Chapter 4
Wireless Local Area Network

4.1 Introduction

All radio communication technologies are developed on cellular architecture. However, the major technological hurdle in use of radio communication is the ability to build seamless convergent solutions for mobile users. Availing services across heterogeneous networks is still a problem for mobile users. The numerous challenges encountered in this respect are mainly due to the following reasons.

1. Multiple access technologies, and administrative domains.
2. Multiple types of services such as voice, data, video, etc.
3. Availability of services every where and all the time.
4. Efficient delivery of traffic.

From the stand point of application development and convenience of usages, innovations in building convergent solutions are more important than the discovery of new networking technologies. Still availability of new networking technology would eventually lead to easy and efficient implementation of convergent communication solutions in overcoming heterogeneity of networks. Thus, a sound understanding of wireless network is an important starting point for developing exciting new applications for mobile computing systems.

In general, wireless data networks can be divided broadly into four different categories based on their intended use.

1. *Wide area networks* (WANs) are created and maintained by cellular carriers. WANs can be viewed as connectionless extensions to circuit switched networks, created in order to facilitate communication between persons and groups belonging to geographically dispersed locations spread over large areas, such as across cities or across countries. The main utility of WANs lies in connecting different LANs and MANs, so that computers and users of one domain can communicate with computers at different domains located far apart.
2. *Metropolitan area networks* (MANs) are created and maintained as a backbone network technology for interconnecting a number of local area networks or LANs.

R.K. Ghosh, *Wireless Networking and Mobile Data Management*,
DOI 10.1007/978-981-10-3941-6_4

Its coverage spans a large geographical area such as a city or a block of buildings spread over a sufficiently large physical area or a campus.

3. *Local area networks* (LANs) are created and maintained by small institutions or organizations for close communication related to professional interactions, collaboration between persons and groups belonging to an institution or an organization.
4. *Personal area networks* (PANs) are created by individuals, usually self-organize, self-maintained. PANs are exclusively for person centric communication with interfaces to local neighborhood and the rest of the world.

Though both WLAN and PAN are based on short range radio transmission technologies, the two have distinct domains of applications. PAN applications typically require low volume, more secure transmission compared to WLANs. Therefore, low range radio transmission technologies such as Bluetooth or ZigBee, are ideally suited for person centric data services as needed by PANs.

In contrast, GSM is the core radio based transmission technology for the applications that require data service over WANs. GSM offers very low speed data service, because mobility management in wide area network is the main focus in GSM. GPRS, EDGE, HSCSD standards which were developed around GSM provided enhanced data rates over WANs by creating packet based network extensions to conventional circuit switched connection of the GSM network.

GSM, GPRS and UMTS have been discussed in the previous chapter. We plan to study PAN separately in Chap. 5 while limiting the focus of the current chapter to the principles and the theories on which wireless LANs are established and used. In order to organize this chapter as a precursor to subsequent discussion on wireless networks, we also take closer looks at: (i) how mobility affects the data rates, and (ii) the details of standards for different wireless networks.

4.2 Mobility Support and Wireless Networks

Figure 4.1 gives a brief introduction on the relationship of achievable data rates with mobility support. WLAN supports only slow mobility while WAN (GSM/wideband cellular) supports range of mobilities starting from discrete and slow to continuous fast (vehicular) mobility. For example, PAN, implemented over Bluetooth, supports slow mobility in an enclosed room, and lies somewhere between fixed and slow mobility (no more than the speed of walking). The mobility in Bluetooth is neither fully controlled nor discrete like in wired LAN. Though wired LAN is fixed, with DHCP, it can provide very limited discrete and slow mobility. A user can access network resources by moving to different locations within a single network administrative domain by changing the terminal's point of attachment with the wired network through DHCP.

