INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. 2001; **14**:1–42

REVIEW

Design alternatives for wireless local area networks

P. Nicopolitidis, G. I. Papadimitriou*,† and A. S. Pomportsis

Department of Informatics, Aristotle University, Box 888, 54006 Thessaloniki, Greece

SUMMARY

In this paper an overview of the wireless local area network (LAN) area is provided. The two types of wireless LAN topologies used today, infrastructure and ad hoc, are presented. The requirements that a wireless LAN is expected to meet are discussed. These requirements impact on the implementation of both the Physical and MAC layer of a wireless LAN. The unique characteristics of wireless physical layers are discussed and the five technology alternatives used today are presented. MAC layer issues are discussed and the two existing standards, IEEE 802.11 and HIPERLAN 1, are examined. Polling-based MAC protocols (RAP, GRAP) are also reviewed. Finally, an introduction is made to wireless technologies that interact with WLANs, such as personal area networking (PAN) and wireless ATM and an overview of HIPERLAN 2, a WLAN using ATM technology, is provided. Copyright © 2001 John Wiley & Sons, Ltd.

KEY WORDS: wireless LANs; physical layer; MAC protocol; IEEE 802.11; HIPERLAN; bluetooth; WATM

1. INTRODUCTION

1.1. Historical overview

Wireless networks, as the name suggests, utilize a wireless medium for transmission of information. Wireless networks are the end result of the move towards integration of network technologies and radio communications. These areas were initially brought together in 1971 at the University of Hawaii under the research project ALOHANET. The idea of the project was to offer bi-directional communications between computers spread over four islands and a central computer without the use of phone lines.

The ALOHANET project however falls under the wide area networking (WAN) category. Wireless local area network (WLAN) growth commenced in the mid-1980s and was triggered by the U.S. Federal Communications Commission (FCC) decision to authorize the public use of the

*Correspondence to: G. I. Papadimitriou, Department of Informatics, Aristotle University, Box 888, 54006 Thessaloniki, Greece.

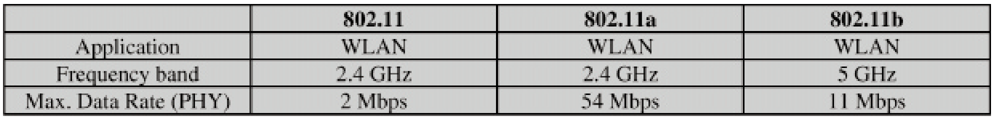
† E-mail: gp@csd.auth.gr

Received 3 April 2000
Accepted 5 September 2000

Industrial, Scientific and Medical (ISM) bands. This decision eliminated the need for companies and end users to obtain FCC licenses to operate their wireless products. Since then, there has been a substantial growth in the area of WLANs. Lack of standards however, led to the appearance of many proprietary products thus dividing the market in several, possibly incompatible parts. Consequently, the need for standardization in the area appeared.

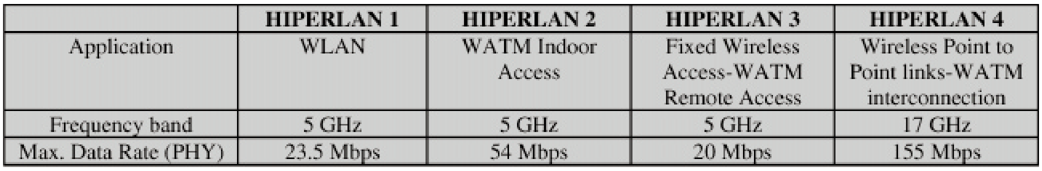
The first attempt to define a standard was made in the late 1980s by IEEE Working Group 802.4, which was responsible for the development of the token-passing bus access method. The group decided that token passing was an inefficient method to control a wireless network and suggested the development of an alternative standard. As a result, the Executive Committee of IEEE Project 802 decided to establish Working Group IEEE 802.11 which has been since then responsible for the definition of Physical and MAC sublayer standards for WLANs. The first 802.11 standard was finalized in 1997 and was developed by taking into consideration existing research efforts and market products, in an effort to address both technical and market issues. It offered data rates up to 2 Mbps at the physical layer using a spread spectrum modulation in the ISM bands. In September 1999, two supplements to the original standard were approved by the IEEE Standards Board. The first standard, 802.11b, extends the performance of the existing 2.4 GHz Physical layer, with potential data rates up to 11 Mbps. The second one, 802.11a aims to provide a new, higher data rate (from 20 up to 54 Mbps) Physical layer in the 5 GHz band. The family of 802.11 standards is shown in Figure 1.

Except for IEEE 802.11, another WLAN standard developed by group RES10 of the European Telecommunications Standards Institute (ETSI), as a Pan-European standard for high speed WLANs, is High Performance European Radio LAN (HIPERLAN). The HIPERLAN 1 standard, like 802.11, covers the Physical and MAC layers, offering data rates up to 23.5 Mbps by using traditional radio modulation techniques in the 5.2 GHz band. Upon completion of the HIPERLAN 1 standard, ETSI decided to merge the work on Radio Local Loop and Radio LANs through the formation of broadband radio access networks (BRAN). This project aims to specify standards for wireless ATM (HIPERLAN Types 2, 3, 4). The family of HIPERLAN standards is shown in Figure 2.



	802.11	802.11a	802.11b
Application	WLAN	WLAN	WLAN
Frequency band	2.4 GHz	2.4 GHz	5 GHz
Max. Data Rate (PHY)	2 Mbps	54 Mbps	11 Mbps

Figure 1. The IEEE 802.11 family of standards.



	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	WLAN	WATM Indoor Access	Fixed Wireless Access-WATM Remote Access	Wireless Point to Point links-WATM interconnection
Frequency band	5 GHz	5 GHz	5 GHz	17 GHz
Max. Data Rate (PHY)	23.5 Mbps	54 Mbps	20 Mbps	155 Mbps

Figure 2. The ETSI HIPERLAN family of standards.

1.2. Benefits of wireless networks

The continual growth in the area of WLANs can be partly attributed to the need to support mobile networked applications. Many jobs nowadays require people to physically move while using an appliance, such as a hand-held PC, which exchanges information with other user appliances or a central computer. Examples of such jobs are healthcare workers, police officers and doctors. Wired networks require a physical connection between the communicating parties, a fact that poses great difficulties in the implementation of practical equipment. Thus, WLANs are the technology of choice for such applications.

Another benefit of using a WLAN is the reduction in infrastructure and operating costs. A wireless LAN needs no cabling infrastructure, significantly lowering its overall cost. Moreover, in situations where cabling installation is expensive or impossible (e.g. historic buildings, monuments or the battlefield) WLANs appear to be the only feasible mean to implement networking. Lack of cabling also means reduced installation time, a fact that drives the overall network cost even lower.

A common fact in wired networks is the problems that arise from cable faults. Cable faults are responsible for most of the times a wired network fails. Moisture which causes erosion of the metallic conductors and accidental cable breaks can bring a wired network down. Therefore, the use of WLANs helps reduce both the downtime of the network and eliminate the costs associated with cable replacement.

1.3. Wireless LAN applications

The four major areas for WLAN applications [1] are LAN extension, cross-building interconnection, nomadic access and ad hoc networking. In the following sections we briefly examine each of these areas.

As mentioned, early WLAN products were aimed to substitute wired LANs. A WLAN reduces installation costs by using less cable than a wired LAN. However with advances in data transmission technology, companies continue to rely on wired LANs, especially those that use category 3 unshielded twisted pair cable. Most of the existing buildings are already wired with this type of cabling and new buildings are designed by taking into account the need for data applications and are thus pre-wired. As a result, WLANs were not able to substitute their wired counterparts to any great extent. However, they were found to be suitable in cases were flexible extension of an existing network infrastructure was needed. Examples include manufacturing plants, warehouses, etc. Most of these organizations already have a wired LAN deployed to support servers and stationary workstations. For example, a manufacturing plant typically has a factory floor, where cabling is not present, which must be linked to the plant's offices. A WLAN can be used in this case to link devices that operate in the non-cabled area to the organization's wired network. This application area of WLANs is referred to as LAN extension.

Another area of WLAN application is nomadic access. It provides wireless connectivity between a portable terminal and a LAN hub. One example of such a connection is the case of an employee transferring data from his portable PC to the server of his office upon returning from a trip or meeting. Another example of nomadic access is the case of a university campus, where students and working personnel access applications and information offered by the campus through their portable computers.

Ad hoc networking is another area of WLAN use. An ad hoc network is a peer-to-peer network that is set up in order to satisfy a temporary need. Example of this kind of application is a conference room or business meeting where the attendants use their portable computers in order to form a temporary network so as to share information during the meeting.

Another use of WLAN technology is to connect wired LANs located in nearby buildings. A point-to-point wireless link controlled by devices that usually incorporate a bridge or router functionality, connects the wired LANs. Although this kind of application is not really a LAN, it is often included in the area of WLANs.

1.4. *Wireless LAN concerns*

The primary disadvantage of wireless medium transmission, compared to wired transmission, is its increased error rate. The wireless medium is characterized by bit error rates (BER) having an order of magnitude even up to 10 times the order of magnitude of a LAN cable's BER. The primary reason for the increased BER is atmospheric noise, physical obstructions found in the signal's path, multipath propagation and interference from other systems. The latter takes either an inward or outward direction.

Inward interference comes from devices transmitting in the frequency spectrum used by the WLAN. However, most WLANs nowadays implement spread spectrum modulation, which operates over a wide amount of bandwidth. Narrowband interference only affects part of the signal, thus causing just a few errors, or no errors at all, to the spread spectrum signal. On the other hand, wideband interference, as the one caused by microwave ovens operating in the 2.4 GHz band, can have disastrous effects to any type of radio transmission. Interference is also caused by multipath fading of the WLAN signals, which results in random phase and amplitude fluctuations in the received signal. Thus, precautions must be taken in order to reduce inward interference in the operating area of a WLAN. A number of techniques that operate either on the Physical or MAC layer (like alternative modulation techniques, antenna diversity and feedback equalization in the physical layer, automatic repeat requests (ARQ), forward error control (FEC) in the MAC layer) are often used in this direction. Outward interference occurs when the WLAN signals disrupt the operation of adjacent WLANs or radio devices, such as intensive care equipment or navigational systems. However, as most WLANs use spread spectrum technology, outward interference is considered most of the times insignificant.

A significant difference between wired and wireless LANs is the fact that, in general, a fully connected topology between the WLAN nodes cannot be assumed. This problem gives rise to the 'hidden' and 'exposed' terminal problems, depicted in Figure 3. The 'hidden' terminal problem describes the situation where a station A, not in the transmitting range of another station C, detects no carrier and initiates a transmission. If C was in the middle of a transmission, the two stations' packets would collide in all other stations B that can hear both A and C. The opposite of this problem is the 'exposed' terminal scenario. In this case, B defers transmission since it hears the carrier of A. However, the target of B, C, is out of A's range. In this case B's transmission could be successfully received by C, however this does not happen since B defers due to A's transmission.

Figure 3. Terminal scenarios: (a) 'Hidden' and (b) 'exposed'.

Another difference between wired and wireless LANs is the fact that, in the latter, collision detection is difficult to implement. This is due to the fact that a WLAN node cannot listen to the wireless channel while sending, because its own transmission would swamp out all other incoming signals. Therefore, use of protocols employing collision detection is not practical in WLANs.

Another issue of concern regarding WLANs is power management. A portable PC is usually powered by a battery having a finite time of operation. Therefore, specific measures have to be taken in the direction of minimizing energy consumption in the mobile nodes of the WLAN. This fact may result in tradeoffs between performance and power conservation.

The majority of today's applications communicate using protocols that were designed for wire-based networks. Most of these protocols degrade significantly when used over a wireless link. TCP for example was designed to provide reliable connections over wired networks. Its efficiency however, is substantially lowered over wireless connections, especially when the WLAN nodes operate in an area where interference exists. Interference causes TCP to lose connections thus degrading network performance.

Another difference between wired and wireless LANs has to do with installation. When preparing for a WLAN installation one must take into account the factors that affect signal propagation. In an ordinary building or even a small office, this is very difficult, if not impossible. Omnidirectional antennas propagate a signal in all directions, provided that no obstacle exists in the signal's path. Walls, windows, furniture and even people can significantly affect the propagation pattern of WLAN signals causing undesired effects. This problem is most of the times addressed by performing propagation tests prior to the installation of WLAN equipment.

Security is another area of concern in WLANs. Radio signals may propagate beyond the geographical area of an organization. All a potential intruder has to do is to approach the WLAN operating area and with a little bit of luck eavesdrop on the information being exchanged. Nevertheless, for this scenario to take place, the potential intruder needs to possess the network's access code in order to join the network. Encryption of traffic can be used to increase security, which however has the undesired effect of increased cost and overhead. WLANs are also susceptible to electronic sabotage. Most of them utilize CSMA-like protocols where all nodes are obliged to remain silent as long as they hear a transmission in progress. If someone sets a node within the WLAN area to endlessly transmit packets, all other nodes are prevented from transmitting, thus bringing the network down.

Finally, a popular issue that has to do not only with WLANs, but also with wireless communications in general is human safety. Despite the fact that a final answer to this question has yet to be given, WLANs appear to be in the worst case just as safe as cellular phones. Radio-based WLAN components operate at power levels between 50 and 100 mW, which is substantially lower than the 600 mW to 3 W range of a common cellular phone. In infrared WLAN systems, threat to human safety is even lower. Diffused infrared (IR) WLANs offer no hazard under any circumstance.

1.5. Scope of this paper

The remainder of this paper provides an overview of the WLAN area. In Section 2 the two types of WLAN topologies, infrastructure and ad hoc, are investigated. In Section 3 the requirements a WLAN is expected to meet are discussed. These requirements impact the implementation of Physical and MAC layers for WLANs. In Section 4, Physical layer features are investigated and the five technology alternatives used today are presented. In Section 5 MAC layer issues are discussed and the two existing WLAN standards, IEEE 802.11 and HIPERLAN 1, are examined. Polling-based MAC protocols (RAP, GRAP) are also reviewed. Finally, Section 6 is an introduction to wireless technologies that interact with WLANs, such as personal area networking (PAN) and Wireless ATM, closing with an overview of HIPERLAN 2, a WLAN standard using ATM technology.

2. WIRELESS LAN TOPOLOGIES

There are two major WLAN topologies, ad hoc and infrastructure (see Figure 4). An ad hoc WLAN is a peer-to-peer network that is set up in order to serve a temporary need. No networking infrastructure needs to be present, as the only things needed to set up the WLAN are the mobile nodes and use of a common protocol. No central co-ordination exists in this topology. As a result, ad hoc networks are required to use de-centralized MAC protocols, such as CSMA/CA, with all nodes having the same functionality and thus implementation complexity and cost. Moreover, there is no provision for access to wired network services that may be collocated in the geographical area where the ad hoc WLAN operates. Another important aspect of ad hoc WLANs is that fully connected network topologies cannot be assumed [2]. This is due to the fact that two mobile nodes may temporarily be out of transmission range of one another.

An infrastructure WLAN makes use of a higher speed wired or wireless backbone. In such a topology, mobile nodes access the wireless channel under the coordination of a base station (BS). As a result, infrastructure-based WLANs mostly used centralized MAC protocols like polling, although de-centralized MAC protocols are also used (for example the contention-based 802.11 can be implemented in an infrastructure topology). This approach shifts implementation complexity from the mobile nodes to the access point (AP), as most of the protocol procedures are performed by the AP thus leaving the mobile nodes to perform a small set of functions. The mobile nodes under the coverage of a BS, form this BS's cell. Although a fully connected network topology cannot be presumed in this case either, the fixed nature of the BS implies full coverage of its cell in most cases. Traffic that flows from the mobile nodes to the BS is called uplink traffic. When the flow of traffic follows the opposite direction, it is called downlink traffic.

