LAN standards are discussed above and researchers propose each of these LAN standards for deployment enlisting the pitfalls of others. With the analysis of different existing wireless LAN technologies discussed earlier, this section proposes the best feasible solution after analyzing quantitatively various LAN technologies. **Bluetooth is inadequate for serious, security-sensitive work, and it lacks the strength required for a wireless extension to an enterprise or public network.** Technologies like IEEE 802.11 are the better choice for corporate LANs (and perhaps WAN connectivity with future improvements of the standards) while Bluetooth technology will be the better option for connectivity between computers and small PDAs, digital cameras, mobile phones and the like. Thus, **Bluetooth and IEEE 802.11, HomeRF are complementary, rather than competing, technologies**. Some analysts believe Bluetooth communication will be widely used for very small, short range computer networks, especially ad-hoc networks involving mobile devices.

With final ratification of the 802.11g wireless standard delayed until spring 2003, researchers are interested in dual-mode access points that let users enjoy Wi-Fi compatibility and higher speeds today. These solutions let companies migrate to the high-speed 802.11a wireless technology (rated at 54 Mbps) while maintaining compatibility with prevalent, affordable 802.11b products.

In the early quarter of this year, 802.11a products had started shipping into the market and researchers have come out with some concrete results with these devices. Two different set of tests were conducted. With the initial 802.11a access point and adapter starting to trickle to market, a set of tests with two different access points of 802.11a and 802.11b with their respective clients is conducted. At near and moderate distances, 802.11a is found to be 3.3 to 4.1 times faster than 802.11b as measured by file transfer times in both adhoc and infrastructure modes. 802.11a technology is still too new to make blanket statements about the differences in speed or range performance. In the benchmark tests conducted, when wireless networked PCs were within range of an access point, 802.11a wireless components were faster than 802.11b devices, but 802.11b found to have greater effective range than 802.11a. Ample bandwidth for streaming video, and avoidance of interference from microwave ovens and 2.4GHz phones should be sufficient reason for home users in particular to adopt 802.11a as the wireless network of choice. With the dual-mode access points available during early fall of this year, a preliminary set of tests were conducted with these access points. The best news is that all of these products worked as promised, letting users connect to the network via a variety of 802.11a and 802.11b adapters.

Widespread adoption of 802.11a isn't expected until dual mode access points for both 802.11b and 802.11a are available (so companies don't have to toss out capital-based equipment that was in all cases relatively recently purchased). The obvious parallel to 10Mbps and 100Mbps Ethernet makes the point that the faster standard didn't take off until 10/100Mbps components were available - the same may happen with 802.11a and/or 802.11g.

References

General:

[1] IEEE 802.11Working Group. **http://grouper.ieee.org/groups/802/11/index.html**.

[2] "*Wireless Networking Choices for the Broadband Internet Home*", **White Paper**, 2001. www.homerf.org

[3] **"**802.11a: A Very-High-Speed, Highly Scalable Wireless LAN Standard", **White Paper**, 2002, www.proxim.com

[4] "Why HiperLAN2**"**, White Paper – **HiperLAN2 Global Forum**.

[5] "A Comparison of HIPERLAN/2 and IEEE 802.11a", White Paper - 2001.

[6] "Bluetooth Specification", White Paper – Bluetooth Special Interests Group (SIG)

[7] www.intersil.com and www.ti.com for information on IEEE 802.11g.

Security:

[8] W. A. Arbaugh, '*An inductive chosen plaintext attack against WEP/WEP2*' **IEEE Document 802.11-01/230**, May 2001.

[9] W. A. Arbaugh, N. Shankar, and Y. J. Wan.'*Your 802.11wireless network has no clothes*'. **http://www.cs.umd.edu/~waa/wireless.pdf**, Mar. 2001.

[10] Brian P. Crow, Indra Widjaja, Jeong Geun Kim, P. T. Sakai, "*IEEE 802.11 Wireless Local Area Networks*", **IEEE Communications Magazine** , Sept. 1997

[11] N. Borisov, I. Goldberg, and D. Wagner, "*Intercepting Mobile Communications: The Insecurity of 802.11.*" **http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html**

[12] White Paper on "Bluetooth Security", Bluetooth Special Interests Group