**Unit-4**

**Wireless Local Area Networks**

**Benefits of Wireless LANs**

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. More-over, in situations where cabling installation is expensive or impossible (e.g. historic build-ings, monuments or the battlefield) WLANs appear to be the only feasible means 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 wired network failures. Moisture which causes erosion of the metal-lic conductors and accidental cable breaks can bring a wired network down. Therefore, the use of WLANs helps reduce the downtime of the network and eliminates the costs associated with cable replacement.

 **Wireless LAN Applications**

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

As mentioned, early WLAN products 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 existing buildings are already wired with this type of cabling and new buildings are designed by taking into account the need for data



Figure:The ETSI HIPERLAN family of standards

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 manu-facturing 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 uncabled 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 in 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. An 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 in order 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.

**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 (BERs) having an order of magnitude even up to ten 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, such as that caused by microwave ovens operating in the 2.4 GHz band, can have disastrous effects on 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 sublayer) are often used in this direction. Outward interference occurs when the WLAN signals disrupt the operation of adjacent



Figure :Terminal scenarios: (a) ‘hidden’’ and (b) ‘exposed’

WLANs or radio devices, such as intensive care equipment or navigational systems. However, as most WLANs use spread spectrum technology, outward interference is consid-ered insignificant most of the time.

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 9.3. 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.

Another difference between wired and wireless LANs is the fact that 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 in 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 trade-offs 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, substantially decreases 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 task 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 signifi-cantly affect the propagation pattern of WLAN signals causing undesired effects. MOST of the time, this problem is 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, the threat to human safety is even lower. Diffused Infrared (IR) WLANs offer no hazard under any circumstance.

 **Wireless LAN Topologies**

There are two major WLAN topologies, ad hoc and infrastructure (Figure 9.4). 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 coordination exists in this topology. As a result, ad hoc networks are required to use decentralized MAC proto-cols, such as CSMA/CA, with all nodes having the same functionality and thus implementa-tion complexity and cost. Moreover, there is no provision for access to wired network



Figure :WLAN topologies: ad hoc and infrastructure

services that may be collocated in the geographical area in which the ad hoc WLAN operates. Another important aspect of ad hoc WLANs is the fact that fully connected network topol-ogies cannot be assumed. This is due to the fact that two mobile nodes may be temporarily 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 use centralized MAC protocols like polling, although decentralized MAC protocols are also used (For example, the contention-based 802.11 can be implemented in an infrastructure topology). This approach shifts imple-mentation 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 not mandatory that the BS and AP be implemented in the same device, most of the time 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 multicell 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 connec-tion 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 (decentralized 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 decentralized 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 9.5. In this example, nonadjacent 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, a scheme that would demand a total 16 £ B of bandwidth.

The above strategy is also known as Fixed Channel Allocation (FCA). Using FCA, chan-nels 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



Figure : Example of frequency reuse

all and still use the same amount of bandwidth as a densely populated cell. Therefore, spectrum utilization is suboptimal. Dynamic channel allocation (DCA), Power Control (PC) or integrated DCA and PC 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 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 interference experienced 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. However, most of these results stem from the assumption that ad hoc WLANs utilize contention MAC protocols (e.g. CSMA) whereas infrastructure networks use TDMA-based protocols. 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.

**Wireless LAN Requirements**

A WLAN is expected to meet the same requirements as 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 to be met. 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 an even more

crucial 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 accom-panied by great delay. Operating throughput in this case is measured to be around 4 Mbps, only 40% 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 sublayers 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 nonreciprocal 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 transmis-sion’s destination node needs to be implemented. Alternatively, buffering can be used at the sender, posing the danger of buffer overflows and packet losses, however. 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. 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 with 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 connec-tion 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 150--300 m

in diameter. The effect of propagation delay can be significant, especially where a WLAN MAC demands precise synchronization among mobile nodes. For example, in cases where unslotted CSMA is used, increased propagation delays result in a rising number of colli-sions, 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 perfor-mance.
* Compliance with standards. As the WLAN market progressively matures, it is of signifi-cant importance to comply with existing standards. Design and product implementations based on new ideas are always welcome, provided, however, that they are optional exten-sions to a given standard. In this way, interoperability is achieved.

**The Physical Layer**

**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 transmis-sion 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 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 optical signal produced is then radiated in 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 the received focused signal over a wider range. 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.