Another use of the BS is to interface the mobile nodes to an existing wired network. When a BS performs this task as well, it is often referred to as an access point (AP). Despite the fact that it is

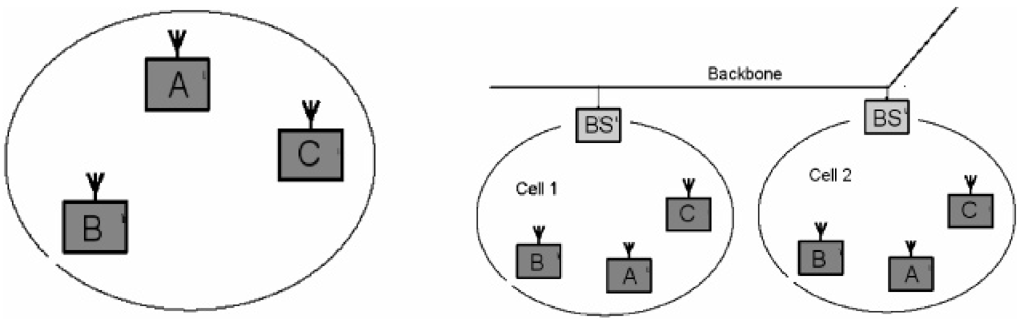


Figure 4. WLAN topologies: ad hoc and infrastructure.

not mandatory that the BS and AP be implemented in the same device, most of the times BSs also include AP functionality. Providing connectivity to wired network services is an important requirement, especially in cases where the mobile nodes use applications originally developed for wired networks.

The presence of many BSs and thus cells is common in infrastructure WLANs. Such multi-cell configurations can cover multiple-floor buildings and are employed when greater range than that offered by a single cell is needed. In this case, mobile nodes can move from cell to cell while maintaining their logical connections. This procedure is also known as Roaming and implies that cells must properly overlap so that users do not experience connection losses. Furthermore, coordination among access points is needed in order for users to transparently roam from one cell to another. Roaming is implemented through handoff procedures. Handoff can be controlled either by a switching office in a centralized way, or by mobile nodes (de-centralized handoff) and is implemented by monitoring the signal strengths of nodes. In centralized handoff, the BS monitors the signal strengths of the mobile nodes and reassigns them to cells accordingly. In de-centralized handoff, a mobile node may decide to request association with a different cell after determining that link quality to that cell is superior to that of the previous one.

As far as the cell size is concerned, it is desirable to use small cells. Reduced cell sizes means shorter transmission ranges for the mobile nodes and thus less power consumption. Furthermore, small cell sizes enable frequency reuse schemes, which result in spectrum efficiency. The concept of frequency reuse is illustrated in Figure 5. In this example, non-adjacent cells can use the same frequency channels. If each cell uses a channel with bandwidth B, then with frequency reuse, a total of $3*B$ bandwidth is sufficient to cover the 16-cell region. Without frequency reuse, every cell would have to use a different frequency channel, as a scheme that would demand a total $16*B$ of bandwidth.

The above strategy is also known as fixed channel allocation (FCA). Using FCA, channels are assigned to cells and not to mobiles nodes. The problem with this strategy is that it does not take advantage of user distribution. A cell may contain a few, or no mobiles nodes at all and still use the same amount of bandwidth with a densely populated cell. Therefore, spectrum utilization is sub-optimal. Dynamic channel allocation (DCA) [3–5], power control (PC) or integrated DCA and PC [6] techniques try to increase overall cellular capacity, reduce channel interference and conserve power at the mobile nodes. DCA places all available channels in a common pool and

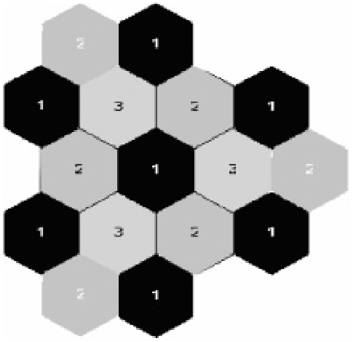


Figure 5. Example of frequency reuse.

dynamically assigns them to cells depending on their current load. Furthermore, the mobile nodes notify BSs about experienced interference enabling channel reuse in a way that minimizes interference. PC schemes try to minimize interference in the system and conserve energy at the mobile nodes by varying transmission power. When increased interference is experienced within a cell, PC schemes try to increase the signal-to-interference noise ratio (SIR) at the receivers by boosting transmission power at the sending nodes. When the experienced interference is low, sending nodes are allowed to lower their transmitting power in order to preserve energy.

Comparison of the above two WLAN topologies yields several differences [7]. However, most of these results stem from the assumption that ad hoc WLANs utilize contention MAC protocols (e.g. CSMA) whereas infrastructure ones use TDMA-based ones. Based solely on topology, one can argue that the main advantage of infrastructure WLANs is their ability to provide access to wired network applications and services. On the other hand, ad hoc WLANs are easier to set-up and require no infrastructure, thus having potentially lower costs.

3. WIRELESS LAN REQUIREMENTS

A WLAN is expected to meet the same requirements with a traditional wired LAN, such as high capacity, robustness, broadcast and multicast capability, etc. However, due to the use of the wireless medium for data transmission, there are additional requirements a WLAN is supposed to meet. Those requirements affect the implementation of the Physical and MAC layers and are summarized below:

- *Throughput*: Although this is a general requirement for every network, it is even more crucial an aspect for WLANs. The issue of concern in this case is the system's operating throughput and not the maximum throughput it can achieve. In a wired 802.3 network for example, although a peak throughput in the area of 8 Mbps is achievable, it is accompanied by great delay. Operating throughput in this case is measured to be around 4 Mbps, only 40 per cent of the link's capacity. Such a scenario in today's WLANs with physical layers of a couple of Mbps, would be undesirable. Thus, MAC layers that shift operating throughput towards the theoretical figure are required.
- *Number of nodes*: WLANs often need to support tens or hundreds of nodes. Therefore the WLAN design should pose no limit to the network's maximum number of nodes.
- *Ability to serve multimedia, priority traffic and client server applications*: In order to serve today's multimedia applications, such as video conferencing and voice transmission, a WLAN must be able to provide QoS connections and support priority traffic among its nodes. Moreover, since many of today's WLAN applications use the client–server model, a WLAN is expected to support non-reciprocal traffic. Consequently, WLAN designs must take into consideration the fact that flow of traffic from the server to the clients can often be greater than the opposite.
- *Energy saving*: Mobile nodes are powered by batteries having a finite time of operation. A node consumes battery power for packet reception and transmission, handshakes with BSs and exchange of control information. Typically, a mobile node may operate either in normal or sleep mode. In the latter case however, a procedure that wakes up a transmission's destination node needs to be implemented. Alternatively, buffering can be used at the sender, posing however the danger of buffer overflows and packet losses. The above discussion suggests that schemes resulting in efficient power use should be adopted.

- *Robustness and security*: As already mentioned, WLANs are more interference prone and more easily eavesdropped on. The WLAN must be designed in a way that data transmission remains reliable even in noisy environments, so that service quality remains at a high level. Moreover, security schemes must be incorporated in WLAN designs to minimize the chances of unauthorized access or sabotage.
- *Collocated network operation*: With the increasing popularity of WLANs another issue that surfaces is the ability for two or more WLANs to operate in the same geographical area or in regions that partly overlap. Collocated networks may cause interference to each other, which may result in performance degradation. One example of this case is neighboring CSMA WLANs. Suppose that two networks, A and B are located in adjacent buildings and that some of their nodes are able to sense transmissions originating from the other WLAN. Furthermore, assume that in a certain time period, no transmissions are in progress in WLAN A and a transmitting node exists in WLAN B. Nodes in A may sense B's traffic and falsely defer transmission, despite the fact that no transmissions are taking place in their own network.
- *Handoff – roaming support*: As mentioned earlier, in cell structured WLANs a user may move from one cell to another while maintaining all logical connections. Moreover, the presence of mobile multimedia applications that pose time bounds on the wireless traffic makes this issue of even greater importance. Mobile users using such applications must be able to roam from cell to cell without perceiving degradation in service quality or connection losses. Therefore, WLANs must be designed in a way that allows roaming to be implemented in a fast and reliable way.
- *Effect of propagation delay*: A typical coverage area for WLANs can be up to 500–1000 ft in diameter. The effect of propagation delay can be significant, especially in case where a WLAN MAC demands precise synchronization among mobile nodes. For example, in cases where unslotted CSMA is used, increased propagation delays result to a rising number of collisions, reducing the WLANs performance. Thus, a WLAN MAC should not be heavily dependent on propagation delay.
- *Dynamic topology*: In a WLAN, fully connected topologies cannot be assumed, due to the presence of the 'hidden' and 'exposed' terminal problems. A good WLAN design should take this issue into consideration limiting its negative effect on network performance.
- *Compliance with standards*: As the WLAN market progressively matures, it is of significant importance to comply with existing standards. Designs and product implementations based on new ideas are always welcome, provided however that they are optional extensions to a given standard. In this way, interoperability is achieved.

4. THE PHYSICAL LAYER

4.1. Wireless transmission characteristics

Electromagnetic waves were predicted by the British physicist James Maxwell in 1865 and observed by the German physicist Heinrich Hertz in 1887. These waves are created by the movement of electrons and have the ability to propagate through space. Using appropriate antennas, transmission and reception of electromagnetic waves through space becomes feasible. This is the base for all wireless communications. Understanding of the signal propagation mechanism is of increased importance, since it provides a means for predicting the coverage area of a transmitter and the interference experienced at the receiver. Although the mechanism that governs propagation of electromagnetic waves through space is of increased complexity, it can generally be attributed to three phenomena: reflection, diffraction and scattering. Furthermore, the mobile nature of a WLAN gives rise to the phenomenon of Doppler shift.

Reflection occurs when an electromagnetic wave falls on an object with dimensions very large compared to the wave's wavelength. Scattering occurs when the signal is obstructed by objects with dimensions in the order of the wavelength of the electromagnetic wave. This phenomenon causes the energy of the signal to be transmitted over different directions and is the most difficult to predict. Finally, diffraction, also known as shadowing, occurs when an electromagnetic wave falls on an impenetrable object. In this case, secondary waves are formed behind the obstructing body despite the lack of line-of-sight (LOS) between the transmitter and the receiver. However, these waves have less power than the original one. The amount of diffraction is dependent on the radio frequency used, with low-frequency signals diffracting more than high-frequency ones. Thus high-frequency signals, especially, ultra high frequencies (UHF), and microwave signals require line of sight for adequate signal strength. Shadowed areas are often large, resulting in the rate of change of the signal power being slow. Thus, shadowing is also known as slow-fading.

In a wireless channel, the signal from the transmitter may be reflected from objects such as hills, buildings, etc. These phenomena cause portions of the signal to propagate over different paths with different path lengths. This is known as multipath propagation and leads to fluctuations of received signal power. Because these fluctuations are experienced over very short distances (typically at half-wavelength distances), the phenomenon is also known as fast fading. When the path lengths differ by a multiple of half of the signal's wavelength, arriving signals may partially or totally cancel each other. Fast fading, also known as Rayleigh fading, causes the received signal power to vary rapidly even by three or four orders of magnitude when the receiver moves by only a fraction of the signal's wavelength. When the path length differences are comparable to the transmitted symbol time, multipath propagation produces intersymbol interference (ISI). The latter is the presence of energy from a previous symbol during the detection time of the current one. However, the average received signal power, which is computed over receiver movements of 10–40 wavelengths and used by the mobile receiver in roaming and power control decisions, is characterized by very small variations and decreases only when the transmitter moves away from the receiver over significantly large distances. Rayleigh fading is also frequency selective [8], meaning that different parts of a channel's spectrum generally experience different effects due to Rayleigh fading during a specific time duration. The zones affected by it tend to be small, multiple areas of space where periodic attenuation of a received signal is experienced. In other words, the received signal strength will fluctuate, causing a momentary, but periodic, degradation in quality.

Another cause of reception errors in wireless transmission is cochannel interference. For example, in a cellular infrastructure WLAN, cochannel interference may arise from non-adjacent cells that use the same frequency. Although use of the same frequency is permitted only on non-adjacent cells, such phenomena often occur in WLAN implementations. Cochannel interference can also be caused by devices operating in the same frequency band with the WLAN, like microwave ovens and electronic equipment.

Finally, the mobility of nodes in WLANs and other mobile computing devices give rise to the phenomenon of Doppler shift. When a signal transmitter and receiver are moving relative to one another, the frequency of the received signal will not be the same as that of the source. When they are moving towards each other the frequency of the received signal is higher than that of the

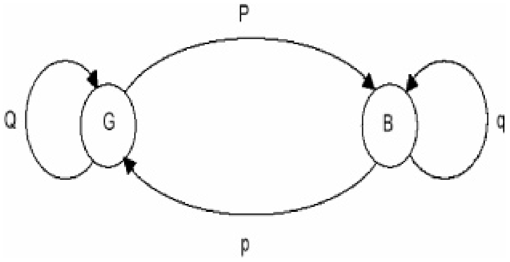


Figure 6. Transition diagram of a Markov chain.

source, and when they are moving away from each other the frequency decreases. This phenomenon becomes important when developing mobile radio systems.

Although there are additional electromagnetic wave propagation impairments, such as free-space loss and thermal noise, fading is the primary cause of reception errors in wireless communications. Measurements reveal that noise errors over fading channels are of bursty nature and Markov chain model approximations have been shown to be adequate for wireless channel error modeling [9,10]. Such models comprise two states, a Good (G) and a Bad (B) one, and parameters that define the transition procedure between the two states. State G is error-free, thus bit errors only occur in state B. Future states are independent of past states and depend only on the present state. In other words the model is memoryless. Figure 6 depicts the transition diagram of a Markov chain. P is the probability of the channel state transiting from state G to state B, p defines the probability of transition from state B to state G, Q and q the probabilities of the channel remaining in states G and B, respectively. Obviously $Q = 1 - P$ and $q = 1 - p$. In state B, bit errors are assumed to occur with probability h. Values for the model parameters are obtained through statistical measurements of particular channels. These values are different for different channels and physical environments. Markov chain models can efficiently approximate the behaviour of a wireless channel and are widely used in WLAN computer simulations.

Physical layer designers often use one or a combination of techniques to combat ISI. Such techniques are spread spectrum, antenna diversity, channel equalization and multisubcarrier modulation. Spread spectrum is discussed in later sections. Antenna diversity, also known as space diversity, is based on the use of multiple antennae at the mobile nodes. The receiver circuitry selects the best of the antennae outputs or uses a number of them in order to co-phase the received multipath signal components. All other things being equal, a system implementing antenna diversity will support a longer range than a system that does not. Furthermore, a system implementing diversity both at the transmitter and the receiver will be able to support greater ranges than one that implements diversity only at one end. Result measurements in Reference [11] show that antenna diversity reduces occurred BER for a given signal-to-interference ratio (SIR). However, diversity is more complicated than other techniques and consequently more power hungry.

