

# Modern Wireless Technologies for Office and Home Networking

by

Maria Nikolitsa ([mnikoli@stanford.edu](mailto:mnikoli@stanford.edu))

Ioannis Papadimitriou ([jpg@stanford.edu](mailto:jpg@stanford.edu))

## **Abstract:**

*Recent breakthroughs in wireless technologies are changing the way people are acting and behaving while at work or at home. For the first time, it is feasible to exchange data, audio and video over broadband wireless channels, enabling the consumer to use a great number of applications with different performance requirements.*

*In this project, we are describing and comparing the standards that will dominate the office and home networking industry in the following years. Their popularity is based on the fact that they all operate in unlicensed frequency bands. We divide these protocols into two areas. The first one (presented by Maria) contains **Bluetooth** and **IEEE 802.11b**, which facilitate the exchange of relatively low-rate personal information between consumer electronic devices, such as PDAs, laptops, cell phones and printers. The second part (presented by Ioannis) is about **IEEE 802.11a** and **HiperLAN/2**, which are able to service high-demanding data and multimedia applications. There is another standard, called **HomeRF**, which is designed exclusively for home networking and it can be placed between these two areas, as its technical characteristics are closer to those of standards of the first area, but can also support applications targeted by standards of the second area. Therefore, it will be treated by both of us while comparing the standards.*

*After a brief description of the standards mentioned above, we focus on comparing them with respect to several aspects: range performance, system capacity, bandwidth sharing techniques, power control, topologies, interference immunity, Quality of Service (QoS), maximum mobility, scalability, security. We explore the tradeoffs that make one better than another under different application requirements and working environments. We finally investigate the important role that cost and market practices can play in determining the standard or standards that will dominate the exponentially growing area of enterprise and home wireless networking.*

## Table of Contents

1.	Bluetooth - IEEE 802.11b .....	3
1.1	Introduction to Bluetooth - Technical features .....	3
1.2	Bluetooth Architecture and Protocols .....	4
1.2.1	Radio .....	4
1.2.2	Baseband .....	5
1.2.3	Link Management Protocol (LMP).....	5
1.2.4	Host Controller Interface (HCI).....	6
1.2.5	Logical Link Control and Adaptation Protocol (L2CAP).....	6
1.2.6	Middleware Protocols .....	6
1.2.7	Applications Protocols .....	6
1.3	IEEE 802.11b - Architecture .....	6
1.3.1	Physical Layer .....	7
1.3.2	Media Access Control (MAC) .....	7
1.4	Comparison between Bluetooth and 802.11b .....	7
1.5	Applications of Bluetooth and 802.11b .....	8
1.6	Co-existence of Bluetooth and 802.11b .....	9
2.	HomeRF .....	10
2.1	Technical Description .....	10
2.2	Comparison of HomeRF, Bluetooth and IEEE 802.11b .....	11
3.	High-rate Wireless LANs.....	12
3.1	HiperLAN/2.....	12
3.2	IEEE 802.11a .....	14
3.3	Technical Comparison .....	14
3.3.1	Physical Layer .....	15
3.3.2	Throughput.....	15
3.3.3	Range Performance.....	15
3.3.4	Quality of Service (QoS).....	16
3.3.5	Security .....	16
3.3.6	Interference Immunity.....	16
3.3.7	Topologies.....	17
3.3.8	Power Control .....	17
3.3.9	Mobility.....	17
3.4	Market Issues: who is going to win? .....	17
4.	Conclusions.....	18
5.	References .....	19

## 1. Bluetooth - IEEE 802.11b

During the last years, we observe the continuous and spectacular evolution of wireless communications, which support a great range of applications. Traditionally, the human mind considers wireless communications to be used only in outdoor environment, such as cellular or microwave radio communications systems. But, in last decade, there is a remarkable growth in wireless local area networking which can be attributed to the IEEE802.11b standard. The evolution of radio frequency technology led the research effort to concentrate on the development of pico-networks supporting short-range ad hoc wireless communications. Bluetooth standard emerged from this effort. This part of the survey presents an overview of Bluetooth and IEEE802.11b standards - description of topology, architecture and other technical attributes. This part of the paper presents an overview of Bluetooth and IEEE802.11b standards - description of topology, architecture and other technical attributes and it attempts a comparison between them by presenting their merits and limitations, various scenarios of their use proving these new RF technologies will be a breakthrough which will impact tremendously the way we lead our lives and run our businesses in order to conclude that a unified approach of these two standards can provide an alternative solution to wireline LANs.

### 1.1 Introduction to Bluetooth - Technical features

Bluetooth was invented in 1994 by M.L Ericsson and it was named after the Danish king Harald Båtand (Bluetooth) 940-981A.D who managed to unite the Scandinavian people. Similarly, the Bluetooth technology has as a goal to unite communications and computing devices. Bluetooth, which started as a temporary name, became a permanent one.



Figure 1: King Harald Bluetooth with laptop and mobile phone  
(<http://news.bbc.co.uk/1/hi/sci/tech/787891.stm>)

The wide spread of Bluetooth technology is promoted by the Special Interest Group (SIG) which was originally founded by Ericsson, IBM, Intel, Nokia and Toshiba in 1998. Their aim was to develop the intellectual property of the Bluetooth specification that is available to adopter members when they launch products in the market. Today, about 2,500 adopter members have joined SIG.

According to the specification developed by SIG for this new RF technology, Bluetooth is defined as a method for data and voice transfer between communications devices and PCs in a wireless medium using short-range, low-power radio links. It can also include home appliances. The devices operate in the unlicensed 2.4GHz industrial, scientific and medical band (ISM). As a great number of devices operate in this band, such as microwaves, baby monitors and garage openers, Bluetooth technology uses a fast frequency-hopping, spread-spectrum (FHSS) technique - 1600 hops/sec in order to avoid interference and operate reliably

with the other devices. In most of the countries around the world, the ISM frequency spectrum is allocated into 79 1-MHz hop channels. The modulation technique in use is the Gaussian frequency shift-keying (GFSK). Bluetooth radios consist of three power classes - class 1, 2 and 3 which have transmit power equal to 20, 4 and 0 dBm respectively. The average range of coverage is 10m which can extend up to 100m by increasing the transmit power to 20dBm. The Bluetooth technology can support the transmission of both voice and data. Actually, it can support one point-to-multipoint asynchronous-connectionless link (ACL) for data transmission with data rate 723.2 kbps and a return link of 57.6kbps and up to three point-to-point synchronous connection-oriented links for mostly voice transmission with 64kbps in each direction.

## 1.2 Bluetooth Architecture and Protocols

The Bluetooth specification supports a protocol hierarchy as it is depicted in the next figure, derived from [10], which consists of three categories: the transport protocols, the middleware protocols and the applications/profiles. The protocols can also be grouped in the following categories: the core protocols (Baseband, LMP, HCI, L2CAP, SDP), which are protocols exclusively developed for the needs of Bluetooth technology, the adopted protocols (RFCOMM, TCS), which are developed for Bluetooth based on existing protocols and the applications protocols (WAP, UDP, TCP, IP, PPP, SDP, TCS) which are closer to the user. These groupings are done according to [10], [1] respectively and are not defined by the specification.