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 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 applica-tion. 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 trans-mitted 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 transmis-sion 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 9.6 and 9.7 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.

Both the preamble and the header of an 802.11 frame transmitted over an IR link are



Figure :16-Pulse position modulation code



Figure:4-Pulse position modulation code

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 milliseconds.
* 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.

**Microwave-based Physical Layer Alternatives**

The microwave radio portion of the electromagnetic spectrum spans from 107 to about 1011 MHz. Being of lower frequency, the Radio Frequency (RF) channel behaves significantly differently from that of IR. Radio transmission can penetrate walls and nonmetallic 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 being 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 spec-trum, 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 fabrica-tion 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 recent years, this part of the spectrum has experienced great

popularity among electronic equipment manufacturers. 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 the relevant 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 immu-nity to interference is guaranteed.

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 MHz, 2400–2483.6 MHz and 5725–5850 MHz) of the spectrum. This decision significantly boosted the WLAN industry in the United States. 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 interfer-ence, 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.

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 exist. 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 band is even more interference-free. The same situation characterizes galactic, atmospheric and man-made noise. 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 that the range in the 2.4 GHz band is around 5% less than that in the 902 MHz band. For the 5.8 GHz band, this number rises to 20%. 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 centered 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 determi-nistic 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.

**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 center 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, of which 50 must be used. In the middle band and upper bands, these channel numbers are 100 (83 in the United States), 75, 125 and 75, respectively. Furthermore, FCC rules state that the transmitters must not spend more than 0.4 s on any one 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 due to 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. In 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 802.11 standard describes how to calculate optimal values for fc. Furthermore, the



Figure: DSSS modulation

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 0s and 1s 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 from 0 to 4096 octets.

**The Direct Sequence Spread Spectrum Physical Layer**

Using direct sequence spectrum spreading, each bit in the original signal is represented by a number of 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 the 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 by a width proportional to the spreading factor. Figure 9.8 shows a binary data stream, a pseudorandom sequence having three times the rate of the data stream, and the resulting spread signal. Figure .depicts the demodulation of the spread signal at the receiver.

bandwidth, DSSS has the significant ability to extract a signal from a background of narrow-band interference and noise, a fact that results in fewer retransmissions, thus enhancing throughput.

DSSS WLANs present a lower potential for interference cancellation than do FH 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 are 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 nonadjacent 0.5 MHz channels, the DSSS WLAN cannot totally avoid interference in any case.

DSSS also has the ability to accommodate a number of simultaneous operating WLANs. Some DS WLANs may be designed to use less than the total available bandwidth. In such a case, additional WLANs using the remaining free channels can be admitted in the same geographical area. Nevertheless, as the number of DSSS subchannels 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 subchannels 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 a data rate of 2 Mbps. 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 they use subchannels with center 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 Mbps, 2 Mbps, 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. An 8-bit field that indicates 1, 2, 5.5, or 11 Mbps operation.
* Service. An 8-bit field reserved for future use.
* Length. A 16-bit field containing the length of the MPDU in milliseconds.
* 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.

**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. However, interference is not common in the 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 that 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 subchannel’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.

**The Orthogonal Frequency Division Multiplexing (OFDM) Physical Layer**

IEEE 802.11a operates in the in the 5 GH z bands and use Orthogonal Frequency Division Multiplexing (OFDM) to spread the transmitted signal over a wide bandwidth. OFDM is a form of multicarrier transmission and divides the available spectrum into many carriers, each one 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 chan-nels, 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 9.10 shows the spectrum for an OFDM transmission.



Figure: Detection of OFDM symbols

The spectrums of the subcarriers 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 subcarriers 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. In order for the technique to work, however, perfect synchronization between the receiver and the transmitter is required.

OFDM effectively combats ISI. The OFDM symbols are artificially prolonged by periodi-cally 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 ortho-gonality is preserved. However, by preceding the useful part of the length by the guard interval, we lose some parts of the signal that cannot be used for transmitting information.

In 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.

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 nondeterministic behavior, 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 was formed in the late 1980s.

In the following paragraphs we examine the MAC sublayer 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.