Channel equalization techniques were first developed to reduce the error rates of systems communicating over a wired link. These techniques aim to predict the channel's ISI and thus cancel it from the signal to be transmitted. A set of coefficients is used at each receiver and transmission of training symbols prior to data is employed in order for the coefficients to converge to a point that describes the channel's behaviour. Once the coefficients have successfully converged, the transmitter 'pre-equalizes' the channel by canceling the predicted ISI from the transmitted signal. Recent research trends aim to reduce the mobile node's hardware complexity by shifting those signal processing tasks from mobiles to BSs thus resulting in asymmetric ISI cancellation architectures. A combination of antenna diversity and channel equalization in an asymmetric architecture by acknowledging the reciprocal property of a wireless link is also used. [12] reviews this approach and discusses the feasibility and implications posed by it.

Multisubcarrier modulation [13] is another technique that achieves ISI reduction. The channel bandwidth is divided into N sub-bands. Over each one of them a separate communication link is established. The data stream is divided into N interleaved sub-streams, which are used to modulate the carrier of each sub-band. This results in reduced ISI, since fading does not occur with the same intensity over the entire bandwidth of a channel.

WLAN performance is affected by the preamble plus header length added by the physical layer and the time required for the transceiver circuit of a node to switch from transmit to receive mode. The latter is also called the Tx/Rx turnaround time and has a significant effect on WLAN performance. These parameters are generally different for different physical layers. [13] provides simulation results of the performance of the IEEE 802.11 MAC over three 802.11 physical layer specifications, concluding that end performance is affected by the above two parameters. The infrared (IR) physical layer shows better performance than the direct sequence spread spectrum (DSSS) one, which in turn is proved to be superior to the frequency hopping spread spectrum (FHSS) physical layer.

4.2. The infrared physical layer

Infrared and visible light are of near wavelengths and thus behave similarly. Infrared light is absorbed by dark objects, reflected by light objects and cannot penetrate walls. Today's WLAN products that use IR transmission operate at wavelengths near 850 nm. This is because transmitter and receiver hardware implementation for these bands is cheaper and also because the air offers the least attenuation at that point of the IR spectrum. The IR signal is produced either by semiconductor laser diodes or LEDs with the former being preferable because their electrical to optical conversion behavior is more linear. However, the LED approach is cheaper and the IEEE 802.11 IR Physical layer specifications can easily be met using LEDs for IR transmission.

Three different techniques are commonly used to operate an IR product: Diffused transmission that occurs from an omnidirectional transmitter, reflection of the transmitted signal on a ceiling and focused transmission. In the latter, the transmission range depends on the emitted beam's power and its degree of focusing and can be of several kilometers. It is obvious that such ranges are not needed for most WLAN implementations. However, focused IR transmission is often used to connect LANs located in the same or different buildings where a clear LOS exists between the wireless IR bridges or routers.

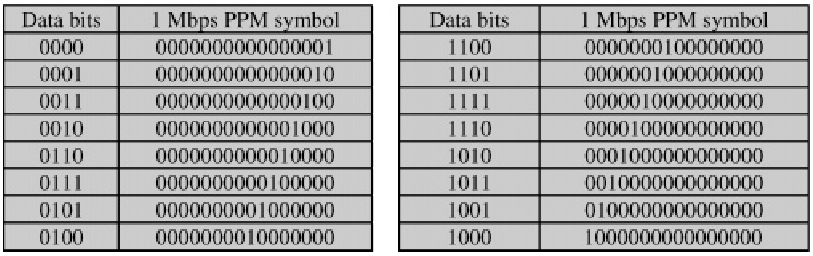
In omnidirectional transmission, the mobile node's transmitter utilizes a set of lenses that converts the narrow optical laser beam to a wider one. The produced optical signal is then radiated to all directions thus providing coverage to the other WLAN nodes. In ceiling bounced transmission, the signal is aimed at a point on a diffusely reflective ceiling and is received in an omnidirectional way by the WLAN nodes. In cases where BSs are deployed, they are placed on the ceiling and the transmitted signal is aimed at the BS which acts as a repeater by radiating over a wider range the received focused signal. Ranges that rarely exceed 20 m characterize both this and the omnidirectional technique.

IR radiation offers significant advantages over other physical layer implementations. The infrared spectrum offers the ability to achieve very high data rates. [13] uses basic principles of information theory to prove that non-directed optical channels have very large Shannon capacities and thus, transfer rates in the order of 1 Gbps are theoretically achievable. The IR spectrum is not regulated in any country a fact that helps to keep costs down.

Another strength of IR is the fact that in most cases transmitted IR signals are demodulated by detecting their amplitude, not their frequency or phase. This fact reduces the receiver complexity, since it does not need to include precision frequency conversion circuits and thus lowers overall system cost. IR radiation is immune to electromagnetic noise and cannot penetrate walls and opaque objects. The latter is of significant help in achieving WLAN security, since it can be made sure that IR transmissions do not escape the geographical area of a building or closed office. Furthermore cochannel interference can potentially be eliminated if IR-impenetrable objects, such as walls, separate adjacent cells.

IR transmission also exhibits drawbacks. IR systems share a part of the spectrum that is also used by the sun, thus making use of IR-based WLANs practical only for indoor application. Fluorescent lights also emit radiation in the IR spectrum causing SIR degradation at the IR receivers. A solution to this problem could be the use of high-power transmitters, however power consumption and eye safety issues limit the use of this approach. Limits in IR transmitted power levels and the presence of IR opaque objects lead to reduced transmission ranges which means that more BSs need to be installed in an infrastructure WLAN. Since BSs are connected with wire, the amount of wiring might not be significantly less than that of a wired LAN. Another disadvantage of IR transmission, especially in the diffused approach, is the increased occurrence of multipath propagation, which leads to ISI, effectively reducing transmission rates. Another drawback of IR WLANs is the fact that producers seem to be reluctant to implement IEEE 802.11 compliant products using IR technology. Furthermore, HIPERLAN does not address IR transmission at all.

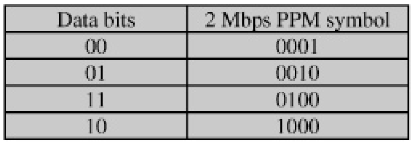
The IEEE 802.11 physical layer specification uses pulse position modulation (PPM) to transmit data using IR radiation. PPM varies the position of a pulse in order to transmit different binary symbols. Extensions 802.11a and 802.11b address only microwave transmission issues. Thus, the IR physical layer can be used to transmit information either at 1 or 2 Mbps. For transmission at 1 Mbps, 16 symbols are used to transmit 4 bits of information, whereas in the case of 2 Mbps transmission, 2 data bits are transmitted using four pulses. Figures 7 and 8 illustrate the use of 16 and 4 PPM. Notice that the data symbols follow the Gray code. This ensures that only a single bit error occurs when the pulse position is varied by one time slot due to ISI or noise.



Data bits	1 Mbps PPM symbol
0000	0000000000000001
0001	0000000000000010
0011	0000000000000100
0010	0000000000001000
0110	0000000000010000
0111	0000000000100000
0101	0000000001000000
0100	0000000010000000

Data bits	1 Mbps PPM symbol
1100	0000000100000000
1101	0000001000000000
1111	0000010000000000
1110	0000100000000000
1010	0001000000000000
1011	0010000000000000
1001	0100000000000000
1000	1000000000000000

Figure 7. Sixteen-pulse position modulation code.



Data bits	2 Mbps PPM symbol
00	0001
01	0010
11	0100
10	1000

Figure 8. Four-pulse position modulation code.

Both the preamble and the header of an 802.11 frame transmitted over an IR link are always transmitted at 1 Mbps. The higher rate of 2 Mbps, if employed, modulates only the sent MPDU. The following describes the frame fields:

- SYNC: Contains alternating pulses in consecutive time slots. It is used for receiver synchronization. The size of this field is between 57 and 73 bits.
- Start frame delimiter: A 4-bit field that defines the beginning of a frame. It takes the value 1001.
- Data rate: a 3-bit field that takes the values 000 and 001 for 1 and 2 Mbps, respectively.
- DC level adjustment: Consists of a 32-bit pattern that stabilizes the signal at the receiver.
- Length: A 16-bit field containing the length of the MPDU in msec.
- FCS: A 16-bit frame check sequence used for error detection.
- MPDU: The 802.11 MAC protocol data unit to be sent. The size of this field ranges from 0 to 4096 octets.

4.3. Microwave radio transmission

The microwave radio portion of the electromagnetic spectrum spans from 10^7 to about 10^{11} MHz. Being of lower frequency, radio frequency (RF) channel behaviour differs significantly from that of IR. Radio transmission can penetrate walls and non-metallic materials, providing both the advantage of greater coverage and the disadvantages of reduced security and increased cochannel interference. RF transmission is robust to fluorescent lights and outdoor operation, thus the only possible technology to serve outdoor applications. Nevertheless, RF equipment is subject to increased cochannel interference, atmospheric, galactic and man-made noise. There are also other sources of noise that affect operation of RF devices, like high-current circuits and microwave ovens making the RF bands a crowded part of the spectrum. However, careful system design and use of technologies such as spread spectrum modulation, significantly reduce interference effects in most cases.

RF equipment is generally more expensive than IR. This can be attributed to the fact that most of the time sophisticated modulation and transmission technologies, like spread spectrum, are employed. This means complex frequency or phase conversion circuits must be used, a fact that might make end products more expensive. However, the advances in fabrication of components promise even larger factors of integration and constantly lowering costs. Finally, as far as the WLAN area is concerned, RF technology has an additional advantage over IR, due to the large installed base of RF-WLAN products and the adoption of RF technology in current WLAN standards.

Microwave radio transmission was first used for long-distance communications using very focused beams. However, in the last few years, this part of the spectrum has been experiencing a great popularity among electronic equipment manufacturers too. As a result, cordless telephones, paging devices and WLAN products that use this band for transmission have appeared. When a company wants to deploy a product that uses a part of the microwave spectrum for transmission, licensing from corresponding authorities is needed. Such authorities are the Federal Communications Commission (FCC) in the United Stated and the Conference of European Postal and Telecommunications Administrations (CEPT) in the European union.

Licensing poses both advantages and disadvantages. A significant advantage is that immunity to interference is guaranteed. If a product experiences performance degradation due to presence of interference, the corresponding authority will intervene and cease operation of the interfering source, since the latter is operating in a part of the spectrum licensed to another user. Disadvantages of licensing are the facts that the procedure can take a significant period of time and the electromagnetic spectrum is a scarce resource, so everyone does not achieves the desired bandwidth. The latter is true, especially in cases where the corresponding product is new and its market success not ensured. Such was the case for WLANs in the mid 1980's, when the licensing authorities seemed to be reluctant to authorize spectrum parts to WLAN vendors. This was due to the fact that the corresponding market was in a premature stage having no significant presence, while traditional voice oriented product vendors continued to demand more bandwidth. Thus, the need to satisfy the bandwidth needs of both the WLAN and existing product communities appeared.

The first step taken to resolve the problem was the authorization by FCC of license-free use of the industrial, scientific and medical (ISM) bands (902–928, 2400–2483.6 and 5725–5850 MHz) of the spectrum. This decision significantly boosted the WLAN industry in the U.S. Since then, manufacturers and users do not need to license bandwidth to operate their products, a fact that lowers both the overall cost and the time needed for deployment and operation of a WLAN. However, to prevent excessive cochannel interference, certain specifications must be met for a product to use these bands, the most important of which is the mandatory use of spectrum spreading and low transmission power.

In 1993, CEPT announced bands at 5.2 and 17.1 GHz for HIPERLAN. One year later, the FCC released an additional 20 MHz of spectrum between licensed bands in the 1.9 GHz band after a request made by WINFORUM. The latter is an alliance between major computer and communication companies and its objective is to obtain and efficiently use license-free spectrum for data communication services. Another initiative started by WINFORUM led FCC to grant public use to 300 MHz of spectrum in the 5 GHz Unlicensed-National Information Infrastructure (U-NII) bands. This decision was taken in 1997 and is compatible with the European 5.2 GHz band allocation for HIPERLAN by CEPT. In these bands FCC lifted the restriction of using only spread spectrum technology, thus providing the ability for higher data rates.

Today, the majority of WLAN products operate in the ISM bands. These bands are characterized by a number of significant differences. The most obvious is the fact that the higher bands, being wider, offer more bandwidth and thus higher potential transmission rates. Furthermore, the higher the band, the most challenging and expensive is the implementation of the corresponding RF equipment. The lower band for example, can be supported with low-cost silicon-based devices. On the other hand, the upper band requires use of expensive gallium arsenide (GaAs) equipment. The middle band can be supported by both technologies and is thus characterized by a moderate cost.

However the situation reverses when noise and interference are taken into account. From this point of view, the higher a band's frequency the more appealing is its use, since at high frequencies less interference and noise exists. For example, the 902 MHz band is extremely crowded by devices such as cellular and cordless telephones, RF heating equipment, etc. The 2.4 GHz band experiences less interference with the exception of microwave ovens whose kilowatt-level powers are concentrated towards the band's lower end. The 5.8 GHz is even more interference-free. The same situation characterizes galactic atmospheric and man made noise [7]. The higher a band's frequency, the more noise free the band is.

As far as transmission range is concerned, the lower the frequency of a band, the higher the achievable range. It is estimated [7] that the range in the 2.4 GHz band is around 5 per cent less than that in the 902 MHz band. For the 5.8 GHz band this number rises to 20 per cent. As a rule of thumb, one can say that the properties of the three ISM bands vary monotonically with frequency. Both significant advantages or disadvantages characterize the high and low bands. The 2.4 GHz band stands in the middle, having the additional advantage of being the only one available worldwide.

Currently, the most popular WLANs use RF spread spectrum technology. The spread spectrum technique was developed initially for military applications. The idea is to spread the transmitted information over a wider bandwidth in order to make interception and jamming more difficult. In a spread spectrum system, the input data is fed into a channel encoder, which uses a carrier to produce a narrowband analog signal centred around a certain frequency. This signal is then spread in frequency by a modulator, which uses a sequence of pseudorandom numbers. In the receiving end, the same sequence is used to demodulate the spread signal and recover the original narrowband analog signal. The latter, of course, is fed into a channel decoder to recover the initial digital data. A random number generator, using an initial value called the seed, produces the pseudorandom sequence of numbers. Those numbers are not really random, since the generator algorithm is a deterministic one. A given seed always produces the same set of random numbers. However, a good random number generator produces number sequences that pass many tests of randomness, thus making interception of the spread signal practically possible only when the receiver possesses knowledge both of the algorithm and the seed used.

Among its other advantages, spread spectrum technology turns out to be quite successful in combating fading. As already mentioned, fading is frequency selective. Thus, since a spread spectrum signal is very wide in frequency, fading only affects a small part of it. In the following paragraphs, the two spread spectrum techniques, frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) and their use as a physical layer for WLANs is presented. Next the alternatives of narrowband microwave transmission and orthogonal frequency division multiplexing physical layers are discussed.

4.3.1. The frequency hopping spread spectrum physical layer. Using this technique, the signal is broadcast over a seemingly random set of frequency channels, hopping from frequency to frequency at constant time intervals. The time spent on each channel is called a chip. The receiver executes the same hopping sequence while remaining in synchronization with the transmitter and thus receives the transmitted data. Any attempt to intercept the transmission would result in reception of only a few data bits. Attempts to jam the transmission succeed in erasing only a few random bits of the original message.