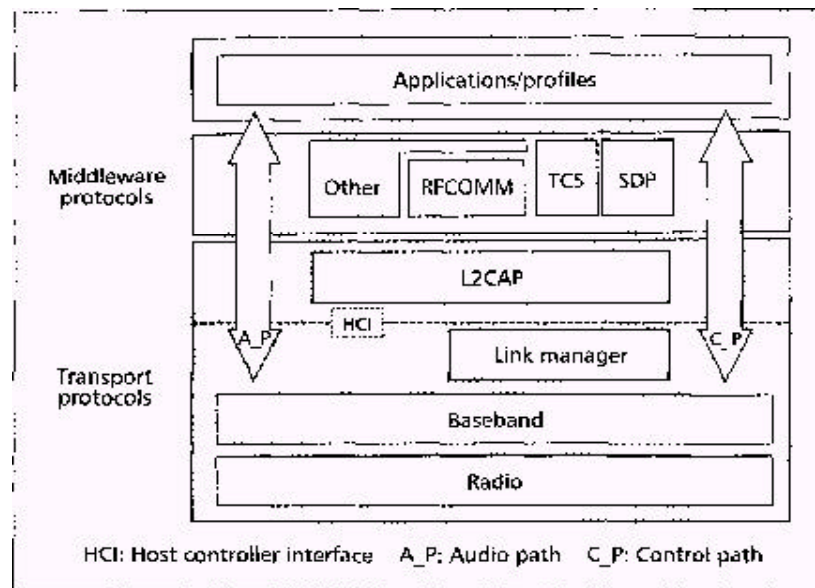


Figure 2: Stack of Bluetooth protocols

### 1.2.1 Radio

The radio includes the description of the technical features of Bluetooth technology, such as its spread spectrum nature (FHSS), its modulation technique (GFSK), its transmission rate (~1.2Mbps) and its transmit power (0 or 4 or 20dBm). (These characteristics have been presented analytically in this survey under the subtitle “Introduction to Bluetooth - Technical features”).

## 1.2.2 Baseband

The baseband enables the creation of Bluetooth piconets, which allow the different devices to communicate with each other and the allocation of power resources among the various devices. It also controls the synchronization and the transmission frequency-hopping pattern.

### Network Topology

Bluetooth devices form in an ad hoc manner piconets, which consist of two to eight devices. A piconet consists of a single master device and up to seven slave devices, which communicate actively with the master. A Bluetooth device can operate both as a master and a slave at different time slots. In addition, more than one piconets can share the same device. This device can be a slave in both piconets or can serve as a master in one piconet and as a slave in the other. Thus, this device connects multiple piconets to form a scatternet, as it is shown in the next figure:

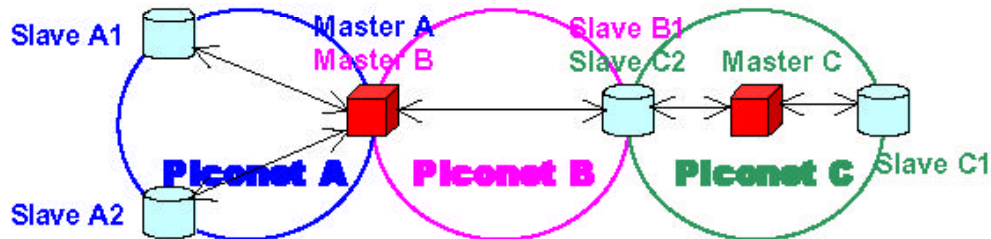


Figure 3: Piconets can be linked to form a scatternet  
(<http://kctechlogyinc.com/pdf/whitepaper.pdf>)

Apart from seven slave devices which can be active in a piconet, there are three more categories of slave devices which use lower power in comparison with the active units - the ones who are in sniff, hold and park mode. The sniff-state devices accept data from the master only at specific time slots and the rest of the time they sleep. The hold-state devices listen to the master and become active when they are said so. The parked devices are synchronized to the piconet by following the specific hopping pattern but they do not listen any more and they do not possess their active member address. As a result, they are not identified by the master any more.

In order to have a connection established between two devices, one device (the master) will start an inquiry process in order to find the devices in its vicinity and then it will continue with a paging process with another device (slave), in order to exchange information regarding the achievement of clock synchronization of the slave to the master's one and the frequency-hopping sequence. The two devices start exchanging data in a time-division-duplex (TDD) manner.

## 1.2.3 Link Management Protocol (LMP)

The LMP is responsible for the creation of the link between two units. It also handles the management of power modes, the authentication procedure by exchanging a link key of 128 bits which uses an initialization key (MAC address and PIN) and the encryption procedure by creating a key of 8-128 bits. Actually, Bluetooth can provide usage protection and information confidentiality. It supports three levels of security (non-secure, service-level and link-level) and two classes of devices (trusted, distrusted). Bluetooth uses two secret keys.

The Bluetooth technology is relatively secure, but it also seems to have a vulnerable side as the PIN and the keys can be obtained by an intruder.

### 1.2.4 Host Controller Interface (HCI)

The HCI provides a uniform interface method to access the hardware capabilities if Bluetooth located in the lower layers (Baseband and LMP).

### 1.2.5 Logical Link Control and Adaptation Protocol (L2CAP)

The L2CAP provides connection-oriented and connectionless data services to upper layers, by conducting the following operations: multiplexing (since a number of protocols can operate over it), segmentation and reassembly of data packets and quality of service exchange information between two Bluetooth units.

### 1.2.6 Middleware Protocols

This category of protocols consists of RFCOMM, TCS and SDP. RFCOMM protocol, which emulates a serial port, provides transport capabilities for upper layer services. TCS protocol provides the signaling for the establishment of calls. SDP defines how a Bluetooth device will act in order to discover services that another device might have.

### 1.2.7 Applications Protocols

Bluetooth provides services to a great number of higher layer standards in order to be able to support various applications, as it is a technology, which intends to eliminate the required technical knowledge of its users in order to enable them to use Bluetooth more easily.

More information about Bluetooth protocols can be found in [3], [7], [9] and [10].

## 1.3 IEEE 802.11b - Architecture

The IEEE 802.11b is a standard for wireless local area networks (WLAN), which operates in the license-free ISM band (2.4-2.4835GHz). By observing the next figure, derived from [17], it is obvious that the 802.11b changed the Physical and Data Link layers of the OSI model “Ethernet-like” services over a radio frequency. The rest of the layers remained the same. This fact contributes to the compatibility and interoperability between 802.11b and Ethernet. The 802.11 standard supports two kinds of networks: peer-to-peer and client/server networks.

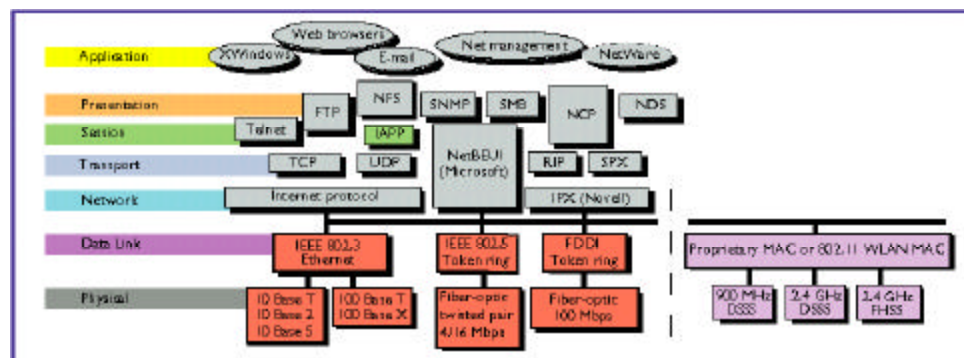


Figure 4: Wired protocols of the OSI model. 802.11b changed the physical and data link layers.

### 1.3.1 Physical Layer

The 802.11b specification provides data rates equal to 5.5 or 11Mbps and achieves these rates by using complementary code keying (CCK). In direct-sequence spread spectrum systems (DSSS), the modulation techniques of DBPSK or DQPSK are used respectively for these two data rates. Typical range of 802.11b is approximately 100m. The limits of radiated power are 1W for the USA, 10mW/1MHz in Europe and 10mW in Japan. The data rates are affected by the distance from the transmitter, the signal strength and quality.