Wide area network data services are typically based on telephone carriers, and built over the new generation voice plus data networks. It offers continuous fast mobility

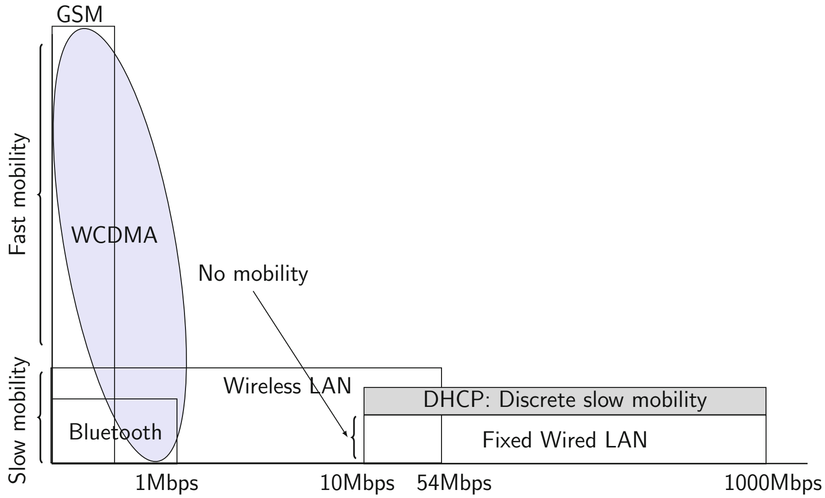


Fig. 4.1 Mobility supports on LAN and WAN

at a vehicular speed. So, GSM and wideband cellular data services has become as ubiquitous as voice calls over the cell phones. Over WANs, the reachability of the data is more important than the quality of the data. The cost of infrastructure supporting WAN services is very high. So, data services over WANs are more expensive compared to those offered through WLAN or Bluetooth.

Wireless MAN (WMAN) is used mainly as a back haul network connecting different wireless LANs. It is ideal for a broadband wireless point to point and point to multipoint connectivity. So, WMAN serves as alternative to cable and DSL modem for last mile broadband access. It can support a few other interesting applications such as IPTv and VoIP. WMAN is based on industry standards known as WiMAX [9] (Worldwide Interoperability for Microwave Access) as it works on Microwave band. There are two variants of WiMAX, one operating in unlicensed frequency band 2–11 GHz while the other operating on licensed band 10–66 GHz. WMAN offers a range up to 50 km and data rate up to 80 Mbps.

Wireless LAN is supported usually by wired infrastructure and provide one-hop wireless connectivities to the clients within a small distance. The typical coverage area could be a university, small enterprise, hospital, airport, etc. Considering the requirements of the clients, wireless LAN should support high data transfer rates as opposed to WANs. WLANs operate on the unlicensed part of the wireless communication spectrum. Its range may spill over to the streets and exposed to vulnerability if the placement of access points are not planned carefully.

In contrast, Bluetooth allows wireless accessibility in enclosed rooms and offers some sort of a physically supervised access. For example, the room access may be through passkey/card, and the devices could either block visibilities through software or demand pass keys for allowing access. Accessories like keyboard, mouse, etc.,

Table 4.1 Summary of wireless communication technologies

Networks	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a/g/b	802.16	GSM/GPRS, CDPD, CDMA
Speed	<1 Mbps	1–54 Mbps	22+ Mbps	10–384 kbps
Range	Short	Medium	Medium-long	Long
Applications	P-to-P	Enterprise network	P-to-P and P-to-MP	PDA/mobile cellular access

can be connected to a computer without cables using Bluetooth. Computers can also be connected to cell phones, or cell phones to head sets over Bluetooth. PANs sometimes termed as ad hoc networks, since they do not depend on pre-existing network infrastructure for connectivity. The participating nodes connect in ad hoc fashion when they are in range of one another. The network disappear as participating nodes move away. PANs like WLAN also support one hop communication and can be seen more as value addition to WLANs. They should not be confused with wireless ad hoc network which are multi-hop network and their usability is independent of WLANs.

The usage of different wireless communication technologies characterized by speed, range and applications are summarized in Table 4.1.

4.3 WLAN Standards

Wireless local area network or WLAN extends a wired infrastructure network by attaching devices known as wireless Access Points (APs). An AP provides network connectivity for a short distance, up to 500 m in the clear air. Multiple number of clients can connect through one access point. WLAN may, therefore, be viewed as a point to multi-point communication technology much like a community radio network. The architecture of WLAN is not just for replacement of cable, it also provides untethered broadband internet connectivity. It is a solution for coverage of *hot spots* like airports, university campus, hospitals, convention centers, government/corporate offices, plants, etc. CISCO, Intel, IBM, Apple are among the companies which manufacture equipment and accessories to setup WLANs. WLAN can support significantly lower data transfer rates between 11 and 54 Mbps. The latest WLAN standard IEEE 802.11n [7] could offer speed up to 300 Mbps. As opposed to WLANs, Wired LANs can support data rates between 100 and 1000 Mbps. Most high performance computing platforms rely on wired LANs that can reach peak transfer rates up to 40 Gbps over point-to-point connections.