As mentioned in the previous paragraph, the hopping sequence is defined by the seed of the random number generator. The hopping rate, also known as chipping rate, defines the nature of the frequency hopping system. If set to a value greater than the transmission time of a single bit, multiple bits are transmitted over the same frequency channel. This technique is known as slow frequency hopping. If the hopping speed is set to a value less than the transmission time of a single bit, one bit is transmitted on more than one frequency. This technique is called fast frequency hopping. In both cases, when in a single channel, the actual transmitted signal is the result of modulation of the channel's centre frequency with the original signal. FCC regulations state that each frequency channel is 0.5 MHz (902 MHz band) or 1 MHz (2.4 and 5.8 GHz bands) wide. In the 902 MHz bands 52 FH channels exist of which 50 must be used. In the middle band and upper bands these channel numbers are 100 (83 in the U.S.), 75, 125 and 75, respectively. Furthermore, FCC rules state that the transmitters must not spend more than 0.4 s on anyone channel every 20 s in the 902 MHz band and every 30 s in the upper bands. Since the peak transmission rate for a FHSS system is equal to a single channel's bandwidth, the two upper bands offer the highest peak transmission rate.

FHSS WLANs are very robust to narrowband interference because of the way they use the channel. Consider the case where a 2.4 GHz FHSS WLAN operates in the presence of 2 MHz narrowband interference. It is obvious that errors will occur only when the system hops to frequencies within the polluted 2 MHz. Since the 2.4 GHz band is 83.5 MHz wide, one concludes that the overall error rate will be very small. Furthermore, an intelligent FH system can replace the polluted channels with new ones. It can choose to use a new hop pattern that contains either a subset, or none, of the polluted channels. This way it can continue to operate in the presence of interference experiencing only small performance degradation.

Another advantage of FHSS WLANs is that they can operate simultaneously in the same geographical area. This is achieved, by setting the WLANs to use orthogonal hopping sequences. Sets of such sequences can be defined, so that the members of each set present optimal cross-correlation properties. The orthogonality property ensures that any two patterns taken from the same set collide at most on a single frequency. As the pattern size can be set to be quite large, multiple FHSS WLANs can operate with acceptable performance in the same area.

The IEEE 802.11 FHSS physical layer specification calls for use of Gaussian frequency shift keying (GFSK) to transmit data either at 1 or 2 Mbps in the 2.4 GHz band. The digital signal is fed into a GFSK modulator, which produces an analog signal centred on a certain frequency. The analog signal is then fed into a FH spreader, which makes use of a pseudorandom number sequence as an index into a table of frequencies. At each successive interval the spreader selects a frequency, which is then modulated by the analog signal produced by the initial modulator. The result, is a signal of the same shape bounded in the frequency channel chosen from the table. Repetition of this procedure produces the frequency-hopped signal. Transmission at 1 Mbps is implemented using two-level GFSK, with a logical 0 transmitted at a frequency of $f_t - f_c$, and logical 1 at $f_t + f_c$. 2 Mbps data transmission is achieved using four level GFSK. The input to the modulator is a combination of two bits. Each of these 2-bit symbols is transmitted at 1 Mbps using the following frequency shifting scheme: Logic 00 is transmitted at $f_t - 2f_c$, logic 01 at $f_t - f_c$, logic 11 at $f_t + f_c$ and logic 10 at $f_t + 2f_c$.

The 802.11 standard describes how to calculate optimal values for f_c. Furthermore, the standard defines three sets, each containing 26 hopping sequences designed to have minimal interference with one another within each set. Thus, BSs can be set to use sequences derived from the same set either to enable WLAN coexistence in the same area or to reduce cochannel interference.

Both the preamble and the header of an 802.11 frame transmitted over an FHSS link are always transmitted at 1 Mbps. The higher rate of 2 Mbps, if employed, modulates only the sent MPDU. The following describes the frame fields:

- SYNC: Consists of 80 alternating 0 and 1's used to synchronize the receiver.

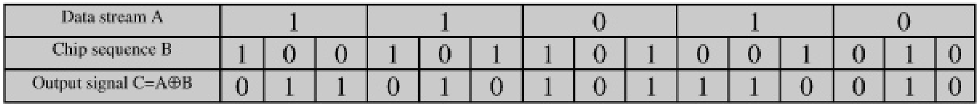
- Start Frame delimiter: A 16-bit field that takes the bit pattern 0000110010111101. It defines the start of a frame.
- PLW: A 12-bit field used to determine the end of the frame.
- PSF: A 4-bit field that takes the values 0000 and 0010 for 1 and 2 Mbps respectively.
- HEC: A 16-bit field used for header error check.
- Whitened MPDU: The MPDU with special symbols stuffed every 4 bytes in order to minimize dc bias of the received signal. The size of this field ranges form 0 to 4096 octets.

4.3.2. The direct sequence spread spectrum physical layer. Using direct sequence spectrum spreading, each bit in the original signal is represented by a number bits in the spread signal. This can be done by binary multiplication (XOR) of the data bits with a higher rate pseudorandom bit sequence, known as chipping code. The resulting stream has a rate equal to that of the chipping code and is fed into a modulator, which converts it to analog form in order to be transmitted. The ratio between the chip and data rates is called the spreading factor and typically has values between 10 and 100 in modern commercial systems. This technique spreads the signal across a frequency band with a width proportional to the spreading factor. Figure 9 shows a binary data stream, a pseudorandom sequence having three times the rate of the data stream, and the resulting spread signal. Figure 10 depicts the demodulation of the spread signal at the receiver.

The actual data rate of the DS spread signal lowers with an increasing spreading factor. FCC specifications, state that in order for a DSSS product to operate in the ISM bands, a spreading factor of at least 10 must be used. For example, if a DSSS WLAN operates at a C MHz wide channel using a spreading factor of 10, the actual data rate cannot exceed $C/10$. On the other hand, a narrowband system can achieve data rates up to C. While seemingly wasteful of bandwidth, DSSS has the significant ability to extract a signal from a background of narrowband interference and noise, a fact that results in fewer retransmissions, thus enhancing throughput.

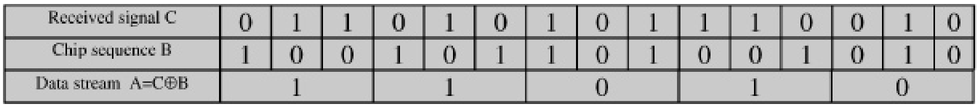
DSSS WLANs present a lower potential for interference cancellation than do FHSS ones. Returning to the example of the previous paragraph, we assume a DSSS WLAN operation occupying a 27 MHz wide channel. If the 2 MHz of noise is contiguous in the spectrum, the system can choose one of the other 27 MHz channels and continue to operate without experiencing interference. However, if the interfering source pollutes four non-adjacent 0.5 MHz channels the DSSS WLAN cannot totally avoid interference in any case.

DSSS also has the ability to accommodate a number of simultaneously operating WLANs. Some DS WLANs may be designed to use less than the total available bandwidth. In such a case,



Data stream A	1			1			0			1			0		
Chip sequence B	1	0	0	1	0	1	1	0	1	0	0	1	0	1	0
Output signal C=A⊕B	0	1	1	0	1	0	1	0	1	1	1	0	0	1	0

Figure 9. DSSS modulation.



Received signal C	0	1	1	0	1	0	1	0	1	1	1	0	0	1	0
Chip sequence B	1	0	0	1	0	1	1	0	1	0	0	1	0	1	0
Data stream A=C⊕B	1			1			0			1			0		

Figure 10. DSSS demodulation.

additional WLANs using the remaining free channels can be admitted in the same geographical area. Nevertheless, as the number of DSSS sub-channels is small, the number of collocated DSSS WLANs is generally smaller than in the FH case.

The IEEE 802.11 DSSS physical layer specification identifies the 2.4 GHz band for operation and divides the available bandwidth in 11 MHz wide sub-channels using a chip sequence of rate 11 to spread each symbol. The specification uses binary phase shift keying (BPSK) to transmit the spread digital data stream at 1 Mbps. BPSK shifts the phase of the carrier frequency in order to represent different symbols. In the case of transmission at 2 Mbps, quadrature phase shift keying (QPSK) is used to transmit pairs of two bits at a rate of 1 Mbps thus achieving 2 Mbps data rate. Of course, since the specification calls for a chip rate of 11, the actual transmitted DSSS signal has a rate of 11 Mbps. Multiple networks can coexist in the same area provided that they use sub-channels with centre frequencies separated by at least 30 MHz in order to avoid interference.

Extending the DSSS physical layer specification, the IEEE 802.11b standard supports 11 Mbps operation with fallback rates of 5.5, 2, and 1 Mbps, in the 2.4 GHz frequency band. The modulation technique used is complementary code keying (CCK). CCK is the mandatory mode of operation for the standard, and is derived from the direct sequence spread spectrum (DSSS) technology. The extension is backward compatible with legacy 802.11 systems.

Both the preamble and the header of a frame transmitted over an 802.11b link are always transmitted at 1 Mbps. The higher rates, if employed, modulate only the sent MPDU. The following describes the frame fields:

- *SYNC*: Contains alternating pulses in consecutive time slots. It is used for receiver synchronization. The size of this field is 128 bits.
- *Start frame delimiter*: A 16-bit field defining the beginning of a frame.
- *Signal*: A 8-bit field that indicates 1, 2, 5.5, or 11 Mbps operation.
- *Service*: A 8-bit field reserved for future use.
- *Length*: A 16-bit field containing the length of the MPDU in msec.
- *FCS*: An 8-bit frame check sequence used for error detection.
- *MPDU*: The 802.11 MAC protocol data unit to be sent. It has adjustable maximum length.

4.3.3. The narrowband microwave physical layer. An alternative to spread spectrum is narrowband modulation. Until recently, all narrowband WLAN products had to use licensed parts of the radio spectrum. However, today's products can either use the newly released parts of the spectrum where licensing is not needed, or use the ISM bands without implementing spectrum spreading. The latter is permitted only if the narrowband transmission is of low power (0.5 W or less).

A narrowband WLAN has generally the opposite characteristics of a spread-spectrum one. It is more vulnerable to fading than a spread spectrum one. However, interference is not common in case of WLANs that license their operating bandwidth. Licensing also ensures proper operation of collocated WLANs. Finally, the peak data rate of a narrowband WLAN operating in a channel of bandwidth C, is generally higher than the one of a spread spectrum one. A DSSS WLAN achieves peak data rates of $C/10$ and a FHSS one has a peak data rate that equals its sub-channel's bandwidth, while a narrowband WLAN can achieve a peak data rate of C.

HIPERLAN 1 uses narrowband modulation in the 5 GHz band. It divides the available bandwidth into five channels with center frequencies separated by 23.5 MHz. The standard defines two data rates. The lower one is at 1.47 Mbps and is used to transmit control information using frequency shift keying (FSK) modulation. The higher data rate, at 23.4 Mbps, is used for data transmission and uses Gaussian minimum shift keying (GMSK) modulation. The physical layer adds to the MPDU the lower data rate header, 450 high rate training bits used for channel equalization, 496*n* high rate bits of payload and a variable number of padding bits. The equalization training bits are necessary in order to support the higher data rate in the presence of ISI. However the standard does not define the equalizing technique leaving it to each implementation.

4.3.4. The orthogonal frequency division multiplexing (OFDM) physical layer. Both IEEE 802.11a and HIPERLAN 2 operate in the 5 GHz bands and use orthogonal frequency division multiplexing (OFDM) to spread the transmitted signal over a wide bandwidth. OFDM is a form of multi-carrier transmission and divides the available spectrum into many carriers, each one being modulated by a low rate data stream using PSK. OFDM resembles FDMA in that the multiple user access is achieved by subdividing the available bandwidth into multiple channels, which are then allocated to users. However, OFDM uses the spectrum in a more efficient way by spacing the channels much closer. This is achieved by making all the carriers orthogonal to one another, preventing interference between the closely spaced carriers. Each carrier is of a very narrow bandwidth, which means that its data rate is slow. Figure 11 shows the spectrum for an OFDM transmission.

The spectrums of the sub-carriers are not separated but partially overlap. However, the transmitted information can still be recovered due to the orthogonality relation, which gives the method its name. The spacing of the sub-carriers is implicitly chosen in such a way that at the frequency where the received signal is evaluated (indicated as arrows), all other signals are zero. However, in order for the technique to work perfect synchronization between the receiver and the transmitter is required.

OFDM effectively combats ISI. The OFDM symbols are artificially prolonged by periodically repeating the ‘tail’ of the symbol and precede the symbol with it. At the receiver, this so-called ‘guard interval’ is removed again. As long as the length of this interval is longer than the maximum channel delay all reflections of previous symbols are removed and the orthogonality is preserved. However, by preceding the useful part of length by the guard interval we lose some parts of the signal that cannot be used for transmitting information.

In both HIPERLAN 2 and 802.11a multiple data rates are supported ranging from 6 to 54 Mbps. The mandatory data rates for 802.11a are 6, 12, and 24 Mbps. Depending upon the data rate, BPSK, QPSK, 16 QAM, or 64 QAM modulation is employed with OFDM in both standards.

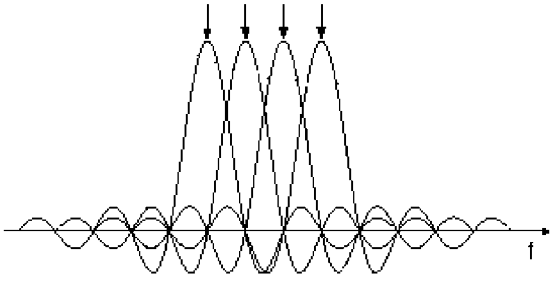


Figure 11. Detection of OFDM symbols.

5. THE MEDIUM ACCESS CONTROL (MAC) LAYER

MAC protocols can be roughly divided into three categories: fixed assignment (e.g. TDMA, FDMA), random access (e.g. ALOHA, CSMA/CD, CSMA/CA) and demand assignment protocols (e.g. polling, token ring, PRMA). Fixed assignment protocols fail to adapt to changes in network topology and traffic and thus exhibit low performance in wireless data applications. Random access protocols however, operate efficiently both without topology knowledge and under changing traffic characteristics. Nevertheless, their disadvantage is their non-deterministic behaviour, a fact that causes problems in supporting QoS guarantees. Demand assignment protocols try to combine the advantages of fixed and random access protocols. However, knowledge of the network's logical topology is required in most cases. The latter, as mentioned, is hard to achieve in WLANs since fading and user mobility result in dynamically changing topologies. The token-based approach is generally thought to be inefficient. This is due to the fact that in a WLAN, token losses are much more likely to appear due to the increased BER of the wireless medium. Furthermore, in a token passing network, the token holder needs accurate information about its neighbors and thus of the network topology. In fact, the inefficiency of token passing was the reason the IEEE 802.4 Working Group, initially responsible for WLAN standardization, suggested the development of an alternative standard for WLANs. As a result, the IEEE 802.11 Working Group appeared in the late 1980s.

In the following paragraphs we examine the MAC layer of ETSI RES10 HIPERLAN 1 and IEEE 802.11. As mentioned earlier, collision detection is very difficult to implement in a WLAN receiver. Therefore, both of these standards employ CSMA/CA which reduces the probability of collisions. 802.11 includes an option that supports time-bounded applications. HIPERLAN 1 also supports time-bounded packet delivery by using an integrated priority mechanism. Issues like security, power saving and supported topologies are also discussed. Finally, two polling protocols, the randomly addressed polling protocol (RAP) and its variation, group RAP (GRAP), are presented.

5.1. The HIPERLAN 1 MAC layer

The HIPERLAN 1 standard was released in 1995 aiming to define a WLAN technology of equal performance to that of traditional wired LANs being capable of supporting isochronous services. Unlike the IEEE 802.11 standard, the HIPERLAN committee was not driven by existing technologies and regulations. A set of requirements was set and the committee started working in order to satisfy them. The standard covers the Physical and MAC layers of the OSI model.