### 1.3.2 Media Access Control (MAC)

This protocol, bearing a great similarity to wireline Ethernet 802.3, defines the use of carrier-sense multiple access with collision avoidance (CSMA/CA), which prevents collision of packets without providing any detection features. This access mechanism is called distributed coordination function (DCF). The collision of packets is avoided by measuring the energy of the received signal at the antenna and concluding that the channel is ready for transmission if that amount of energy is below a threshold. Another strategy for avoidance of collisions is to use the carrier sense in order to assess if the channel is clear for transmission by finding that the channel contains a signal of the same type as 802.11b (no other RF transmitters should exist in the channel as the channel is no longer clear for transmission). Another way to achieve minimum number of collisions is by exchanging request-to-send (RTS), clear-to-send (CTS), data and acknowledgement frames between the transmitting and the receiving stations. The CTS frame informs the transmitting station that it can start with the transmission and the other stations are informed to “back-off“ while the transmission takes place. A frequent problem of 802.11b is the one known as hidden-node. A node cannot detect that another node already transmits and it concludes that the channel is free for transmission. As for security, a Wired Equivalent Protocol (WEP) has been developed, which supports confidentiality, access control and message integrity. The 802.11b uses the RC4 algorithm and a 40/64 bits key for encryption, which makes it vulnerable to, attempts to break the code behind it as its length (<80 bits) implies little time to break [6].

More information about IEEE 802.11b can be derived from [1], [15], [17] and [18].

## 1.4 Comparison between Bluetooth and 802.11b

A comparison between these two wireless standards is essential in order to obtain an insight on their strong and weak points, figure out potential applications for each standard and conclude that the existence of both WPAN and WLAN is necessary as they target different applications which ameliorate the quality of human life. The differences between Bluetooth technology and IEEE 802.11b are presented below:

- The Bluetooth standard has now started to hit the market, while the 802.11b is very popular, as it exists more years and it has the advantage of being the first technology, which opened the market of wireless networks.
- The 802.11b is a wireless version of Ethernet and it is compatible with it. As a result, it can access very easily resources of LAN without any need of conversion. In addition, due to its networking characteristics, it presents complexity in use. For example, the 802.11b runs TCP/IP and the user is required to configure the peripheral devices. On the other hand, the Bluetooth technology supports point-to-point and point-to-multipoint communications. Two Bluetooth devices can very easily and simply communicate with each other without the need to configure hardware or drivers. Bluetooth can access a LAN by using a LAN access point.

In that case, Bluetooth will have to run TCP/IP or the LAN point should provide access conversion capabilities. But, if that is the case, Bluetooth defeats the objective of easy and simple use.

- The Bluetooth is an ad hoc network, which allows the transmission between two devices without the existence of infrastructure. On the other hand, 802.11b as it is a LAN networking on RF medium requires the existence of infrastructure, such as a RF transmitter in order to facilitate the exchange of data between two devices.
- As for architecture, the Bluetooth is a FHSS standard hopping in a different frequency with rate 1600hops/sec, while 802.11b is a DSSS wireless standard.
- As for range, the average one for Bluetooth is 10m - which can increase up to 100m accompanied by an increase in transmit power, while the IEEE802.11b has a greater average coverage area with radius of 305m in open areas, 76-122m in closed areas.
- The required transmit power for the Bluetooth is low (1-10-100mW), while the transmit power for 802.11b is high (for the USA up to 1W). This is a great advantage for Bluetooth as it has a longer battery life because of its low power consumption. In addition, due to its low power, Bluetooth chip needs less space and minimum complexity. As a result, Bluetooth becomes really cost-effective (approximately \$5 / module). The 802.11b has a much shorter battery life and a greater component cost (\$25). Actually, what increases the total cost of installing 802.11b is not only its module higher cost but also the use of access points.
- The bandwidth used by Bluetooth is 1Mbps (shared), while the bandwidth for 802.11b is equal to 11Mbps (shared). 802.11b is more attractive for use as a great number of applications require a high data rate. The effective bandwidth for Bluetooth is 700kbps (smaller than the bandwidth due to interference with other RF device equipment). As for 802.11b, its effective bandwidth ranges from 2 to 3Mbps (with WEP enabled). This decrease in bandwidth is due to the access technique (CSMA/CA), the interference with other devices and the increase in distance from the access point.
- As for security, Bluetooth is quite secure as it has a service-level or link-level authentication, but it also requires an encryption key of 128bits, which is extremely safe as, according to a rule of thumb, a key with length more than 80 bits is extremely difficult to break with brute force. On the other hand, 802.11b is not as safe as Bluetooth as the authentication enabled with WEP is easy to break and the encryption key of length 40/64 bits can be broken easily with brute force [6].
- As for error handling, Bluetooth applies an optional FEC, while IEEE 802.11b uses CRC-16 and CRC-32 with retransmissions.
- As for the number of devices, which can have access at the same time, Bluetooth supports eight, while 802.11b supports multiple.
- As for the quality of service, the Bluetooth technology has a mechanism of supporting it, while 802.11b does not provide it at all.
- The interoperability of 802.11b among different branches is considered to be good while the interoperability for the Bluetooth is predicted to be equally good.

More information about the comparison of these standards can be found in [1], [21], [22].

### **1.5 Applications of Bluetooth and 802.11b**

The above mentioned differences in specifications of Bluetooth and 802.11b, lead to different kinds of usage for these two wireless standards, in office and home environments.

The typical usage for Bluetooth is the replacement of the interconnect cabling between a great variety of devices, such as laptop computers, personal digital assistants, PDAs, PCs, digital cameras, MP-3 players, headsets, modems and other devices, providing short range interconnectivity, as it is shown in the figure below, derived from [9]:

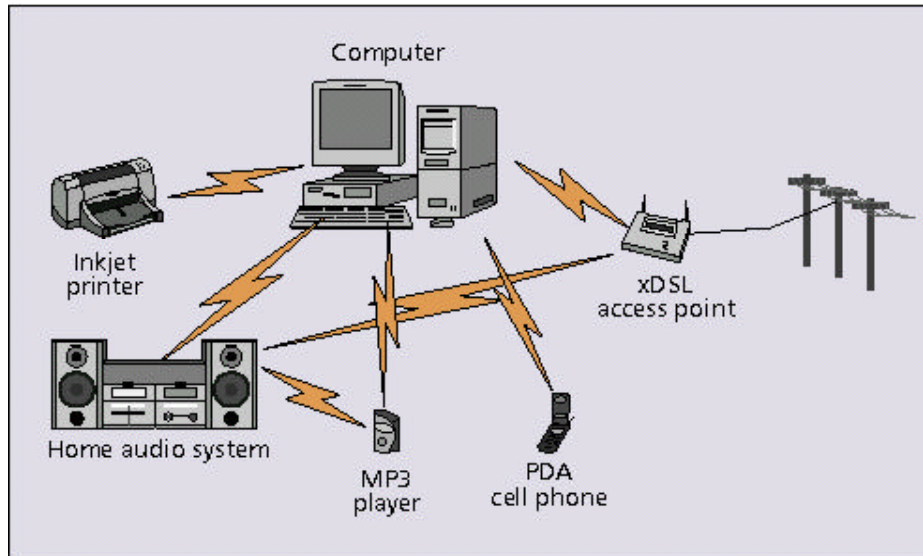


Figure 5: A Bluetooth network

PC and peripheral devices networking, hidden computing and data synchronization between devices are the main applications of the Bluetooth technology. In addition, Bluetooth is suitable for installation in low-power devices such as mobile phones and PDAs. Bluetooth enables the connection between phones and PDAs for exchange of data or the connection of PDAs to printers or even to fax machines. Moreover, Bluetooth provides hands-free units for phones, web browsing, e-mailing without attachments and generally applications where high bandwidth is not crucial. These applications can be used not only in an office environment, but also in home environment. In both cases, Bluetooth is appropriate to serve a small area (an office or a room). Another office-oriented application of Bluetooth is the support of a meeting between colleagues when they want to connect their laptops in an ad hoc manner and do not intend to use any infrastructure. Other application could include smart appliances, entertainment devices and heating systems in the home environment, but in that case Bluetooth should have evolved in a standard with greater reliability, supporting greater data rates and perhaps operating at a greater range.