Figure : HIPERLAN 1 system architecture

**The HIPERLAN 1 MAC Sublayer**

The HIPERLAN 1 standard was released in 1995 aiming to define a WLAN technology of equal performance to that of traditional wired LANs and 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 9.11. It divides the functions of the Medium Access Control (MAC) into two subparts, which it refers to as Channel Access and Control (CAC) and MAC sublayers. 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 attempt will be made, if contention is necessary. The HIPER-LAN MAC sublayer defines the various protocols which provide the HIPERLAN features of power conservation, lookup, security, and multihop 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 inter-mediate forwarding stations. The lookup functionality enables collocated operation of more than one HIPERLAN network. Finally, the standard supports priorities, power conservation and support for encryption.

**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 define 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 1. This mechanism is used by HIPERLAN 1 to support time bounded applications.

**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 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.
* 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 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 3%. EY-NPMA simulation results in Ref. [9] show typical performance for a contention protocol:

* Performance increases 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 an 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.

**Supported Topologies and Multihop Routing**

HIPERLAN 1 supports both infrastructure and ad hoc topologies. Furthermore, the standard supports multihop configurations, where a station can transmit a packet to another station out of its radio range without the need for additional infrastructure. This can be achieved with the help of intermediate stations that can forward packets destined for other stations. Each HIPERLAN station will select one and only one neighbor 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 nonforwarder. Nonforwarders are required to know only their direct neighbors.

Forwarding in a WLAN poses some problems. First, 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 neighbors, a fact that limits the useful bandwidth of the channel.

**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 at 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.

Security

The MAC sublayer 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, 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 a random number generator that outputs a bitstream of length equal to the MPDU length. The two bitstreams 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.

**The IEEE 802.11 MAC Sublayer**

The IEEE 802.11 standard covers the physical and MAC layers of the OSI model. It defines a single MAC sublayer 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 Coordination Function (DCF); it offers only 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 Coordination Function (PCF) and is offered only in 802.11 infrastructure networks.

**The 802.11 MAC Protocol**

**Distributed Coordination Function** The DCF sublayer uses a slotted CSMA/CA algorithm Thus, data transmissions can only start at the beginning of each slot. The IEEE



Figure: The IEEE 802.11 system architecture

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.

DCF uses three IFS values in order to enable priority access to the channel (Figure 9.13). These are, from the shortest to the longest, the Short IFS (SIFS), the Point Coordination Function IFS (PIFS) and the Distributed Coordination function IFS (DIFS). Their actual duration is defined by the slot duration and is thus physical layer dependent. Ref. [9] provides simulation results of the performance of the IEEE 802.11 DCF over three 802.11 physical layer specifications, concluding that end performance is highly dependent on the above two parameters. The Infrared (IR) physical layer shows better performance than the Direct Sequence Spread Spectrum (DSSS) layer, 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 sublayer. Since it is shorter than DIFS it gives the Polling Coordinator (PC) the ability to lock out asynchronous traffic and allocated bandwidth for time 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



Figure: DCF operation

packets. As a result, the acknowledging station is favored 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 trans-mitted frame, the transmitting station assumes a collision occurred and re-contends for the channel.

* Fragmentation. MAC frames are passed down from the Logical Link Control (LLC) sublayer to the MAC sublayer. The MAC sublayer 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 receipt 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 frag-ments have been delivered.
* RTS/CTS. This mechanism enhances the two-way handshake CSMA/CA algorithm (DATA-ACK) to a four-way handshake algorithm (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.

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 , 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.

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 ¼ 1023) 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 which leads to more collisions. show that when the number of hidden pairs exceeds 10%, 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 Coordination 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 Coordinator (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 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. 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 dura-tion of the PCF. It can take a value no larger than the one that is required by the DCF in order to transmit 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 these parameters using a Beacon frame. Stations that hear the Beacon frame defer until the CFP ends. The CFP can be terminated before the expiration time 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 PCF portion of 802.11 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 algo-rithm 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 implementa-tion of the polling algorithm and leaves it to the PC implementor. Joint simulations of the DCF and PCF ,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.

**Supported Topologies**

The 802.11 standard supports both infrastructure and ad hoc network configurations. Infra-structure networks comprise one or more cells that contain mobile nodes. The mobile nodes access the backbone network, referred to as the Distribution System 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 Distribution System (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.

**Security**

The 802.11 standard defines two security procedures. The first allows for encrypted frame transmissions, in a way similar to that implemented by HIPERLAN 1. Encryption is imple-mented 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 bit sequence produced.
* 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 as 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 steps are as follows:

* The requesting station sends an authentication frame to another station.
* Upon receipt 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 authen-tication.

**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.