The HIPERLAN 1 project, has defined the system architecture shown in Figure 12. It divides the functions of the medium access control into two sub-parts, which it refers to as channel access and control (CAC) and MAC layers. The CAC layer defines how a given channel access attempt will be made depending on whether the channel is busy or idle, and at what priority level the

<table>
<tr><td>Lookup</td><td>Routing</td><td>Power saving</td><td>Priority mechanism</td></tr>
<tr><td colspan="4">MAC</td></tr>
<tr><td colspan="4">Channel Access (EY-NPMA protocol)</td></tr>
<tr><td colspan="4">Physical Layer</td></tr>
</table>

Figure 12. HIPERLAN 1 system architecture.

attempt will be made, if contention is necessary. The HIPERLAN MAC layer defines the various protocols which provide the HIPERLAN features of power conservation, lookup, security, and multi-hop routing, as well as the data transfer service to the upper layers of protocols. The routing mechanism supports the ability of HIPERLAN nodes to forward packets to stations out of their range with the help of intermediate forwarding stations. The lookup functionality enables collocated operation of more than one HIPERLAN networks. Finally, the standard supports priorities, power conservation and support for encryption.

5.1.1. The priority mechanism and QoS support. Although the HIPERLAN 1 standard does not define different priorities for the various traffic classes, like voice or multimedia, it tries to support time-bounded delivery of packets. HIPERLAN 1 dynamically assigns channel access priorities to packets by taking into account the packet's lifetime and its MAC priority. The MAC priority of a packet can be either normal or high, with normal being the default value. Every packet is generated with a specific lifetime ranging from 0 to 32767 ms, with the default value set at 500 ms. Packets that cannot be delivered within the allocated lifetime are dropped. The residual lifetime of a packet in combination with its priority defines the packet's channel priority. Therefore, as time expires, the channel priority of each packet increases. Channel priority values range from 1 to 5, with priority p being higher than priority $p+1$. This mechanism is used by HIPERLAN 1 to support time bounded applications.

5.1.2. The HIPERLAN 1 MAC protocol. In HIPERLAN 1, a station can immediately commence transmission after sensing an idle medium for a duration of 1700 high rate bit times. However, even under moderate loads the above criterion is hardly ever fulfilled. When a station senses the medium busy, it waits until it becomes idle and then the Elimination Yield-Non-Preemptive Priority Multiple Access (EY-NPMA) Protocol is applied. After the end of the detected transmission, all stations that want to transmit wait for another 256-bit period which is called a synchronization slot. Then, the EY-NPMA protocol is applied, which comprises the following phases:

- *The prioritization phase*: This phase is 1–5 slots long and each slot has a 256 high rate bit time duration. A station having to transmit a packet with channel priority p transmits a burst at slot $p+1$, if it has not already sensed a higher priority burst from another station. Stations that sense higher priority bursts are dropped from contention and have to wait either for the next synchronization slot or for a 1700 bit idle period.
- *The elimination phase*: This phase consists of 1–13 slots each one being 256 high rate bits long. In this phase, stations that transmitted a burst during the previous phase, now contend for access to the medium. Each station transmits a burst for a geometrically distributed number of slots and then senses the medium for an additional slot. If it detects another burst during this slot, it stops contending for the channel, if not it proceeds to the next phase. Thus stations that transmitted the longest burst and halted at the end of the same slot proceed to contend for access to the channel. The probability of a station's burst being of i slots, ($i < 12$), is 0.5^{i+1}.
- *The yield phase*: This phase consists of 1–15 slots each one being 64 high rate bits long. Stations that make it to this phase defer for a geometrically distributed number of slots while sensing the channel. The probability of backing off by j slots is 0.1×0.9^{j}. The station that waits the less seizes the channel and commences transmission. All other stations that made it to this phase sense the winner's transmission and wait until the next synchronization slot.

The purpose of the elimination phase is to reduce the contending stations and the yield phase tries to ensure that in the end, a single-station gains access to the channel. According to the HIPERLAN 1 committee, the chances of two or more stations surviving all three phases (a fact that results in collision) are less than three per cent. EY-NPMA simulation results in Reference [14] show typical performance for a contention protocol:

- Increased performance for increasing packet sizes, since the larger the packet size, the less significant is the overhead added by the contention period.
- Decreasing throughput and increasing mean delay for increasing number of stations.

Finally, overall throughput in HIPERLAN 1 is shown to be affected by the hidden terminal scenario, with increased intensity at high overall loads. The HIPERLAN 1 specification does not address this problem.

The combination of the EY-NPMA protocol and the priority mechanism supports time-bounded delivery of packets. It has to be noted however, that time bounded does not mean QoS. HIPERLAN 1 just favours high-priority packets, it cannot allocate a fixed portion of bandwidth to a particular application. From this point of view, it is just a best-effort network. Simulations in Reference [14] show that for a small number of high-priority stations, increasing lower-priority traffic does not affect the overall high-priority throughput. However, increased numbers of high-priority stations are likely to damage this good behaviour, since with many high-priority stations active, no mechanism for QoS establishment exists.

5.1.3. Supported topologies and multi-hop routing. HIPERLAN 1 supports both infrastructure and ad hoc topologies. Furthermore, the standard supports multi-hop configurations, where a station can transmit a packet to another station out of its radio range without the need of additional infrastructure. This can be achieved with the help of intermediate stations that can forward packets destined for other stations. Each HIPERLAN 1 station will select one and only one neighbour as its forwarder and transmit all packets destined for stations out of its range to the forwarder. Forwarded packets are relayed from forwarder to forwarder until they reach their destination. This means that a forwarder needs to know the network topology and maintain and dynamically update routing databases. However, it is optional for a station to forward packets. A station can announce its decision not to forward packets and become a non-forwarder. Non-forwarders are required to know only their direct neighbours.

Forwarding in a WLAN poses some problems. First of all, a forwarder needs to have a consistent image of the network topology at every moment. Since common routing algorithms are not designed for dynamically changing topologies, new algorithms need to be developed. Furthermore, maintenance of routing databases at a forwarder demands periodic exchange of information with its neighbours, a fact that limits the useful bandwidth of the channel.

Another problem arises due to the increased BER that characterizes wireless links. As a forwarded packet will travel over more than one such link, it is more likely to be corrupted or not arrive at all. Moreover, forwarding relies on the presence of stations willing to donate resources and processing power to serve other stations. Consequently, in a limited-resource HIPERLAN 1 environment it is likely that forwarders are few. Simulations of forwarding topologies in HIPERLAN 1 [14] depict decreased throughput performance when compared to a fully connected HIPERLAN 1 topology.

5.1.4. Power saving. The HIPERLAN 1 standard supports power saving by using both hardware-specific and protocol-based techniques. The first method relies on the existence of the two transmission speeds. As mentioned, the header of each packet is transmitted in the lower 1.47 Mbps rate. A node that hears a packet destined for another station can shut down the error correction, channel equalization and other receiver circuits until it receives a packet destined for itself.

Using the second power saving method, known as the p-saver method, a node can announce that it only powers up to receive incoming packets periodically. All other stations wishing to transmit to it, known as p-supporters, transmit to the p-saver only when it listens. A p-supporter may be an ordinary HIPERLAN device or a forwarder. As far as multicasts are concerned, p-supporters relaying multicasts announce their schedule for doing so, thus giving p-savers the option to power up in order to receive the multicast packets. P-saver schedules can be re-declared at any time in order to reflect new requirements.

5.1.5. Security. The MAC layer offers the ability to encrypt the transmitted MPDU. Each HIPERLAN packet carries a 2-bit field in the payload header that tells whether the payload is encrypted or not. If it is, the header identifies one of three possible keys. The standard defines a small set of keys, however the key distribution mechanisms are not defined.

The HIPERLAN 1 security algorithm operates as follows:

- At the transmitter, the key is XORed with a random bit sequence of equal length. Both are 30 bits. The resulting 30-bit value is used as input to a random number generator that outputs a bit stream of length equal to the MPDU length. The two bit streams are again XORed to produce the encrypted data.
- The encrypted MPDU is encapsulated into a physical layer frame and transmitted to the destination. The key and the encrypted data are transmitted within the packet to the destination.
- Upon extraction of the encrypted MPDU at the destination, the process is executed in reverse and the unencrypted data is obtained.

5.2. The IEEE 802.11 MAC layer

The IEEE 802.11 standard covers the physical and MAC layers of the OSI model. It defines a single MAC layer for use with all the aforementioned 802.11 physical layers. There was considerable discussion within the committee before release of the final standard. The MAC protocol used is a CSMA/CA protocol called distributed foundation wireless MAC (DFWMAC) and is very similar to the IEEE 802.3 Ethernet LAN line standard. DFWMAC, also referred to as the distributed co-ordination function (DCF), only offers a best-effort service. However, the 802.11 Working Group included optional support for time-bounded services through the use of a contention-free mechanism. This service is known as the point co-ordination function (PCF) and is offered only in 802.11 infrastructure networks.

The 802.11 Working Group has defined the system architecture shown in Figure 13. DCF operates on top of the physical layer providing ordinary asynchronous traffic. PCF is built on top of the DCF and uses services offered by the DCF to provide contention-free traffic. The IEEE 802.11 MAC layer also offers mechanisms for authentication and privacy, encryption and power saving.

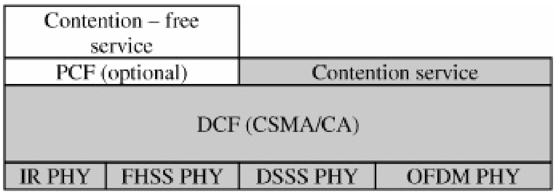


Figure 13. The IEEE 802.11 system architecture.

5.2.1. The 802.11 MAC protocol

Distributed co-ordination function: The DCF sublayer uses a slotted CSMA/CA algorithm Thus, data transmissions can only start at the beginning of each slot. The IEEE 802.11 standard utilizes a set of delays, known as interframe spaces (IFS). The steps taken for channel access are as follows:

- When a station has a packet to transmit, it first senses the medium. If the medium is sensed idle for an IFS, then the station can commence transmission immediately.
- If the medium is initially sensed busy, or becomes busy during the IFS, the station defers transmission and continues to monitor the medium until the current transmission is over.
- When the current transmission is over, the station waits for another IFS, while monitoring the medium. If it is still sensed idle, the station backs off a number of slots using a binary exponential backoff algorithm and again senses the medium. If it is still free, the station can commence transmission.

Of course, two or more stations can select the same slot to commence transmission, a fact that results in a collision. The actual size of the slot is physical layer dependent and is defined to be, at least, equal to the sum of the transmitter turn-on time plus busy medium detection time plus the maximum propagation delay between any two stations. This selection for the slot time ensures that collisions occur only when two or more stations select the same slot to transmit, as knowledge of a transmission commenced at slot k is propagated over the network before the start of slot $k + 1$. For the FHSS implementations, the slot time is 28 μs whereas in DSSS implementations it is 10 μs.

DCF uses three IFS values in order to enable priority access to the channel (Figure 14). These are, from the shortest to the longest, the Short IFS (SIFS), the point co-ordination function IFS (PIFS) and the distributed co-ordination function IFS (DIFS). Their actual durations are defined by the slot duration and are thus physical layer dependent. Weinmiller *et al.* [14] provides simulation results of the performance of the IEEE 802.11 DCF over three 802.11 physical layer specifications, concluding that end performance is dependent on the value of the slot time. The infrared (IR) physical layer shows better performance than the direct sequence spread spectrum (DSSS) one which in turn is proved to be superior to the frequency hopping spread spectrum (FHSS) physical layer.

DIFS is the minimum delay for asynchronous traffic contending for medium access. PIFS is used by the PCF portion of the MAC layer. Since it is shorter than DIFS it gives the polling co-ordinator (PC) the ability to lock out asynchronous traffic and allocate bandwidth for time

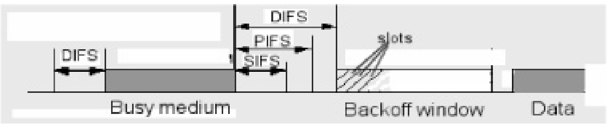


Figure 14. DCF operation.

bounded operations. The Point coordination Function is discussed later. SIFS is used in conjunction with the following 802.11 MAC operations:

- *MAC level acknowledgment* (ACK): When a station receives a frame destined only for itself it responds with an ACK frame after waiting only for a SIFS. Thus, a station acknowledging a received frame has to wait less time than stations trying to transmit packets. As a result, the acknowledging station is favoured to gain access to the medium. MAC level acknowledgment provides for efficient collision recovery, since collision detection is not implemented in IEEE 802.11. When an ACK is not received for a transmitted frame, the transmitting station assumes a collision occurred and recontends for the channel.
- *Fragmentation*: MAC frames are passed down from the logical link control (LLC) sublayer to the MAC layer. The MAC layer can choose to fragment unicast packets in order to increase transmission reliability. Unicast packets of size greater than the user manageable parameter *Fragmentation_Threshold*, are fragmented into multiple packets of size *Fragmentation_Threshold* and transmitted sequentially to the destination. Upon receipt of the first fragment, the destination waits for a SIFS and transmits an ACK. Upon reception of the ACK the source station immediately (after SIFS) sends the next fragment. As a result, the source station seizes the channel until all of the packet's fragments have been delivered.
- *RTS/CTS*: This mechanism enhances the two-way handshake CSMA/CA algorithm (DATA-ACK) to a four-way handshake one (RTS-CTS-DATA-ACK). When a station wants to transmit a packet, it sends a small request to send (RTS) packet to the data packet destination. The latter, if ready to receive the data packet, responds after a SIFS with a clear to send (CTS) packet allowing the sending station to commence data transmission a SIFS after the CTS reception.

The RTS/CTS mechanism tries to combat the hidden terminal problem. The RTS and the CTS packets inform the neighbours of both communicating nodes about the length of the ongoing transmission. Stations hearing either the RTS or the CTS packet defer until the DATA and ACK transmissions are completed. RTS and CTS packets are very small (20 and 14 bytes, respectively) compared to the maximum 802.11 data frame (2346 bytes). As a result, when a collision between RTS or CTS packets occurs, less bandwidth is wasted when compared to collisions involving larger data frames. However, the use of the mechanism in a lightly loaded medium or in environments that are characterized by small data packets imposes additional delay due to the RTS/CTS overhead.

The use of the RTS/CTS mechanism is optional. RTS/CTS usage can be asymmetrical inside the same WLAN as only a subset of the WLAN nodes may decide to use the mechanism. A station can choose to never use RTS/CTS, use RTS/CTS when the data frame to be transmitted exceeds a certain user-defined value (called the RTS threshold) or always use RTS/CTS. Simulations in Reference [15] identify that the RTS threshold value that leads to optimal network performance is not constant, but depends on the length of the preamble added by the physical layer. The optimal value for the RTS threshold increases for increased preamble length.

The collision avoidance part of the protocol is implemented through a random backoff procedure. As mentioned, when a station senses a busy medium, it waits for an idle DIFS period and then computes a backoff value. This value consists of a number of slots. Initially, the station computes a backoff time ranging from 0 to 7 slots. When the medium becomes idle, the station decrements its backoff timer until it reaches zero, or the medium becomes busy again. In the latter case, the backoff timer freezes until the medium becomes idle again. When two or more station counters decrement to zero at the same time, a collision occurs. In this case, the stations compute a new backoff window given in slots by the formula $[2^{2+I}$ *ranf()] *Slot_time, where i is the number of times the station attempts to send the current data frame, ranf() a uniform variate in (0,1) and $[x]$ the largest integer less than or equal to x. Successive collisions cause the size of the backoff window, also known as contention window (CW) to increase exponentially. When it reaches a certain maximum, which is a user defined parameter known as CWMax, i is reset to 1 and the size of the backoff window is reinitialized to 7. When a certain number of retransmissions occurs for a specific frame, the frame is discarded.