The IEEE 802.11b can support applications with high bandwidth, reliability and great range. It can also support web browsing, e-mail of bulk files (with attachments) and file sharing, which make it really attractive for a business environment. Additionally, it is suitable in the corporate, campus, hotels, restaurants, coffee shops, shopping malls, warehouse and airports. As for the home environment, 802.11b can be a great networking solution as its range is such that it can cover the entire house and support data and audio applications. 802.11b can also support video, telemetry and control applications as long as it is accompanied by a QoS extension.

### 1.6 Co-existence of Bluetooth and 802.11b

In many cases, Bluetooth and 802.11b do not compete but actually they support complementary applications. As a result, a current research issue is the co-existence of these two technologies, which causes degradation of their performance due to the growing interference between them when they operate in the same environment. Recent studies and simulations [26] prove that the level of interference is moderate in some cases and in the future these two standards will be able to co-exist. By this remark, the vision of seamless

mobility and wireless interconnectivity seems to be close to reality. A bright future offering high living standards seems to be ahead of us!

## 2. HomeRF

### 2.1 *Technical Description*

The HomeRF Working Group is a consortium of companies that developed the Shared Wireless Access Protocol (SWAP), designed to service high-quality voice and high-rate data applications under a residential environment. More specifically, the standard enables the simultaneous support of three major application categories:

- (a) Up to 8 Toll-Quality Voice Connections, which are very sensitive in latency and jitter requirements and less demanding as far as bandwidth and error performance are concerned. HomeRF extends the DECT protocol, so that the connection to the PSTN is seamless.
- (b) Multiple Asynchronous applications, such as file/printer/internet sharing and alarm/security device controlling. Although the latency and jitter requirements are considerably relaxed here, there is a need for high data rate and low error rate.
- (c) Up to 8 prioritized streaming media sessions, such as audio/video streaming, which are demanding in both bandwidth and jitter.

Since all these applications are supported, the following sections compare HomeRF with Bluetooth/802.11b and 802.11a/HiperLAN2 standards within home. Before that, its basic features are described below.

There are four types of devices in a HomeRF network. The voice (isochronous) devices (called I-nodes) have functionality similar to a DECT headset. The asynchronous data devices (called A-nodes) send and receive data asynchronously (e.g. laptops or web-enabled devices). AI-nodes combine the functionality of I-nodes and A-nodes. Finally, a Connection Point device (CP) is connected to a personal computer (usually via USB) and acts as a gateway between the devices mentioned above, the PC and the PSTN. While I-nodes are always configured as a network managed by the Connection Point to ensure synchronization, low jitter and low latency, Anodes can be configured either as a managed network if they require power management and streaming services from the CP, or as a peer-to-peer network (without a CP) otherwise. These two types of configurations (managed and peer-to-peer) may exist in the same home simultaneously. To avoid multiple overlapping between two different SWAP networks, each network has its own 24-bit Network Identifier (NWID) and nodes are allowed to listen only to frames having the NWID of the network they participate in.

The HomeRF standard specifies the physical (PHY) and Media Access Control (MAC) OSI layers. As far as PHY layer specifications are concerned, SWAP operates in the unlicensed 2.4 GHz band. It uses the Frequency Hopping Spread Spectrum (FHSS) technology at 50 or 100 hops/sec. It provides up to 10Mbps peak raw data rate and is able to cover the whole home area even under hostile environment conditions. The transmitter power ranges between 100 and 250 mW.

What makes HomeRF an interesting standard is the fact that the MAC layer functionality depends on the type of data to be delivered. Following the DECT standard, voice traffic is serviced by the TDMA access mechanism. When it comes to data traffic, SWAP is based on the 802.11 and OpenAir standards and as a result provides a CSMA/CA service. Finally, in case that streaming sessions are established, SWAP provides a prioritized, connection-oriented service that decreases jitter. Bits are organized in MAC frames called superframes. There are two types of superframes. When there are no active voice connections, the

superframe lasts for 20 msec, the frequency hops every 20msec and only A-nodes are serviced through the CSMA/CA (contention based) data protocol. Nevertheless, when there are active voice connections, the MAC layer sends subframes of 10 msec and the frequency hops every 10msec to lower the latency and increase the interference immunity. Each subframe contains two Contention-Free-Periods (CFP1 and CFP2) based on the TDMA access mechanism and a Contention-Based-Period (CBP) based on the CSMA/CA protocol. CFP1 is used for the re-transmission of voice information that failed to be delivered successfully during the previous subframe. CFP2 is used for the transmission of new voice information.

As mentioned above, the Connection Point (CP) has the ability to store isochronous and asynchronous data in order to provide power management services to both the I-nodes and the A-nodes when the network is configured as a managed one. I-nodes, which are very sensitive about power consumption, have power-down periods even during an active voice call. A nodes also enter a power-saving mode and the signaling needed for interaction with these nodes depends on whether unicast or broadcast data are sent to them.

As far as Quality of Service (QoS) is concerned, HomeRF uses different protocols depending on what traffic flow is delivered. The highest priority is given to voice connections, since HomeRF uses frequency and time diversity, as well as hopset adaptation, to ensure that maximum delay is about 10msec. Additionally, the Priority Asynchronous Data Service assigns to each streaming flow a unique number, in order to remove the possibility of collision during the contention-based period of the MAC frame. This scheme ensures that stream packets have maximum delay of about 30msec. More information about HomeRF QoS can be found in [38].

When it comes to security, the major issues to be faced by a wireless protocol are Data Compromise, Unauthorized Access and Denial of Service Attacks. HomeRF uses a 128-bit encryption scheme and a 32-bit Initialization Vector with defined management in order to make data compromise difficult. Frequency hopping, in conjunction with the requirement for a secret Network Identifier, is used against unauthorized access. Finally, denial-of-service attacks are very difficult because of the Frequency Hopping Spread Spectrum technology. In [39], security issues and solutions given by HomeRF are described.

More details on how HomeRF works can be found in [34], [35] and [36]. Paper [37] describes the techniques used to accomplish interference immunity.

## **2.2 Comparison of HomeRF, Bluetooth and IEEE 802.11b**

HomeRF, Bluetooth and 802.11b are standards with different technical attributes, which are compared for the case of operation in home environment:

- -As for the architecture, HomeRF uses a FHSS scheme at 50 hops/sec, while Bluetooth uses FHSS at 1600 hops/sec and IEEE 802.11b deploys a DSSS scheme. In addition, HomeRF can support simultaneously host/client and peer-to-peer network topology, while 802.11b can support them both but not at the same time and Bluetooth has a point-to-multipoint topology.
- As for the cost, HomeRF and Bluetooth are more cost-effective as both of them use fewer RF semiconductor chips and passive components than 802.11b as a result of their lower complexity. The lower complexity of HomeRF and Bluetooth reduces the size of the printed circuit board and makes them fit in light and personal devices at home. This is not the case for 802.11b, which uses a PC Card. As a result, it is expected that HomeRF and Bluetooth will have their modules built-in to several appliances.