4.3.1 IEEE Standards

WLANs mostly use wireless Ethernet technology based on IEEE 802.11 standards [6]. There are three well known operational standards for WLANs, namely, IEEE 802.11a, IEEE 802.11b and IEEE 802.11g. IEEE 802.11 standard was first proposed in 1997. After two years in 1999, IEEE 802.11b [13], known popularly as WiFi, was released. It uses 2.4 GHz unlicensed spectrum, and supports the transfer rates in the range of 5–11 Mbps. IEEE 802.11a was also released around the same time. The industry name for the implementation of IEEE 802.11a is WiFi5 because it uses the frequency spectrum in 5 GHz band. It uses more efficient transmission method called Orthogonal Frequency Division Multiplexing (OFDM) in its physical layer for better performance. In 2003, IEEE announced 802.11g standard in 2.4 GHz band using OFDM. It supports a raw data rate of 54 Mbps as against 11 Mbps by 802.11b. As both 802.11g and 802.11b operate in same 2.4 GHz band, they are compatible to each other. Total of 14 overlapping channels exists at a spacing of 5 MHz from the left outer band edge as shown in Fig. 4.2. Since each channel width is 22 MHz, and the center frequency f_c of channel 1 is 2.412 GHz, the upper frequency f_u of channel 1 must be 2.423 GHz. This means any channel whose lower frequency f_l is higher than 2.423 GHz would be non-overlapping with channel 1. Since, channel 6's $f_l = 2.426$ GHz, channel 6 is non-overlapping with channel 1. Similarly $f_u = 2.448$ GHz for channel 6, and f_l of channel 11 is 2.451. So channel 11 is non-overlapping with 6. Therefore, in IEEE 802.11b supports just three non-overlapping channels, namely 1, 6 and 11, and uses transmit spectrum mask to limit power leakage to the adjacent channels. It causes the energy outside ±11 MHz around the center frequency f_c to drop down by 30 dB relative to the peak energy at f_c. Similarly, the signal must attenuate by at least 50 dB outside ±22 MHz around f_c relative to peak energy at f_c. Note that this may still cause some amount of interference in adjacent channel.