However, consider the case of two stations, A and B, competing for access to the medium. A has either newly entered the competition or selects a backoff time due to a collision that occurred during its last transmission. Therefore, A selects a backoff value between 0 and CW. B however, deferred a few slots ago and decrements its backoff timer when it senses the medium to be idle. Assume that B's backoff timer has decremented to a value of K slots ($0 < K < \mathrm{CW}$) when A selects its backoff value. It is obvious, that the slots between 0 and K have a higher probability of being chosen. This is due to the fact that although A uniformly selects slots between 0 and CW, the remaining backoff value for B can range only between slots 0 and K. Therefore, the backoff algorithm does not efficiently assign slots to competing stations and the increased selection likelihood of 'early' slots leads to increased collisions. This scenario is depicted in Figure 15. [15] proposes two algorithms that try to distribute contention slots to users in a uniform way. Stations that newly enter the competition select 'late' slots with higher probability, thus reducing collisions.

Simulation results [13,15–17] of DFWMAC reveal that under a fairly noiseless medium ($\mathrm{BER} = 10^{-6}$) maximum throughput can reach satisfying percentage values, higher than those achieved for the same number of stations by HIPERLAN 1. However, the higher data rate offered by the physical layer of HIPERLAN 1 translates to higher transmission rates.

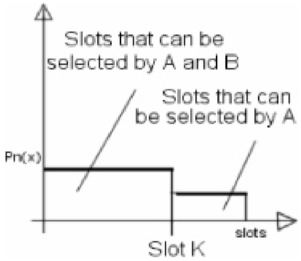

Slots that can be selected by A and B
Slots that can be selected by A
Pn(x)
slots
Slot K

Figure 15. Slot selection probabilities. B is continuing a previous backoff and A newly enters the competition.

In a noiseless medium the use of large Fragmentation_Threshold values is preferable. This is due to the fact that for increased packet sizes, the resulting protocol overhead is not significant. Under harsh fading (BER $= 10^{-3}$) the protocol's performance drops sharply. Under such conditions the use of small Fragmentation_Threshold values is preferable, as smaller packets are more likely to be transmitted without suffering errors. Being a random access protocol, DFWMAC peak performance decreases as the number of WLAN nodes increases. This is due to increased contention that leads to more collisions. Finally, the hidden terminal scenario greatly affects the performance of DFWMAC. Simulations in Reference [17] show that when the number of hidden pairs exceeds 10 per cent, the protocol's performance drops sharply. However, significant performance improvements are achieved when using the RTS/CTS mechanism to reserve bandwidth for frame transmissions. Although the problem is not completely solved, 802.11 has an advantage over HIPERLAN 1 which does not address the hidden terminal problem at all.

Point co-ordination function: PCF is an optional access method that supports isochronous, contention-free traffic and is built on top of the DCF. PCF is implemented only in infrastructure 802.11 WLANs. It operates by polling with a centralized polling master, known as the point co-ordinator (PC), which is usually the AP inside a cell. The PC makes use of the PIFS mentioned before. Since PIFS is smaller than DIFS, the PC can lock out all asynchronous traffic while it polls stations and receives responses. To avoid complete seizure of the medium by the PC, the 802.11 standard defines an interval known as the superframe. The first part of this interval serves contention-free traffic, while at the second part, the PC remains idle so as to give stations the chance to contend for medium access using DCF. During each PCF period, the PC polls stations demanding isochronous service. These stations are known as contention-free period (CFP) aware stations. A station that chooses not to participate in the CFP is called a non-CFP-aware station. The superframe structure is depicted in Figure 16. If at the end of the superframe the medium is busy, the PC has to wait until it becomes idle again in order to seize it. As a result, the next superframe is of reduced size.

Several user-definable parameters govern the joint operation of DCF and PCF. The contention free-period repetition interval, (CFP_Rate) defines the nominal superframe length. The CFP maximum duration (CFP_ Max_Duration) determines the maximum duration of the PCF. It can take a value no larger than the one that limits the DCF to transmit only a maximum size data frame successfully using the RTS-CTS-DATA-ACK mechanism. At the beginning of each superframe, the PC senses the medium. If the medium is idle for a PIFS period, the PC transmits the CFP_Rate and CFP_Max_Duration using a Beacon frame. Stations that hear the Beacon frame defer until the CFP ends. The CFP can be terminated before the expiration time

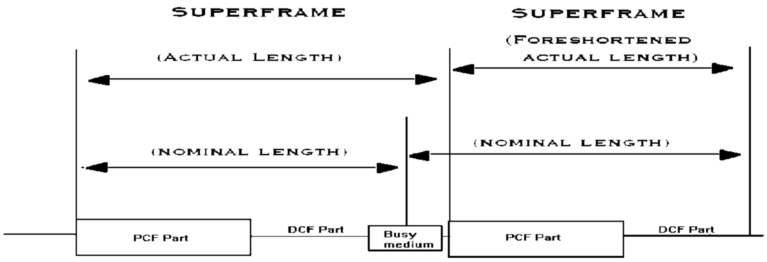


Figure 16. The superframe structure.

determined by CFP_Max_Duration. This can happen when all CFP-aware stations have transmitted their isochronous traffic. In this case, the PC terminates the CFP by transmitting a CFP-END frame.

The PC polls a CF-aware station by sending it a CF-POLL frame. The station then responds by broadcasting either a CF-ACK frame, or a CF-ACK + DATA frame. In the first case, the PC receives a single acknowledgment of the CF-POLL receipt since the polled station does not have isochronous traffic buffered. Users who are idle repeatedly are removed from the poll cycle after k polls and are polled again at the beginning of the next CFP. In the second case, the PC receives a packet containing both the acknowledgment and data. In this case, the PC can resume polling by transmitting either a Data + CF-ACK + CF-POLL or a CF-ACK + CF-POLL frame. The CF-ACK part of the frame acknowledges the receipt of the previous data frame sent to the PC and the CF-POLL part is used to poll the next station. Of course, a CF-aware station can also send isochronous data to stations other than the PC. In this case, the destination station transmits a DCF acknowledgment to the source and the PC resumes polling a PIFS interval after the receipt of the DCF ACK. The combined polling and data transmission mechanism reduces protocol overhead and increases CFP performance.

The PCF portion which 802.11 offers supports time-bounded applications better than HIPERLAN 1, as the polling mechanism guarantees transmission time to stations requesting it. However, when the number of stations requesting contention-free service increases, the polling algorithm must decide either to reduce the bandwidth offered to each station or deny contention-free service to some stations. The 802.11 standard however does not define the implementation of the polling algorithm and leaves it to the PC implementor. Joint simulations of the DCF and PCF in Reference [16] reveal that setting k to 1 is optimal when all time-bounded data are voice data streams. This is explained by the fact that in relation to the duration of the CFP, voice streams are sent in slow on-off bursts.

5.2.2. Supported topologies. The 802.11 standard supports both infrastructure and ad hoc network configurations. Infrastructure networks comprise one ore more cells that contain mobile nodes. The mobile nodes access the backbone network, referred to as the Distribution System (DS) in 802.11 terminology, via APs. The set of stations associated with a given AP forms this AP's basic service set (BSS). Two or more BSSs are interconnected using a DS. The 802.11 protocol does not define a specific DS. As a result, technologies like 802.x wired LANs, ATM or even another WLAN may be used as a DS.

The interconnection of multiple BSSs via the DS is called an extended service set (ESS). Inside an ESS, data moves between BSSs through the DS. An ESS appears as a single logical WLAN to the LLC layer. An ad-hoc network, having no AP, is called an independent basic service set (IBSS). The standard allows infrastructure and ad-hoc topologies to coexist.

The BSSs inside an ESS can be disjoint, overlap or be physically collocated. Disjoint BSSs offer the advantage of reduced interference, paying however the price of lack of continuous coverage. The reverse holds for BSSs that overlap. Finally, physically collocated BSSs can be used to form a higher performance WLAN. For example, multiple FHSS 802.11 WLANs using orthogonal hopping sequences might operate in the same geographical area to provide higher aggregate throughput.

The 802.11 standard identifies the following three mobility types: no-transition, BSS-transition, and ESS-transition. The first type refers to nodes that either move inside a single BSS or do not move at all. The second type refers to nodes that roam from one BSS to another BSS while remaining in the same ESS. The third type refers to nodes that roam from a BSS in one ESS to a BSS in a different ESS. The 802.11 standard supports the first two types of mobility. However, it does not specify how roaming is performed, leaving this task to product implementors.

Stations inside a BSS must remain synchronized in order for the MAC protocol to function properly. In infrastructure networks, the AP periodically transmits beacon frames that contain synchronization information, such as the hopping sequence that is used inside the BSS and timing information. In case of IBSS networks, all stations periodically send beacon frames for synchronization purposes.

5.2.3. Security. The 802.11 standard defines two security procedures. The first one allows for encrypted frame transmissions, in a way similar to the one implemented by HIPERLAN 1. Encryption is implemented by using the wired equivalent privacy (WEP) algorithm, which implements symmetric encryption. The WEP algorithm generates secret shared keys that can be used by both source and destination nodes to encrypt and decrypt data transmissions. However, the standard does not define the process of installing keys in stations.

The steps taken to encrypt a frame are the following:

- At the sending station, the WEP generates a 32-bit integrity value for the payload of the MAC frame. This value is used to alert the receiving station of possible data modification.
- A shared encryption key is used as an input to a pseudorandom number generator to produce a random bit sequence of length equal to the sum of the lengths of the MAC payload and the integrity value. Those fields are then encrypted by binary multiplication (XOR) with the produced bit sequence.
- The sending station places the encrypted MAC payload inside a MAC frame and hands it down to the Physical layer for transmission.
- At the receiving station, the WEP algorithm uses the same key to decrypt the MAC payload and calculates an integrity value for the MAC payload. If the calculated value is the same with the one sent with the frame, it passes the MAC payload to the LLC.

The second security procedure concerns authentication between two communicating stations. Two authentication procedures are defined: open system authentication and shared key authentication. The open system authentication procedure, is a two way handshake mechanism and is used when a high level of security is not required. Using this procedure, a station announces its desire to communicate with another station or AP by transmitting to it an authentication frame. The receiving station responds with another Authentication frame that identifies success or failure of the authentication.

Shared key authentication, is a four-way handshake mechanism, which uses the WEP algorithm. The process steps are as follows:

- The requesting station sends an authentication frame to another station.
- Upon reception of an authentication frame, a station responds by transmitting another authentication frame containing a sequence of 128 bytes.
- The requesting station encrypts the received sequence using the WEP algorithm and sends it to the responding station.
- At the receiving station the bit sequence received is decrypted. If the decrypted sequence matches the one sent to the requesting station, the latter is informed of successful authentication.

5.2.4. Power saving. The 802.11 standard supports power saving by buffering of traffic at the transmitting stations. When a mobile node is in sleep mode, all traffic destined to it is buffered until the node wakes up. In an infrastructure network, mobile nodes periodically wake up and listen to beacons sent by the access point. A station that hears a beacon indicating that the AP has buffered data for that station wakes up and requests reception of the data. In ad-hoc networks, stations that implement power saving, wake up periodically to listen for incoming frames.

5.3. The RAP and GRAP MAC protocols

As mentioned earlier, demand assignment protocols try to combine the advantages of fixed and random access protocols. However, special effort is needed, as knowledge of the network's logical topology is required in most cases. The randomly addressed polling (RAP) [2] MAC protocol lifts this requirement by working, not with all the nodes contained in cell, but only with the active ones seeking uplink communication. The RAP protocol assumes an infrastructure cellular topology. Within each cell, multiple mobile nodes exist that compete for access to the medium. The cell's BS initiates a contention period in order for active nodes to inform their intention to transmit packets. For a RAP WLAN consisting of N active stations, the stages of the protocol are as follows:

- *Contention invitation stage*: Whenever the BS is ready to collect packets from the mobile nodes, it transmits a READY message, which may be piggybacked in a previous downlink transmission.
- *Contention stage*: All active mobile nodes generate a random number R, ranging from 0 to $P-1$ and transmit it simultaneously to the BS using a form of orthogonal transmission, such as CDMA or FDMA. The number transmitted by each station identifies this station during the current cycle and is known as its random address. To combat the medium's fading characteristics a station may transmit their generated random numbers up to q times in a single contention stage. When an error-free transmission is assumed, $q=1$ suffices. Optionally, the contention stage may be repeated L times. Each time, stations generate and transmit random numbers as described above.
- *Polling stage*: Suppose that at the lth stage ($1 \leqslant l \leqslant L$) the BS received the largest set of distinct numbers and these are, in ascending order, $R_1, R_2, \ldots, R_n$. The BS polls the mobile nodes using those numbers. When the BS polls mobile nodes with R_k, nodes that transmitted R_k as their random address at the lth stage transmit packets to the BS. Obviously, if two or more nodes transmitted the same random number at the lth stage a collision will occur. If $n=N$ however, no collision occurs.
- If a BS successfully receives a packet from a mobile node, it sends a positive acknowledgment (PACK). If reception of the packet at the BS is unsuccessful either due to noise or a collision, the BS informs the mobile node by sending a negative acknowledgment (NACK). Acknowledgment packets are transmitted right before polling the next mobile node. If a mobile node receives a PACK, it assumes correct delivery of its packet, otherwise it waits for the current polling cycle to complete and retries during the next one.

A complete description of RAP with implementation issues discussed is provided in Reference [18]. Numerical results in References [1,18] show thats increasing values of L yields better throughput results, however, the performance gain with $L > 2$ is very small. As a result a value of 2 for L seems to be a good choice. Comparisons with CSMA show that although the mean delay in RAP also rises rapidly under heavy load, RAP is characterized by smaller delays for a given throughput value. Moreover, by increasing the value of P the delay reduces significantly. If the number of active stations N is significantly less than P, RAP depicts increased throughput and decreased delay.

A critical point seems to be the use of the proper technique for orthogonal transmission of the random numbers. Orthogonal signaling can be implemented using CDMA, transmission in adequate time slots, etc. The use of long sequences for random number transmission is undesirable, since it would increase the overhead of the protocol. However, use of relatively short sequences and large values of P, leads to increased circuit complexity. As a result, values of P around 5, which still provide significant performance gains over conventional protocol are suggested.

A modification of RAP, Group RAP is proposed in Reference [19]. GRAP adopts the super-frame structure, consisting of $P+1$ frames and divides active nodes into groups. At the beginning of each frame only the BS is allowed to transmit. After the BS completes transmission, the polling procedure, begins. However, GRAP does not allow all active nodes to compete in a single contention period. GRAP states that all nodes that successfully transmitted during the previous polling cycles maintain their random addresses and form the groups from 0 to $P-1$. A mobile station joins group j if the random address for its previously successful transmission was j. All the new joining stations form the Pth group. Furthermore, all mobile stations that have time bounded packets can join any group for contention. After the $P+1$ groups have been formed, the polling procedure begins. The members of each group are polled according to the RAP protocol.

An advantage of GRAP is that it allocates much more bandwidth to the BS, a fact that is desirable in infrastructure WLANs. This is because most of the applications in this kind of networks are of client server nature, with the mobile stations being the clients and downlink traffic from the server demanding an increased portion of bandwidth. Another advantage of GRAP (and RAP) is the fact that roaming is easy to implement. Uplink traffic of a roaming station is not of concern, since it can decide to transmit under the co-ordination of the BS with the strongest signal. The case of downlink traffic requires an implementation of a simple tunneling-like technique: For every mobile station, a permanent BS is defined. When a mobile station enters another cell, it notifies its permanent BS about this fact. The BS then tunnels downlink traffic to the mobile station through the BS of its current cell.