- As for the range, HomeRF and 802.11b are in an advantageous position as with ranges over 50m (under adverse conditions) can provide coverage to the entire house. On the other hand, Bluetooth has an adequate range for home coverage equal to 100m when its power increases to 100mW. But, Bluetooth is expected to be installed in low-power devices and provide single room coverage.
- As for the power consumption, Bluetooth and HomeRF have a clear advantage in comparison with 802.11b, as they consume lower power than 802.11b especially when they are mainly in the standby mode.
- As for the data throughput, HomeRF and 802.11b are in an advantageous position as they demonstrate peak data rates of 10Mbps, which are much higher than the Bluetooth data rate.
- As for the support of streaming media, HomeRF provides it by using prioritized sessions. Bluetooth cannot provide it due to its restricted bandwidth and 802.11b handles the case of simultaneous appearance of data traffic unpredictably.
- As for the voice support, both HomeRF and Bluetooth have voice services. HomeRF has the advantage of a standardized interoperable call stack with DECT features and interference mitigation for packet losses. 802.11b offers a poor support of voice services.
- As for the scalability of these three standards regarding high density residential applications, HomeRF and Bluetooth due to their FHSS scheme have more independent channels, while 802.11b has only three channels.
- As for security, HomeRF is more secure than the other two wireless standards.

More analytical information regarding this comparison is presented in [36], [37] and [39].

### 3. High-rate Wireless LANs

In this chapter, we are looking at Wireless LAN standards, which provide high-data rates and are therefore capable of supporting demanding applications, such as streaming video/audio and High Definition Television (HDTV). Products of this category have very recently appeared in the market, which means that there is still much room for innovation and research in this area.

At the moment, the competing standards for home and office use are HiperLAN/2 (although there are no products in the market yet) and IEEE 802.11a. HomeRF also competes as far as residential environments are concerned. The basic features of HiperLAN/2 and IEEE 802.11a are described below. Next, a technical comparison of these 3 standards in 9 different categories is presented. Furthermore, we discuss some economic issues, which we believe that are going to play a major role in determining the standard that will dominate this area.

#### 3.1 *HiperLAN/2*

High Performance Radio Local Area Network - type 2 (HIPERLAN/2), defined by the European Telecommunication Standardization Institute (ETSI), is one of the wireless technologies that support high data rates and Quality of Service (QoS) in the 5GHz band. In contrast to HomeRF, which is intended for home use only, this standard can work under various environments: at home, at the office, indoors, outdoors.

A HiperLAN/2 wireless network contains two types of devices: Mobile Terminals (MT) and Access Points (AP). The preferred topology for office environments is centralized (like a cell) with one AP servicing several MT's. In this mode, if more than one AP's are needed to cover a wide area, they are connected through a fixed network (e.g. Ethernet LAN). In the direct mode of operation (preferred for home environments) the MT's automatically configure themselves in a peer-to-peer (ad hoc) network and one of them plays the role of the AP to control the allocation of resources.

The standard specifications describe three layers, namely the Physical layer (PHY), the Data Link Control layer (DLC) and the Convergence layer. The following figure, derived from [28], depicts these layers as well as their sublayers:

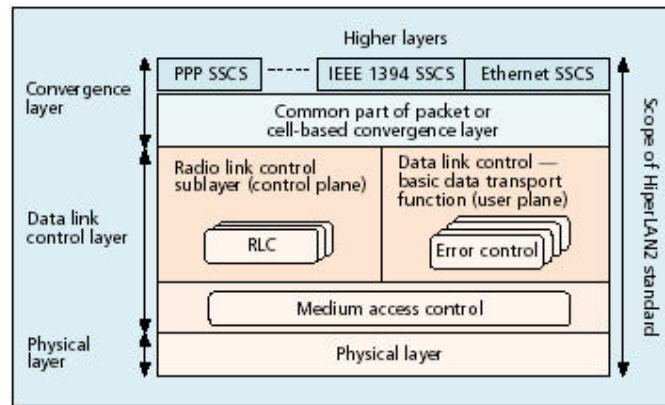


Figure 6: HiperLAN/2 protocol architecture

The Convergence layer acts as an abstraction between the HiperLAN/2 Data Link Control (DLC) layer and higher layers implementing different networks/protocols. In this way, DLC and PHY become core-network independent. Its main functionality is to convert the higher-layer packets into HiperLAN/2 DLC SDUs through padding, segmentation and reassembly. Packet-based convergence layers are used with Service-Specific Convergence Sublayers (SSCS) when the higher protocols have packets of different sizes (e.g. Ethernet). Cell-based convergence layers are used with SSCS's when higher protocols have fixed-size packets (e.g. ATM).

The Data Link Control (DLC) layer contains the Radio Link Control, the Error Control and the Media Access Control sublayers. When a connection between an AP and a MT is about to be established, their **Radio Link Control (RLC)** sublayers exchange signaling messages pertaining to authentication, association/de-association, link capabilities, encryption, handover, dynamic frequency selection, MT alive, power control and setup/release/modification of unicast/multicast/broadcast user-connections. The **Error Control (EC)** sublayer determines the reliability of user connections. There are three modes: the acknowledged mode provides highly-reliable user connections through acknowledgments; the repetition mode ensures reliability through repetition of user PDUs but no acknowledgements are exchanged; the unacknowledged mode is an unreliable (but low-latency) type of transmission. The **Media Access Control (MAC)** sublayer uses a TDMA/TDD access scheme. The MAC frame lasts 2 msec (fixed-size) and contains 4 phases. During the broadcast phase, the AP sends to all associated MTs information such as transmission power levels, network identifiers, resource allocation and previous access attempts results. The downlink and uplink phases are used for transmission of data and control information between the AP and the MT in both directions. Finally, the random access phase is used by the MT's to request resources (i.e. capacity) from the closer AP.

The Physical layer uses Orthogonal Frequency-Division Multiplexing (OFDM) to compensate against intersymbol and co-channel interference. Each channel is 20MHz wide and contains 52 subcarriers (48 for data and 4 for pilots). HiperLAN/2 uses link adaptation, i.e. supports different code rates and modulation schemes in order to adapt to the current transmission conditions. The maximum data rate that can be provided is 54Mbps when 64QAM modulation is used.

As far as Quality of Service is concerned, the standard is connection-oriented. This means that a MT can request multiple DLC connections, each with unique QoS demands provided by the AP.

Finally, HiperLAN/2 defines a number of vendor-specific radio functions, such as dynamic frequency selection (for avoidance of interfered frequencies when AP's determine their frequency of operation), link adaptation, multi-beam antennas (to increase the signal-to-interference ratio), user mobility (which needs support of handovers initiated by the MT's) and power control (to save MT battery and to reduce interference). More information about HiperLAN/2 performance and MAC frame structure can be found in [27], [28] and [32].

### **3.2 IEEE 802.11a**

The most popular standard supporting high rate wireless communications today is IEEE 802.11a, which is actually an extension of the IEEE 802.11b described above. Consequently, in this chapter, we do not present the details of 802.11a, instead we focus on the main differences between 802.11a and 802.11b.

More specifically, the two standards share the same MAC layer functionality. This means that what makes 802.11a quicker than 802.11b is due to its physical layer characteristics. First of all, 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM) and not Direct Sequence Spread Spectrum (DSSS) as its modulation scheme. OFDM is better than DSSS as far as spectrum efficiency and intersymbol interference are concerned, but costs more (because multiple modulators/demodulators are needed) and consumes more power.

802.11a operates in the unlicensed 5GHz range, which is less crowded than the 2.4GHz range, where 802.11b, Bluetooth, HomeRF and microwave ovens operate. Hence, interference is reduced but 802.11a and 802.11b are not interoperable and signals in the 5GHz range have a higher absorption rate from walls and other obstacles. Additionally, the available bandwidth for 802.11a in the U.S. is 300 MHz (83.5MHz for 802.11b), which means that at maximum 12 non-overlapping channels can be allotted for an 802.11a network (3 channels for 802.11b).