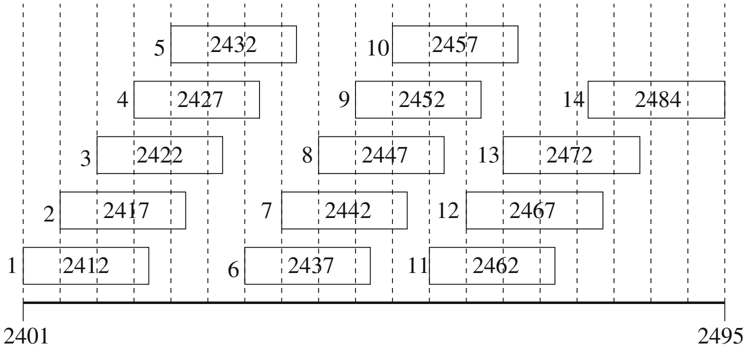


Fig. 4.2 Channelization of 2.4 GHZ band for WLAN

IEEE 802.11a is particularly well suited for multiple users running applications that require high data rates. It supports a maximum raw data transfer rate of 54 Mbps. 802.11a is designed originally for three distinct subbands 5.15–5.25, 5.25–5.35 and 5.725–5.825 GHz. This implies that every 40 MHz channel spans over 4 channel numbers. The lower and middle subbands have total of eight carriers of width 40 MHz at 20 MHz spacing. The upper subband has four carriers also at 20 MHz spacing. The outermost channels in lower and middle subbands are at 30 MHz spacing from the band edges. Figure 4.3 illustrates the channelization scheme. However, the outermost channels in the upper subband are at 20 MHz spacing from the band edges. Channelization for the upper subband is illustrated by Fig. 4.4. A spectral mask is used in 802.11a to limit the power leakage into the adjacent channels. The power output drops down sharply after a spacing of 9 MHz on both the sides of central frequency. After 11 MHz spacing from the central frequency, the power output goes down steadily and becomes as low as −40 dB at ±30 MHz from the central frequency f_c as shown in Fig. 4.5. In Europe the lower and the middle segments are free, so a total of eight non-overlapping channels are offered. Each channel is of width 20 MHz centered at 20 MHz intervals. Since, 802.11a uses OFDM, it can employ multiple carriers. OFDM is based on the inverse idea of code division multiple access (CDMA). CDMA maps multiple transmissions to a single carrier whereas OFDM encodes a single transmission into multiple sub-carriers. OFDM is able to use overlapping sub-carriers because one can be distinguished from the other due to orthogonality. However, 802.11a was not as popular as 802.11b. Due to higher frequency, the range of 802.11a network is short compared to that of 802.11b. It covers just about one fourth of the area covered by 802.11b. Furthermore, 802.11a signals cannot penetrate walls and other obstructions due to shorter range. The use of 802.11a, thus, never really caught on.

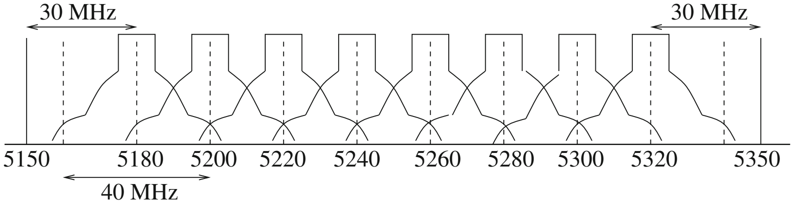
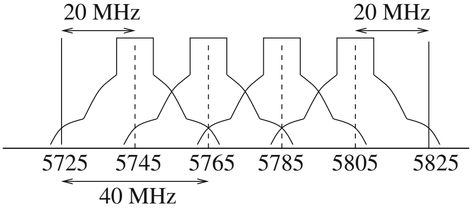


Fig. 4.3 Lower and middle subband channelization scheme for 802.11a

Fig. 4.4 Upper subband channelization scheme for 802.11a



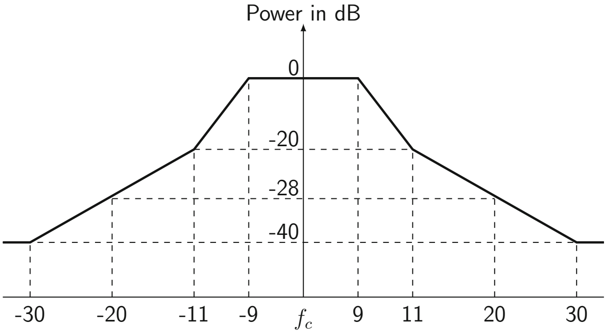


Fig. 4.5 Transmit spectrum mask

The IEEE 802.11b standard, using DSSS as physical layer, sets aside 14 channels for WLAN usage. But the governmental restrictions in different countries may not allow the use of certain channels. USA and Canada allow channels 1–11, most of Europe except Spain and France allow 1–13 channels. Where Japan allows all 14 channels for WLAN usage. France allows four (10–13) and Spain allows only two (10–11) channels for WLAN. The channels are overlapping. For avoiding adjacent channels rejection at the receiver end, there should be a gap of 30 MHz between neighboring channels. The center frequencies (the actual channel frequency used for communication between a receiver and transmitter) are located at 5 MHz intervals. According to the adjacent channel rejection demand, there should be five channels in-between to avoid interference caused by the neighboring access points. So, out of fourteen channels, at most three are non-overlapping. In other words, at most three access points can be placed adjacent to one another.