6. AN INTRODUCTION TO PERSONAL AREA NETWORKS AND WIRELESS ATM TECHNOLOGIES

6.1. Personal area networks

Personal area networks (PANs) are very small networks covering a reduced geographical space such as office or desktop space. Their main goals are freedom from cables and easy sharing of information between all kinds of wireless devices. The most popular technology in the area, is led by a group of companies that form the Bluetooth group [20–22]. The purpose of the group is to create a *de facto* wireless standard that meets the communication needs of all mobile computing and communication devices, located in a reduced geographical space, regardless of their size or power budget. A Bluetooth radio in these personal devices allows them to communicate using wireless transmission and without line-of-sight restrictions. The Bluetooth group mainly targets the following types of applications:

- *Personal device synchronization*: Automatic data synchronization between mobile wireless equipment such as a mobile phone, notebook PC, etc., that execute similar applications.
- *Ad hoc connectivity*: Transferring files, and other information to another user's Bluetooth-enabled device.
- *Cordless computer*: Wireless interfacing of devices like mice, keyboards, game pads to the computer.
- *Cordless peripherals*: Access to a variety of wireless peripherals including printers, scanners, fax, copier, storage systems, etc.
- *Localized wireless LAN access*: Bluetooth-enabled devices can gain access to services offered by wired LANs through Bluetooth compatible APs.
- *Internet access*: Downloads email or browse a web page using a Bluetooth enabled device, such as a mobile phone.
- *Wireless synchronization*: Synchronization of portable devices with the stationary servers via Bluetooth access points.
- *Cordless telephony/headset*: A user selects a contact name from a handheld, the handheld wirelessly prompts the mobile phone in its proximity to dial the number, and the audio from the call is wirelessly forwarded to the user's headset.

The Bluetooth specification 1.0 was released in July 1999. It defines transmission ranges of 10 m or less using 1 mW FHSS modulation in the 2.4 GHz band, chosen due to its world-wide availability. However, the specification allows for transmission power up to 100 mW, which increases range to about 100 m. The specification is open, which makes it possible for vendors to freely implement their own protocols on the top of the Bluetooth-specific ones.

6.1.1. Bluetooth operation and architecture. Bluetooth devices can communicate as soon as they are within range of one another. However, since the in-range neighbours of a Bluetooth device change with time, a procedure that informs a device about its neighbours is needed. This procedure is carried out by issuing inquiries. Assume three Bluetooth devices, B, C and D are within range of device A which wants to acquire knowledge about its neighbours. To do so, A issues an inquiry, which is received by B, C and D that of course must be enabled to accept inquiries from other radios in their area. Therefore, each Bluetooth device is set to consume 18 time slots (of 0.625 ms duration each) every 1.25 s searching for inquiries. Upon reception of an inquiry, devices reply to A by sending a FHSS packet containing their 48-bit DeviceID and Clock parameters, whose use is described later. If two or more devices simultaneously reply to A, a collision occurs. In this case, the colliding devices wait for a random period of time and then resume listening for inquiries. After the completion of this procedure, device A possesses information of all radios within its range.

When two Bluetooth devices, A and B, connect, the one requesting the connection, also known as the master, pages the other, the slave. Assuming that A is the master and B is the slave, the paging procedure is as follows: A is supposed to possess B's Device ID and an estimate of its Clock parameter. These parameters were made known to A through the inquiry procedure described earlier. To connect to B, A pages B with B's DeviceID. Upon reception of the page, B responds by sending its DeviceID to A. Finally, A transmits to B a packet containing the master's DeviceID and Clock values and connects to B as master.

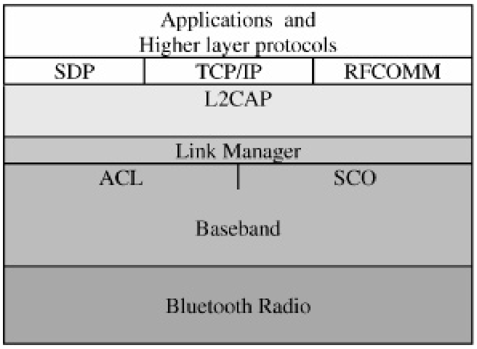


Figure 17. Bluetooth protocol stack.

Each master–slave connection supports symmetrical and asymmetrical transfer rates up 432 and 721 kbps, respectively. A given master can maintain up to seven connections to slaves. As a result, several very small networks, called piconets, can be established. Devices inside a piconet hop together according to the master's DeviceID and Clock parameters. The first parameter defines the hopping sequence used inside the piconet, while the second one is used for synchronization purposes. Piconets can be linked together to form a lager PAN, called a scatternet.

The Bluetooth Protocol stack is shown in Figure 17. Its aim is to provide a common data link and physical layer to applications and high-level protocols that communicate over the Bluetooth wireless link and maximize the re-use of existing protocols at the higher layers. All protocols, except for RFCOMM and TCP/IP are Bluetooth-specific and are referred to as Bluetooth Core protocols. The functionality of each part of the stack is summarized below:

- The Bluetooth radio channel is represented by a pseudorandom hopping sequence hopping through a set of 79 (US and Europe) RF channels spaced 1 MHz apart. The wireless link comprises time slots, 0.625 ms each, with each slot corresponding to a hop frequency. The nominal hop rate is 1600 hops/s. At each hop, the transmitted signal is modulated using GFSK with a binary one being represented by a positive frequency shift and a binary zero by a negative frequency shift.
- The baseband layer enables the wireless link between Bluetooth devices. Being on top of the Bluetooth radio, it essentially acts as a link controller performing operations like link connection and power control. The baseband layer specification states that use of the wireless link in the time domain is slotted. For a pair of communicating Bluetooth devices, the master always starts transmission at even numbered slots while slave transmission is set to be initiated only at odd numbered slots. The baseband layer handles two types of links: synchronous connection-oriented (SCO) and asynchronous connectionless (ACL). A SCO link is a symmetric point-to-point link between a master and a slave. SCO links are maintained by the master using reserved slots at regular intervals. They are mainly used to convey voice information and do not support packet retransmission. ACL links are point-to-multipoint links between the master and all the slaves inside a piconet. An ACL link is used to carry data traffic and is maintained by the master using those slots not reserved for SCO links. SCO and ACL links may be multiplexed over the same wireless link, however only a single ACL link is permitted to exist at any given time. Data or audio transmitted over SCO and ACL links can be provided with different levels of FEC or

CRC and can be encrypted. The baseband layer uses 'Stop and Wait' ARQ to guarantee that a packet is received correctly before the next packet is sent.

- The Link Manager protocol is concerned with link set-up between Bluetooth devices. It offers authentication and encryption services to upper layers that use SCO and ACL links and performs power control operations.
- The logical link and adaptation layer (L2CAP) provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly (SAR) operation, and group abstractions. L2CAP permits higher level protocols and applications to transmit and receive L2CAP packets up to 64 Kilobytes in length. L2CAP only supports ACL links and thus data traffic. Audio data carried in SCO packets is not conveyed through L2CAP and is exchanged directly between the baseband layer of the master and the slave.
- Service discovery protocol (SDP) is used in order for a Bluetooth device to learn about offered services and neighboring device information. Using SDP, neighboring devices can be queried in order for a connection to be established.
- RFCOMM is a serial line RS-232 control and data signal emulation protocol. It is used for cable replacement, offering transport capabilities over the wireless link to applications that use serial line as a transport mechanism.

6.2. Wireless ATM

Recently, considerable research effort has been put in the direction of integrating the broadband wired ATM and wireless technologies. In 1996 the ATM Forum approved a study group devoted to Wireless ATM, WATM. WATM [23,24] aims to provide end to end ATM connectivity between mobile and stationary nodes. WATM can be viewed as a solution for next-generation personal communication networks, or a wireless extension of the B-ISDN networks, which will support guaranteed QoS integrated data transmission. ATM implementation over the wireless medium poses several design and implementation challenges that are summarized below:

- ATM was originally designed for a transmission medium whose BER are very low (about 10^{-10}). However, wireless channels are characterized by low bandwidth and high BER values. It is questioned whether ATM will function properly over such noisy transmission channels.
- ATM calls for a high resource environment, in terms of transmission bandwidth. However, as we have seen, the wireless medium is a scarce resource that calls for efficient medium use. An ATM cell carries a header, which alone poses an overhead of about 10 per cent. Such an overhead is undesirable in wireless data networks since it reduces overall performance.
- ATM was designed for stationary hosts. In the wireless case, users may roam from one cell to another thus causing frequent setup and release of virtual channels. Thus, fast and efficient mechanisms for switching of active VCs from the old wireless link to the new one are needed. When the handover occurs, the current QoS may not be supported by the new data path. In this case, a negotiation is required to set up new QoS. Handover algorithms should take those facts under consideration.

The protocol architecture currently proposed by ATM Forum is shown in Figure 18.

The WATM items are divided into two parts: Mobile ATM, which consists of a subpart of the control plane, and radio access layer (shaded items in the figure). Mobile ATM deals with the

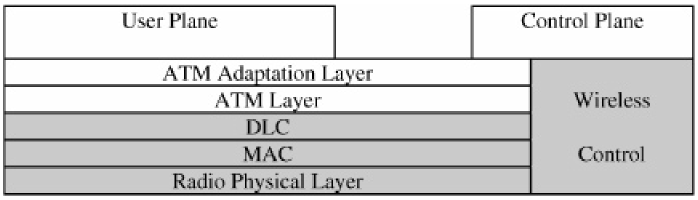
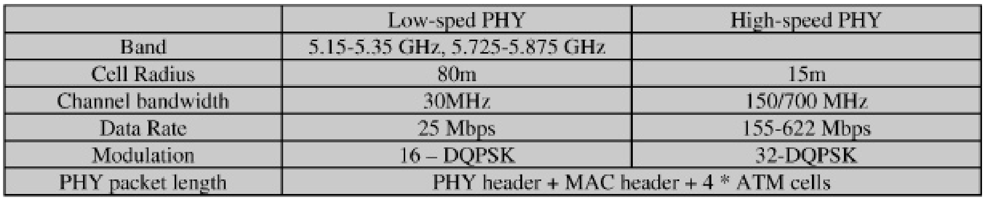


Figure 18. WATM protocol architecture.



	Low-sped PHY	High-speed PHY
Band	5.15-5.35 GHz, 5.725-5.875 GHz	
Cell Radius	80m	15m
Channel bandwidth	30MHz	150/700 MHz
Data Rate	25 Mbps	155-622 Mbps
Modulation	16 – DQPSK	32-DQPSK
PHY packet length	PHY header + MAC header + 4 * ATM cells	

Figure 19. Physical layer requirements for WATM.

higher-layer control/signaling functions that support mobility. The radio access layer is responsible for the radio link protocols for wireless ATM access. Radio access layer consists of the physical layer, the media access layer, the data link layer, and the radio resource control. Up to now, only PHY and MAC are under consideration. The protocols and approaches for DLC and RRC have not been proposed yet. The physical and mac layers for WATM are briefly discussed below:

Physical layer (PHY): While a fixed ATM station can own 25 up to 155 Mbps data rate, such values are difficult to implement over wireless channels. However, projects under development such as the MEDIAN project [25] succeeded in achieving data rates of 155 Mbps by employing OFDM transmission at 60 GHz. The suggested physical layer requirements for WATM are shown in Figure 19.

MAC layer: Most of the proposed MAC algorithms for WATM [23] describe a form of TDMA system in which the frames are divided into two parts. One contention part, which is used by the mobiles to reserve bandwidth for transmission and one part in which information is transmitted. Some general requirements for an efficient WATM MAC protocol are the following:

- Allow for decreased complexity and energy consumption at the mobile nodes.
- Allow support of negotiated QoS under any load condition.
- Enable the adoption of mechanisms to reduce the delay of channel assignment to connections.
- Support efficient management and rerouting of ATM connections as users move while maintaining negotiated QoS levels [26].
- Provide support for efficient location management techniques in order to track mobiles and locate them prior to connection setup [26].

WATM, being a member of the ATM family, provides support for applications, like multimedia, which are characterized by stringent requirements, such as increased data rates, constant end-to-end delay and reduced jitter. Traditional WLANs cannot support these requirements, and have limited support for QoS applications, as we mentioned before. As a result, considerable research projects target the area of WLANs using ATM technology (WATM LANs). Such a project is HIPERLAN 2 [27], a standard being developed by ETSI. The standard is planned to be available in mid-2000.

6.2.1. HIPERLAN 2. HIPERLAN 2 aims to provide high-speed access (up to 54 Mbps at the physical layer) to a variety of networks including third generation mobile networks, ATM networks and IP-based networks, and for private use as a wireless LAN system. Supported applications include data, voice and video, with specific QoS parameters taken into account. The standard adopts an infrastructure topology where mobile terminals are located within cells and communicate with the AP of their cell. Communication between two mobile terminals is also possible, however this procedure is still in an early phase of development. Mobile terminals may roam from cell to cell while maintaining their logical connections. The APs automatically configure the network by taking into account changes in topology due to mobility.

HIPERLAN 2 is characterized by high transmission rates, up to 25 Mbps. As mentioned, it uses OFDM in the physical layer and thus effectively combats the increased fading occurrence experienced in indoor radio environments. Being compatible with ATM, HIPERLAN 2 is a connection-oriented network using fixed sized packets. Signaling functions are used to establish connections between the mobile nodes and the AP in a cell and data are transmitted over these connections as soon as they are established, using a time division multiplexing technique. The standard supports two types of connections: bi-directional point-to-point connections between a mobile node and an AP, and unidirectional point-to-multipoint connections carrying traffic to the mobile nodes. Finally, there is a dedicated broadcast channel used by the AP to transmit data to all mobiles within its coverage.

The connection-oriented nature of HIPERLAN 2 makes support for QoS applications easy to implement. Each connection can be created so as to be characterized by certain quality requirements, like bounded delay, jitter and error rate. This support enables the HIPERLAN 2 network to support multimedia applications in a way similar to the ATM network.

HIPERLAN 2 also provides support for aspects like encryption and security, power saving, dynamic channel allocation, radio cell handover, power control, etc. However, most of these issues are either not standardized yet or left to the vendors to implement.

In Figure 20 the protocol reference model for the HIPERLAN 2 standard is shown. The protocol stack comprises a control plane part and a user plane part following the semantics of ISDN functional partitioning. The user plane includes functionality for transmission of traffic over established connections, and the control plane provides procedures to control established

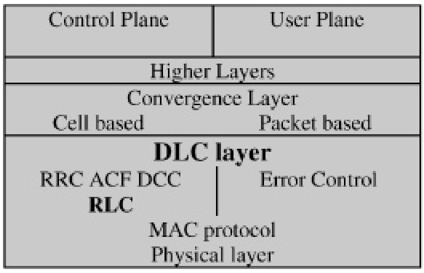


Figure 20. The HIPERLAN 2 protocol stack.

connections. The protocol has three basic layers: the physical layer (PHY), the data link control layer (DLC), and the convergence layer (CL). At the moment, there is only control plane functionality defined in the DLC.