As a result of the modulation scheme and the increased bandwidth, the maximum raw data rate supported by 802.11a is 54Mbps for a maximum range of 50 meters, while 802.11b provides 11Mbps for a distance of 100 meters. This means that in order to cover a specific area, more Access Points (AP) will be needed, thus increasing the cost. Obviously, there is a trade-off between data rate, range and cost. In [14], actual measurements show that 802.11a and 802.11b have the same range up to 225 feet in an office environment with only one cell, but 802.11a delivers 2 to 4.5 more throughput. In a system of 8 cells under the same environment, the system capacity of 802.11a is 8 times greater than that of 802.11b. Hence, additional cost due to deployment of more AP's is compensated by the much higher throughput supported by 802.11a.

More information about the 802.11a standard and its differences from 802.11b can be found in [12], [13], [14], [19].

### **3.3 Technical Comparison**

In this section, IEEE 802.11a, HiperLAN/2 and HomeRF are compared from a technical point of view in many different categories. The first two standards can be deployed at the office and at home, while HomeRF only at home. Hence, any comparison between HomeRF and the other two standards is restricted to residential environments.

The following paragraphs also show that there are a lot of tradeoffs that make one implementation sometimes better than the others under specific conditions and requirements and sometimes inferior to the others when the environment changes. Additionally, it must be pointed out that technical superiority does not always mean market success, as discussed in the next section.

### **3.3.1 Physical Layer**

What differentiates IEEE 802.11a from HiperLAN/2 is mainly their MAC layer functionality, since the physical layers are almost the same. They both operate in the 5GHz band, use OFDM to mitigate ISI and allocate 20Mhz per frequency channel. They also modulate the signal by choosing among BPSK, QPSK, 16-QAM and 64-QAM, although there are some differences in the codes associated with these modulation schemes. The maximum raw data rate is 54 Mbps. The standards differ in the scrambler initialization and the preamble training sequence used for time and frequency synchronization.

On the other hand, HomeRF works in the 2.4 GHz band. This means that the signal passes easier through walls and other obstacles, but gets more interfered by other devices operating in the same crowded band (Bluetooth, IEEE 802.11b, microwave ovens). The maximum raw data rate is 10Mbps and uses Frequency Hopping Spread Spectrum (FHSS) to reduce ISI and narrowband interference.

### **3.3.2 Throughput**

Probably the most important performance metric of a wireless system is throughput, i.e. the maximum effective user data rate. It is different from the raw data rate because it depends not only on the physical layer but also on the MAC layer implementation.

Analytical calculations and simulations in [30], [31] and [32] agree that HiperLAN/2 provides higher user data rate than IEEE 802.11a, although the raw rate is 54Mbps for both of them. What differentiates them is mainly the packet size. Although both standards have the same BER (which is independent of the frame length), the PER drops as the packet size increases. Simulations in [30] show that as the IEEE 802.11a MAC frame gets longer, the efficiency increases (because more payload bytes are included in the frame), but higher transmission power is needed to keep the same PER, otherwise a lower-rate modulation must be chosen. Since there are specific limits for transmission power, IEEE 802.11a is driven to lower data rates. Furthermore, authors of [31] analytically derive a better throughput for HiperLAN/2 with respect to 802.11a and conclude that the relative throughput of the former is independent of the PHY mode (i.e. the raw data rate chosen by the link adaptation module), while the relative throughput of the latter depends on the PHY mode (due to the fact that the waiting time for sensing the carrier is always the same, no matter what the raw data rate is).

HomeRF provides only 10 Mbps raw data rate, which leads to approximately 5Mbps of peak TCP/IP throughput. Although this is adequate for most contemporary home applications, it is expected to be a severe constraint for most future residential needs, especially when applications such as video streaming and High-Definition Television (HDTV) become popular.

### **3.3.3 Range Performance**

The higher throughput provided by IEEE802.11a and HiperLAN/2 is not for free; it is compensated for reduced range. For example, both standards operate at 54 Mbps for distances up to 50 meters, in contrast to IEEE 802.11b, which operates at peak rate for at least 100 meters. This means that more Access Points (AP's) will be needed to cover a specific relatively large area, thus increasing the total cost required for office and public use.

Nevertheless, this range is usually enough for deploying a one-cell network (only one AP) at home. Hence, range does not give a clear advantage to HomeRF, which provides peak rate up to more than 100 meters and therefore requires only one Connection Point (CP).

### **3.3.4 Quality of Service (QoS)**

Standards such as IEEE 802.11a, HiperLAN/2 and HomeRF have been specified in order to support a variety of applications with diverse and often conflicting requirements. Voice is low rate demanding but is synchronous and therefore has very tight delay and jitter constraints. Most data applications need much more bandwidth but delays are not of major importance. Finally, during the last years, streaming applications are becoming more and more popular and demand quite high bandwidth and low delays. Hence, it is crucial for contemporary networks to provide Quality of Service (QoS).

To meet these requirements and to provide contention-free services, IEEE 802.11a has specified the Point Coordination Function (PCF), which gives high priority to a Point Coordinator (usually an AP) in order to poll other devices for data. Nevertheless, the point coordinator must contend with the other devices to gain access at the beginning [36]. The standard usually provides good QoS because of its bandwidth, but has a lot of problems when there are a lot of high-rate users. Hence, IEEE 802.11a QoS mechanism is not considered to be adequate and therefore IEEE has started the 802.11e group to deal with these issues.

HiperLAN/2 uses TDMA/TDD as the access method and establishes connection-oriented links. The allocation of resources is centralized and dynamic. In [31], several simulation scenarios containing asynchronous and synchronous flows show that although IEEE 802.11a and HiperLAN/2 give almost the same average delays, HiperLAN/2 provides higher data rates and less variant delays. Furthermore, simulations in [32] show that IEEE 802.11a does not perform well with real-time data.

HomeRF also provides QoS and uses different methods depending on what type of data is transmitted. Voice flows have the highest priority and the frame length decreases to ensure low maximum delay. If some voice packets get blocked, they are retransmitted during the following frame. Streaming flows are also prioritized in relation to data flows. Therefore, HomeRF provides good QoS, especially for voice applications since it has incorporated most of the DECT functionality [38].

### **3.3.5 Security**

Security in wireless communications has always been a critical issue (especially in corporate environments), since they are more vulnerable than wired communications. The standards under discussion have taken different ways to address this matter. IEEE 802.11a, based on the Wired Equivalent Privacy (WEP) protocol, has the most significant problems since it only provides one-way authentication and uses 40-bit keys. As a result, the IEEE 802.11i group is specifying new mechanisms to enhance security and authentication. The details pertaining to the security properties of each standard can be found in [20] for IEEE 802.11a, in [27] for HiperLAN/2 and in [39] for HomeRF).

### **3.3.6 Interference Immunity**

All standards take special care as far as interference immunity is concerned. IEEE 802.11a uses link adaptation and the listen-talk property of the CSMA/CA access method [30], [32]. HiperLAN/2 uses Dynamic Frequency Selection (DFS), power control and link adaptation for the same reason [30]. Finally, HomeRF uses frequency hopping and ensures that two adjacent hops will not get both interfered. It also uses hopping adaptation, to mitigate the impact from static interferers such as micro ovens. For voice flows, the frame duration reduces to half and unsuccessfully delivered voice packets get retried within the next frame [37].