IEEE 802.11n is a relatively new standard, finalized in 2009 [7]. It could achieve higher transfer rate by relying on multiple input and multiple output (MIMO) antennas [15]. It operates on both 2.4 and 5 GHz bands. IEEE 802.11n allows up to four transmit and four receive antennas. The number of simultaneous data streams is restricted by the minimum number of antennas used on both ends of a connection. The notation $n_1 \times n_2 : n_3$, where $n_3 \leq \max\{n_1, n_2\}$, is used to describe a MIMO antenna's capabilities. The first parameter n_1 gives the maximum number of transmit antennas, the second parameter n_2 specifies the maximum number of receive antennas that can be used by the radio. The third parameter n_3 restricts number of spatial data streams that can be used by the radio. That is the number n_3 indicates that the device can only send or receive on n_3 antennas. Therefore, on a $2 \times 2 : 2$ radio a device have two receive and two transmit antenna, however, only two simultaneous data streams can be supported.

A summary of physical properties of different IEEE standards for wireless local area network appears in Table 4.2.

Table 4.2 Physical properties of IEEE standards for WLAN

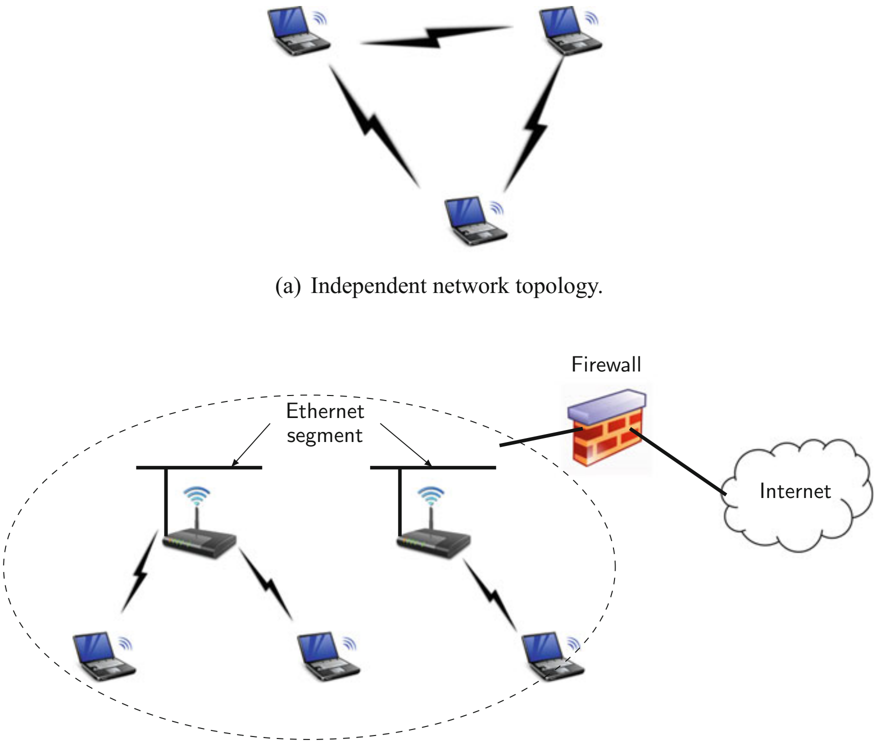
Standard	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Bandwidth (Mbps)/Chanl. width (MHz)	300/20	83.5/22	83.5/22
Basic N/W size[a]	254	254	254
Maximum packet size	104 B	341 B	2048 B
Inter-node range	10m	1–10m	1 m
Protocol stack size	4–32 kB	>250 kB	≈425 kB
Number of channels[b]	12/8	11/3	11/3
Maximum raw data rate Mbps	54	11	54
Modulation	OFDM	DSSS/CCK	DSSS/PBCC
Topology	BSS	BSS	BSS
Architecture			
Protocol	CSMA/CA	CSMA/CA	CSMA/CA
Traffic type	Text	Text, audio, compressed video	File, and object transfers
Battery life	Years	Days	Months
Success matrics	Reliability, low power, low cost	Low cost, low latency, convenience	Reliability, secured, privacy, low cost
Application	Sensor network	Consumer electronics, cell phones	Remote control

[a] 0 and 255 are special addresses
[b] Total and number of non-overlapping channels

4.4 Network Topology

IEEE 802.11 supports two basic topologies for wireless networks: (i) independent networks, and (ii) infrastructured networks.