The DLC layer is used to establish the logical links between APs and the MTs. The DLC layer comprises a number of sublayers providing medium access and transmission services to the user plane and connection handling services to the control plane. The MAC protocol used by HIPERLAN 2 is based on time-division duplex (TDD) and dynamic time-division multiple access (TDMA). The wireless medium is shared in the time domain through the use of a circulating MAC frame containing slots dedicated either to uplink or downlink traffic. Slots within a frame are allocated dynamically depending on the need for transmission resources. The MAC frame has a fixed duration of 2 ms and consists of several transport channels:

- The broadcast channel (BCH) is a downlink channel used to convey to the mobiles control information regarding transmission power levels, wake-up indicators for nodes in power save mode and means for identifying the HIPERLAN 2 network and the AP the mobile belongs to.
- The frame control channel (FCH) is a downlink channel used to notify the mobile nodes about resource allocation within the current MAC frame both for uplink and downlink traffic.
- The random access channel (RCH) is used in the uplink both in order to request transmission in the downlink and uplink portions of future MAC frames and to transmit signaling messages. The RCH comprises contention slots which are used by the mobiles to compete for reservations. Collisions may occur and the results from RCH access are reported back to the mobiles in the access feedback channel.
- The access feedback channel (ACH) is used on the downlink to notify about previous access attempts made in the RCH.

The above three transport channels are used as a means to support a number of logical HIPERLAN 2 channels. These are the following:

- The slow broadcast channel (SBCH) is a downlink channel that conveys broadcast control information concerning all the nodes within a cell. This transmission is initiated upon decision of the AP and may contain information regarding encryption, handover acknowledgments, MAC address assignments, etc.
- The dedicated control channel (DCCH) is of bi-directional nature and is implicitly established when a terminal associates with the AP within a cell. Each terminal has its own DCCH which is used by the AP to convey control signaling information only to this terminal.
- The user data channel (UDCH) transports user data between a mobile node and an AP and vice versa. A UDCH for a specific mobile node is established through signaling transmitted over the node's DCCH. The UDCH establishment takes place after negotiation of certain quality parameters that characterize a connection. The DLC guarantees in sequence delivery of the transmitted data to the convergence layer. The use of ARQ techniques is possible in UDCH operation, although there might be connections where ARQ is not desirable, such as multicasts and broadcasts.
- The link control channel (LCCH) is used to exchange information regarding error control (EC) over a specific UDCH. The AP determines the needed transmission slots for the LCCH in the uplink and the grant is announced in an upcoming FCH.
- The association control channel (ASCH) is used by the mobile nodes either to request association or disassociation from a cell's AP.

The error control (EC) protocol of the HIPERLAN 2 protocol stack uses a Selective Repeat ARQ scheme in order to provide error-free, in-sequence data delivery to the upper layers. Positive and negative acknowledgments are transmitted over the LCCH channel. Furthermore, the EC layer includes an out-of-date PDU discard mechanism. If data becomes obsolete, then the sender EC layer can decide to discard it.

The radio link control (RLC) protocol provides services to the association control function (ACF), radio resource control function (RRC), and the DLC user connection control function (DCC). Those entities implement control plane functionality. The ACF is used by mobile nodes to exchange information with the AP prior to connection establishment. For example, an AP may inform the mobile node about the capabilities and characteristics of the links it can offer, such as the physical layer used, whether encryption is possible or not, etc. After the mobile node and the AP agree on association, the AP assigns a DCCH to the mobile node which is used by the latter to establish data connections, possibly of different QoS each, with the AP. The DCC function is used to establish DLC user connections by transmitting signaling messages over the DCCH. The signaling scheme is quite straight-forward comprising a request for a specific QoS connection followed by an acknowledgment in case the request can be fulfilled. Finally, the RRC function manages issues like handover, channel allocation and power-saving.

The convergence layer of the protocol stack carries out two functions. The first is to segment the higher layer PDUs into fixed size packets used by the DLC. The second is to adapt the services demanded by the higher layers to those offered by the DLC. This function requires reassembly of the fixed-size DLC packets to the original variable-size packets used by the higher layers. There are currently two different types of CLs defined: cell-based and packet-based. The cell-based CL serves interconnection to ATM networks and transparently integrates HIPERLAN 2 with ATM whereas the packet based one can be used to interconnect WATM mobiles to legacy wired LANs like Ethernet. In the cell-based CL, Segmentation and Reassembly (SAR) functionality is not included because ATM cells fit into the HIPERLAN 2 DLC PDU. Nevertheless, a compression of the ATM cell header is necessary, transmitting only its most important parts.

The overall performance of a HIPERLAN 2 system depends on a number of factors, including available channel frequencies, propagation conditions and experienced interference. Measurements in Reference [28] show that in most of the cases speeds above 20 Mbps are likely to be achieved.

7. CONCLUSIONS

In this paper an overview of the wireless local area network area was provided. The two types of Wireless LAN topologies used today, infrastructure and ad hoc, were presented. Ad hoc WLANs are preferable in cases where temporary and rapid deployment of a WLAN is demanded. On the other hand, infrastructure WLANs offer the ability to access data and services that are offered by collocated wired LANs. Access to these services is made through the use of base stations that implement access point functionality. Each base station forms its own cell and provides wired network access to all the nodes within its coverage. By employing frequency reuse schemes in cellular structures, the total available bandwidth of a system can significantly increase.

The requirements expected to be met by a WLAN stem from the use of the wireless channel as a means of transmission. Wireless transmission is characterized by increased BER and interference, increased threat for unauthorized access, and in most cases the need for spectrum licensing or use of spread-spectrum techniques. Furthermore, the mobile nature of WLAN nodes results in dynamically changing, possibly not fully-connected, network topologies where measures for power preservation at the mobile nodes must be taken. Those facts greatly affect the implementation of the protocol stack of a WLAN and should be taken into consideration when designing WLAN products.

The five current physical layer alternatives are infrared transmission, frequency hopping spread spectrum modulation, direct sequence spread spectrum modulation, narrowband modulation and orthogonal frequency division multiplexing. IR transmission offers the advantages of greater security and potentially higher data rates, however not many IR-based products exist. The Spread Spectrum and the OFDM approaches offer superior performance in the presence of fading which is the dominant propagation characteristic of wireless transmission. The Spread Spectrum techniques trade off bandwidth for this superiority, offering moderate data rates. Narrowband modulation on the other hand can potentially offer higher data rates than spread spectrum, being subjected however to increased performance degradation due to fading. The OFDM approach is a form of multi-carrier modulation that achieves relatively high data rates. The 802.11 standard supports all of the above alternatives, except for narrowband modulation, which is used by HIPERLAN 1. OFDM is used in the HIPERLAN 2 Physical Layer.

The two WLAN MAC standards available today, IEEE 802.11 and HIPERLAN 1, employ contention-based CSMA-like algorithms in order to access the wireless channel. The 802.11 MAC layer, when used in conjunction with the 802.11b and 802.11a Physical layer extensions can offer data rates up to 11 and 54 Mbps, respectively. However, only 802.11b products are available at this time. HIPERLAN 1 offers data rates up to 24 Mbps having however the disadvantage of incompatibility with 802.11 and the absence of an installed product base. The 802.11 MAC includes a mechanism that combats the hidden terminal problem whereas such a technique is not included in the HIPERLAN 1 standard. The latter includes a mechanism for multi-hop network support, effectively increasing the network operating area. It pays however the price of reduced overall performance compared to the single hop case. Both of the standards try to support time-bounded services, with 802.11 addressing it through the use of an optional contention-free mechanism. HIPERLAN 1 has an integrated priority mechanism that tries to support time-bounded applications, however QoS cannot be offered due to the absence of a mechanism that assigns a certain amount of bandwidth to a station. 802.11 can offer support for QoS applications, through bandwidth assignment to stations by the polling procedure, however the latter is not defined in the standard.

Polling-based protocols developed especially for WLANs, such as the randomly addressed polling (RAP) and Group RAP (GRAP) protocols try to combine the deterministic behavior of fixed assignment protocols and the flexibility of contention-based ones. RAP and GRAP provide superior access to CSMA and enable easy implementation of handoff.

In the last sections, an introduction to personal area networks and wireless ATM has been made. PANs target very small operating areas and are the technology of choice for applications, such as short data transfers, or voice pass through, running between limited powered devices. Bluetooth, the most popular technology in the area, is an open specification aiming to interconnect devices at medium data rates over short ranges. Wireless ATM can be viewed as a solution for next-generation personal communication networks, or a wireless extension of the B-ISDN networks, which will support guaranteed QoS integrated data transmission. However, the use of wireless links imposes additional challenges on WATM design, mainly the need for efficient connection management of WATM links. HIPERLAN 2 is a connection-based WLAN standard compatible with ATM that offers increased data rates and support for QoS applications.

Besides being a useful and profitable business, the WLAN area is also an extremely rich field for research, due to the difficulties posed by the wireless medium and the increasing demand for better and cheaper services. It is very difficult to foresee the state of the area in the next decades or even years. However, the WLAN market is likely to increase in size and possibly integrate with other wireless technologies, in order to offer support for mobile computing applications, of perceived performance equal to that of wired communication networks.

REFERENCES

1. Pahlavan K, Probert TH, Chase ME. Trends in local wireless networks. *IEEE Communication Magazine* 1995.
2. Chen K-C. Medium access control of wireless LANs for mobile computing. *IEEE Network* 1994.
3. Lagrange X. *Multitier cell design. IEEE Communications Magazine* 1997.
4. Zander J. Radio resource management in future wireless networks: requirements and limitations. *IEEE Communications Magazine* 1997.
5. Nettleton RW, Schoemer GR. Self organizing channel assignment for wireless systems, *IEEE Communications Magazine* 1997.
6. Lozano A, Cox DC. Integrated dynamic channel assignment and power control in TDMA mobile wireless systems. *IEEE Journal on Selected Areas in Communications* 1999; **17**.
7. Bantz DF, Bauchot FJ. Wireless LAN design alternatives. *IEEE Network* 1994.
8. Andersen JB, Rappaport TS, Yoshida S. Propagation measurments and models for wireless communication channels, *IEEE Communications Magazine* 1995.
9. Gilbert E. Capacity of a burst noise channel. *Bell System Technology Journal*. 1960; **39**.
10. Zorzi M, Rao RR, Milstein LB. On the accuracy of a first-order Markov model for data transmission on fading channels. *ICUPC 95*, Tokyo, Japan, November 1995.
11. Falconer DD, Adachi F, Gudmundson B. Time division multiple access methods for wireless personal communications. *IEEE Communications Magazine* 1995.
12. Badra RE, Daneshrad B. Asymmetric physical layer design for high-speed wireless digital communications. *IEEE Journal on Selected Areas in Communications* 1999.
13. Barry JR. Kahn JM, Lee EA, Messerschmitt DG. High-speed nondirective optical communication for wireless networks. *IEEE Network Magazine* 1991.
14. Weinmiller J, Schlager M, Festag A, Wolisz A. Performance study of access control in wireless LANs IEEE 802.11 DFWMAC and ETSI RES 10 HIPERLAN. *ACM Mobile Networks and Applications* (Special Issue on Channel Access) 1997; **2**.
15. Weinmiller J, Woesner H, Ebert J-P, Wolisz A. Analyzing and tuning the distributed coordination function in the IEEE 802.11 DFWMAC Draft Standard.
16. Crow BB. Performance evaluation of the IEEE 802.11 wireless local area network protocol. *Masters Thesis*, Department of Electrical and Computer Engineering, University of Arizona, 1996.
17. Kahol A, Khurana S, Jayasumana AP. Effect of hidden terminals on the performance of IEEE 802.11 MAC protocol. *Proceedings of 23rd IEEE Annual Conference on Local Computer Networks (LCN '98)*.
18. Chen K-C, Lee C-H. RAP-a novel medium access control protocol for wireless data networks. *Proceedings of IEEE GLOBECOM*, 1993.
19. Chen K-C,, Lee C-H. Group randomly access polling for wireless data networks. *Proceedings of IEEE ICC*, 1994.
20. Kardach J. Bluetooth architecture overview.
21. 3Com Networks, Bluetooth and IEEE 802.11b. Wireless Technology Positioning Paper, Version 1.1, February 2000.
22. Mettala R. Bluetooth Protocol Architecture. Bluetooth Special Interest Group (SIG), Version 1.0, September 1999.
23. Kubbar O, Mouftah HT. Multiple access control protocols for wireless ATM: problem definition and design objectives. *IEEE Communications Magazine* 1997.
24. Pahlavan K, Krishnamurthy P. Wideband local access: wireless LAN and wireless ATM. *IEEE Communications Magazine* 1997.
25. Priscolli FD. Design and implementation of a simple and efficient medium access control for high-speed wireless local area networks. *IEEE Journal on Selected Areas in Communications* 1999; **17**.

26 Veeraraghavan M, Karol MJ, Eng KY. Mobility and connection management in a wireless ATM LAN. *IEEE Journal on Selected Areas in Communications* 1997; **15**(1).

27. Johnsson M. HiperLAN/2—the broadband radio transmission technology operating in the 5 GHz frequency band. HiperLAN/2 Global Forum, 1999, Version 1.0.

28. Torsner J, Malmgren G. Radio network solutions for HIPERLAN/2. *Proceedings of VTC '99*, Spring, Houston.
29. Pahlavan K, Levesque A. *Wireless Information Networks*. Wiley: New York, 1995.
30. Taylor L. *HIPERLAN Type* 1 *Technology Overview*. TTP Communications Ltd. Revision 0.9 June 1999.
31. Broadband Radio Access Networks (BRAN). HIgh PErformance Radio Local Area Network (HIPERLAN), Type 1, Functional specification V1.2.1 July 1998.
32. Hayes V. Standardization efforts for wireless LANs. *IEEE Network Magazine* 1991.
33. Toh C-K. A handover paradigm for wireless ATM LANs. *ACM Symposium on Applied Computing (SAC 96)*.
34. Geier J. *Wireless LANs*, *Implementing Interoperable Networks*, Macmillan Network Architecture and Development Series.
35. Stallings W. *Data and Computer Communications*, (5th edn), Prentice-Hall: Englewood Cliffs, NJ.
36. Stallings W. *Local and Metropolitan Area Networks* (5th edn).
37. Tannenbaum A. *Computer Networks* (3rd edn), Prentice Hall: Englewood Cliffs, NJ.
38. Obaidat MS, Ahmed CB. Schemes for mobility management of wireless ATM networks. *International Journal of Communication Systems* 1999; **12**(3): 153–166.

AUTHORS' BIOGRAPHIES

Petros Nicopolitidis received the BS degree in Computer Science from the Department of Informatics of Aristotle University of Thessaloniki (A.UTH) in 1998. Since 1999 he is a PhD student at the same department. His research interests are in the areas of Wireless Local Area Networks and mobile communications.

Georgios I. Papadimitriou received the Diploma and PhD degrees in Computer Engineering from the University of Patras, Greece in 1989 and 1994 respectively. From 1989 to 1994 he was a Teaching Assistant at the Department of Computer Engineering of the University of Patras and a Research Scientist at the Computer Technology Institute, Patras, Greece. From 1994 to 1996 he was a Postdoctorate Research Associate at the Computer Technology Institute. Since 1997, he has been a Lecturer at the Department of Informatics, Aristotle University of Thessaloniki, Greece. His research interests include design and analysis of broadband networks and learning automata. He has published several dozens of papers in international journals and conferences.

Andreas S. Pomportsis received a BS degree in Physics and an MS degree in Electronics and Communications (both from the University of Thessaloniki), and a Diploma Degree in Electrical Engineering from the Technical University of Thessaloniki. In 1987 he received a PhD degree in Computer Science from the University of Thessaloniki. Currently, he is Professor in the Department of Informatics, Aristotle University of Thessaloniki, Greece. His research interests include computer architecture, parallel and distributed computer systems, and multimedia systems.