### 3.3.7 Topologies

All three standards support client-server (centralized) and peer-to-peer (ad hoc) networking. Client-server topologies need the use of a special device, called 'Access Point (AP)' in IEEE 802.11a and HiperLAN/2 specifications and 'Connection Point (CP)' in HomeRF specifications. It is responsible for the network management and its functionality differs depending on the standard. When it comes to ad-hoc networking, 802.11a is more suitable because it uses CSMA/CA (instead of TDMA/TDD), which is inherently decentralized [30].

### 3.3.8 Power Control

Power control algorithms are used in order to lower the power consumption of mobile devices (stand-by or battery-safe mode) and to reduce the interference between devices operating at the same frequency, when there are multiple cell-like wireless networks deployed in the same area. IEEE 802.11a does not support this service. HiperLAN/2 specifications describe the requirements concerning power control, although the actual implementation and the choice of power-level measurements to be exchanged between AP's and MT's are vendor-specific. As a result, simulations in [32] show that the average terminal transmission power is significantly lower in HiperLAN/2 than in IEEE 802.11a. Finally, when HomeRF operates as a client-server network, the Connection Point provides power control services to Inodes and Anodes, so that these nodes can enter a power-saving mode.

### 3.3.9 Mobility

These standards support pedestrian mobility. Since HiperLAN and 802.11 can be deployed over relatively large areas (e.g. campus or company buildings), handover mechanisms have been specified. On the other hand, HomeRF, being designed exclusively for residential environments, does not need to support handover.

## 3.4 Market Issues: who is going to win?

Following the technical discussion of the previous sections, a number of questions are natural to be posed. The target of this section is to try to predict what will happen in the years to come, based on the evidence we have nowadays.

One question is whether we will have only one standard for both office and home networking or people will use one protocol at work and another at home. Given the HomeRF paradigm, it seems that the first alternative is more likely to happen. From the technical description above, it is obvious that during the previous years when data rates were still low, HomeRF was superior to the other standards for home use, mainly because of its QoS and DECT support. In April 2000, HomeRF products represented more than 90% of the sales. This figure dropped below 30% for 2001 and forecasts argue that these numbers will continue to drop, as 802.11 products are getting more popular. Two are the main reasons for this change:

- People do not want to have two different configurations/line cards on their laptops. Since IEEE 802.11 currently dominates the corporate environment, it is more convenient for the user to have the same technology at home too.
- Economic issues have led great companies to support the IEEE 802.11 standards. Intel for example was one of the HomeRF founding companies. Nevertheless, in March 2001 people at Intel predicted that it would be economically better for the company to support one technology instead of two and since IEEE 802.11 was working well for corporate use, they decided to support the 802.11 groups. Intel recently announced its intention to invest \$150 million in 802.11 technologies.

It becomes clear that, although the HomeRF Group is trying to improve the standard as far as peak rates are concerned, it is highly likely that its role will continue to decrease in the following years. This means that the competition in high-rate applications for office and home

use will be between the IEEE 802.11 group and the HiperLAN/2 Forum. Issues to be considered are the following:

- HiperLAN/2 MAC layer is technically superior to the 802.11a MAC layer. What differentiates them is mainly data throughput, QoS and security. Having realized that, the IEEE has established the 802.11i and 802.11e task groups in order to improve the MAC layer security and QoS respectively. So, it is expected that the two standards will provide similar services in the future.
- HiperLAN/2 Forum had serious problems with the MAC layer implementation due to its complexity. Although the specifications have been finalized, there are no products in the market yet. This means that before HiperLAN/2 products start selling, the 802.11 products will have already dominated the market. Since the two standards are not interoperable, it is likely for most companies that have already bought 802.11 products to keep on with the same technology.
- Another issue is cost. Nowadays, 802.11a Access Points can be bought in the \$150-\$250 range. Additionally, the price for network cards attached to PCs and laptops has dropped close to \$100. On the other hand, the first HiperLAN/2 products are expected to be more expensive, due to increased MAC layer complexity and to low number of sales (economy of scales).
- IEEE 802.11a standard has problems in penetrating the European market, since it is still banned by the European Telecommunication Standards Institute (ETSI), as it does not meet the strict European requirements. Although at least one company has already taken license to ship its 802.11a products in Europe, the problem is going to be resolved in mid-2003 when the first IEEE 802.11f products will get to market. This standard is similar to IEEE 802.11a, but adds transmission power control and Dynamic Frequency Selection (DFS), so that all ETSI requirements are met.

Adding more to this competition between different standards, this month (December 2002) the first IEEE 802.11g products will be shipped. IEEE 802.11g works in the 2.4Mbps band, offers maximum raw data rate of 54Mbps and is backward compatible with 802.11b products.

Taking everything into account, it is not clear which standard is going to dominate high-rate wireless communications for office and home use. The WLAN field is a really interesting area at this period and engineers are working on a great number of projects. Most likely, in the following years, several standards will co-exist. It must be pointed out though that at the moment it seems that the IEEE 802.11 specification series have a clear advantage over the others, as they have succeeded in capturing most of the market. This means that in the following years the hardest competitor of an 802.11 standard will probably be another 802.11 standard.

#### **4. Conclusions**

Putting everything together, Wireless LANs are expected to change the way people work at the office and live at home. New technologies have enabled the support of a great number of different applications, such as exchange of control information, voice and video between devices in a wireless manner. As a result, the area concentrates the interest of the academic and the industry world.

We divided these technologies based on their applications. At the beginning, we presented Bluetooth and IEEE 802.11b as well as a comparison between them. Next, we described HomeRF (which is targeted towards residential use only) and compared it with Bluetooth and

IEEE 802.11b. Turning to high-rate technologies, we focused on IEEE 802.11a and HiperLAN/2. These two standards were then compared at the office level and with HomeRF at the home level.

## 5. References

### Papers of Common Interest

**[1] Wireless communications and networking: an overview**

*Jordan, R.; Abdallah, C.T.*

IEEE Antennas and Propagation Magazine, Volume: 44 Issue: 1, Feb. 2002

Page(s): 185–193

**[2] End-User Perspectives on Home Networking**

*Sandy Teger, David J. Waks*

IEEE Communications Magazine April 2002

Page(s): 115-119

**[3] Networking gets personal**

*Bravo-Escos, M.*

IEEE Review, Volume: 48 Issue: 1, Jan. 2002

Page(s): 32 –36

**[4] RF challenges for 2.4 and 5 GHz WLAN deployment and design**

*Ming-Ju Ho; Rawles, M.S.; Vrijkorte, M.; Fei, L.*

Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE, Volume: 2, 2002

Page(s): 783 -788 vol.2

**[5] Throughput performance of wireless LANs operating at 2.4 and 5 GHz**

*Kammerman, A.; Aben, G.*

Personal, Indoor and Mobile Radio Communications, 2000. PIMRC 2000. The 11th IEEE International Symposium on, Volume: 1, 2000

Page(s): 190 -195 vol.1

**[6] Security in wireless residential networks**

*Krishnamurthy, P.; Kabara, J.; Anusas-Amornkul, T.*

Consumer Electronics, IEEE Transactions on, Volume: 48 Issue: 1, Feb. 2002

Page(s): 157–166

### Bluetooth

**[7] Bluetooth: a new era of connectivity**

*Wei-Shin Wang*

IEEE Microwave Magazine, Volume: 3 Issue: 3, Sept. 2002

Page(s): 38 –42

**[8] The Bluetooth technology: merits and limitations**

*Shorey, R.; Miller, B.A.*

Personal Wireless Communications, 2000 IEEE International Conference on , 2000

Page(s): 80 –84

**[9] Bluetooth in wireless communication**

*Sairam, K.V.S.S.S.S.; Gunasekaran, N.; Redd, S.R.*

IEEE Communications Magazine, Volume: 40 Issue: 6, June 2002

Page(s): 90 –96

**[10] An overview of the Bluetooth wireless technology**

*Chatschik, B.*

IEEE Communications Magazine, Volume: 39 Issue: 12, Dec. 2001

Page(s): 86 –94

**[11] Bluetooth -based wireless personal area network for multimedia communication**

*Khan, J.Y.; Wall, J.; Rashid, M.A.*

Electronic Design, Test and Applications, 2002. Proceedings. The First IEEE International Workshop on, 2002

Page(s): 47 –51

**802.11**

**[12] IEEE Std. 802.11a – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – High Speed Physical Layer in the 5 GHz band**

**[13] IEEE 802.11 Wireless Local Network**

*Brian Crow, Indra Widjaja, Jeong Geun Kim, Prescott T. Sakai*

[www.cs.bilkent.edu.tr/~korpe/courses/cs515/papers/802.11.pdf](http://www.cs.bilkent.edu.tr/~korpe/courses/cs515/papers/802.11.pdf)

**[14] Measured Performance of 5GHz 802.11a Wireless LAN System**

*James C. Chen, Jeffrey Gilbert*

[www.atheros.com/AtherosRangeCapacityPaper.pdf](http://www.atheros.com/AtherosRangeCapacityPaper.pdf)

**[15] The IEEE 802.11b security problem. I**

*Williams, J.*

IT Professional, Volume: 3 Issue: 6, Nov.-Dec. 2001

Page(s): 96 –95

**[16] Experimental study on coexistence of 802.11b with alien devices**

*del Prado, J.; Sunghyun Choi*

Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th, Volume: 2, 2001

Page(s): 977 -981 vol.2

**[17] 802.11: leaving the wire behind**

*Kapp, S.*

IEEE Internet Computing , Volume: 6 Issue: 1 , Jan.-Feb. 2002

Page(s): 82 –85

**[18] Wi-Fi hotspot networks sprout like mushrooms**

IEEE Spectrum , Volume: 51 Issue: 9 , Sept. 2002

Page(s): 18 –20

**[19] Understanding Wi-Fi**

January 2002

<http://h30008.www3.hp.com/images/whitePapers/understandingWiFi.pdf>

**[20] Your 802.11 Wireless Network has No Clothes**

*William A. Arbaugh, Narendar Shankar, and Y.C.Justin Wan.*

<http://www.cs.umd.edu/~waa/wireless.pdf>

**Comparing 802.11b with Bluetooth**

**[21] Performance issues on wireless 2.4 GHz ISM band in multisystem environment**

*Sydanheimo, L.; Keskilammi, M.; Kivikoski, M.*

Consumer Electronics, 2002. ICCE. 2002 Digest of Technical Papers. International Conference on, 2002  
Page(s): 304–305

**[22] Wireless Standards Security Comparisons**

[http://www.bluetooth.com/upload/14Bluetooth\\_Wifi\\_Security.pdf](http://www.bluetooth.com/upload/14Bluetooth_Wifi_Security.pdf)

**[23] Evaluation of interference between IEEE 802.11b and Bluetooth in a typical office environment**

*Chandrashekar, M.V.S.; Choi, P.; Maver, K.; Sieber, R.; Pahlavan, K.*

Personal, Indoor and Mobile Radio Communications, 2001 12th IEEE International Symposium on, Volume: 1, 2001

Page(s): D-71 -D-75 vol.1

**[24] Empirical study for IEEE 802.11 and Bluetooth interoperability**

*Howitt, I.; Mitter, V.; Gutierrez, J.*

Vehicular Technology Conference, 2001. VTC 2001 Spring. IEEE VTS 53rd, Volume: 2, 2001

Page(s): 1109 -1113 vol.2

**[25] Wi-Fi (802.11b) and Bluetooth: enabling coexistence**

*Lansford, J.; Stephens, A.; Nevo, R.*

IEEE Network, Volume: 15 Issue: 5, Sept.-Oct. 2001

Page(s): 20 –27

**[26] Co-existence of bluetooth and IEEE 802.11b WLANs: results from a radio network testbed**

*Matlieus, K.; Zurbes, S.*

Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on, Volume: 1, 2002

Page(s): 151 –155

**HIPERLAN/2**

**[27] HiperLAN2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band**

*Martin Johnsson*

[www.hiperlan2.com/presdocs/site/whitepaper.pdf](http://www.hiperlan2.com/presdocs/site/whitepaper.pdf)

**[28] HiperLAN/2: Broadband Wireless Communications at 5 GHz**

*Jamshid Khun-Jush, Peter Schram, Goran Malmgren, Hohann Torsner*

IEEE Communications Magazine June 2002

Page(s): 130-136

**Comparing 802.11a with HiperLAN/2**

**[29] Coexistence and internetworking of IEEE 802.11a and ETSI BRAN HIPERLAN/2 in Multihop Scenarios**

*Stefan Mangold, Jorg Habetha, Sunghyun Choi, Chiu Ngo*

IEEE Workshop on WLANs, September 27-28, 2001 Boston, MA

[www.wlan01.wpi.edu/proceedings/wlan16d.pdf](http://www.wlan01.wpi.edu/proceedings/wlan16d.pdf)

**[30] A comparison of the HIPERLAN/2 and IEEE 802.11a Wireless LAN Standards**

*A. Doufexi, S. Armour, M. Butler, A. Nix, D. Bull, J. McGeehan, P. Karlsson*

IEEE Communications Magazine May 2002

Pages: 172-180

**[31] IEEE 802.11 or ETSI BRAN HIPERLAN/2: Who Will Win the Race for a High Speed Wireless LAN standard?**

*A. Hettich, M. Schrother*

European WL Conference, Germany, October 1999, Pages: 169-174

[http://easy.intranet.gr/paper\\_3.pdf](http://easy.intranet.gr/paper_3.pdf)

**[32] A system simulation of wireless local area networks operating in the 5GHz band**

*Master's thesis by Fredrik Kristensen and Magnus Sandgren*

[www.hiperlan2.com/presdocs/site/rapporten039.doc](http://www.hiperlan2.com/presdocs/site/rapporten039.doc)

[www.hiperlan2.com/presdocs/site/Abstract.doc](http://www.hiperlan2.com/presdocs/site/Abstract.doc)

**[33] 5 GHz goes the distance for home networking**

*Fowler, P.*

IEEE Microwave Magazine, Volume: 3 Issue: 3, Sept. 2002

Page(s): 49 –55

**HomeRF**

**[34] HomeRF: wireless networking for the connected home**

*Negus, K.J.; Stephens, A.P.; Lansford, J.*

IEEE Personal Communications, Volume: 7 Issue: 1, Feb. 2000

Page(s): 20 –27

**[35] The design and implementation of HomeRF: a radio frequency wireless networking standard for the connected home**

*Lansford, J.; Bahl, P.*

Proceedings of the IEEE, Volume: 88 Issue: 10, Oct. 2000

Page(s): 1662 –1676

**[36] Wireless Networking Choices for the Broadband Internet Home**

[http://homerf.org/data/tech/homerfbroadband\\_whitepaper.pdf](http://homerf.org/data/tech/homerfbroadband_whitepaper.pdf)

**[37] Interference Immunity of 2.4GHz Wireless LANs**

[http://homerf.org/data/tech/hrf\\_interference\\_immun\\_wp.pdf](http://homerf.org/data/tech/hrf_interference_immun_wp.pdf)

**[38] Quality of Service in the home networking model**

[http://homerf.org/data/tech/HomeRF\\_QoS\\_whitepaper.pdf](http://homerf.org/data/tech/HomeRF_QoS_whitepaper.pdf)

**[39] A comparison of Security in HomeRF versus IEEE 802.11b**

[http://homerf.org/data/tech/security\\_comparison.pdf](http://homerf.org/data/tech/security_comparison.pdf)