A single access point and all stations associated with this access point together define a Basic Service Set (BSS). A BSS is different from the coverage area of an access point which is referred to as a Basic Service Area (BSA). A Basic Service Set IDentifier (BSSID) uniquely identifies each BSS. So, a BSSID can be seen as analogous to a work group in Microsoft .NET environment. The MAC address of the access point for a BSS serves as the BSSID for that BSS. Though MAC address is machine friendly, a user will find it difficult to remember. It is, therefore, unfair to expect that a user would provide BSSID to connect to a BSS. A user friendly name known as Service Set IDentifier (SSID) is used to identify a BSS. An SSID is referred to as a name of a WLAN or the network. Typically, a client can receive the SSID of a WLAN from its access point. However, for security reasons, some wireless access points may disable automatic SSID broadcast. In that case client has to set the SSID manually for connecting itself to the network. An Independent BSS (IBSS) is an ad hoc network that does not have an access point. In an IBSS every station should be



(a) Independent network topology.

(b) Infrastructured network topology.

Fig. 4.6 WLAN basic topologies

in range of each other. The first station which starts the network chooses the SSID for IBSS. Each station in an IBSS broadcasts SSID by turn which is performed in a pseudo random order.

Figure 4.6 depicts the two basic topologies described above. Independent network services are available to the stations for communication within a small geographical coverage area called a Basic Service Area (BSA) much like a cell in a cellular architecture. In the case of infrastructured network, the communication among nodes is controlled by a distributed coordination function which will be discussed later in Sect. 4.6. There are specialized nodes called access points (APs) through which wireless stations communicate. The communication can span over at most two wireless hops. One from the sender to its AP, and the other from the AP of the receiver to itself when both the sender and the receiver are wireless enabled. Both the receiver and the sender may be linked to same AP or two different APs. APs essentially act as relay points and vital to the WLAN architecture. The placement of the APs should be planned in advance to provide coverage to the wireless stations. The planning should consider issues such as maximizing coverage, minimizing interferences, restricting blind spots (the areas with no wireless coverage), minimizing unwanted signal spillovers, and maximizing opportunities for implementing the Extend Service Set (ESS). ESS facilitates Internet connectivity for mobile nodes.

4.5 Physical Layer and Spread Spectrum

The purpose of a communication system is to transfer information. But transmission in baseband suffers from many problems. Firstly, baseband signals, being limited to few kHz, cannot fully utilize the bandwidth. Secondly, the noise due to external interferences and electronic circuits reduce the signal to noise ratio at the receiver. Thus, the receiver cannot receive the transmission properly. If the wire length is shorter than wavelength (as in base band), the wire would act as an antenna. Consequently, the biggest challenge originates from the requirement of infrastructure. For example, if we want to communicate in a signal bandwidth of 3000 Hz, the wavelength $\lambda = c/3.10^3 = 3.10^8/3.10^3$ = 100 km. The theory of antenna [5] tells us that any conducting material can function as an antenna on any frequency. Furthermore, the height antenna should be about one quarter of the wavelength in free space on smooth flat terrain. So, with λ = 100 km, the required height of antenna would be 25 km. Erecting vertical antennas reaching heights more than few meters is impractical. However, with modulation it is possible to reduce the length of the antenna which makes its erection practical. For example, if the signal is modulated with a carrier wave at 100 MHz, then λ becomes $c/10^8$ m = 3 m. So, an antenna height of (3/4) m = 75 cm would suffice for the communication.

4.5.1 Standard for PHY and MAC Layers

IEEE standards focus on the bottom two layers, physical (PHY) and medium access control (MAC) of the OSI model [14]. The Logical Link Layer specification is available in IEEE 802.2 standard. The architecture is designed to provide a transparent interface to the higher level layers for the clients. The client terminals may roam about in WLAN yet appear stationary to 802.2 LLC layer and above. So existing TCP/IP remains unaffected and need not be retooled for wireless networks. Figure 4.7 shows the different IEEE standards for MAC and PHY layers.

IEEE standards specify use of two different physical media for connectivity in wireless networks, namely, optical and radio. Infrared (IR) supports wireless optical communication. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are meant for radio based connectivity. Both IR and FHSS operate in 2.4 GHz band, while DSSS operates in 5 GHz band.

IR operates only in baseband, and is restricted to the Line Of Sight (LOS) operations. In order to minimize damages to human eye, IR transmission is restricted to about 25 m. The LOS requirement restricts mobility. But diffused IR signal [11]

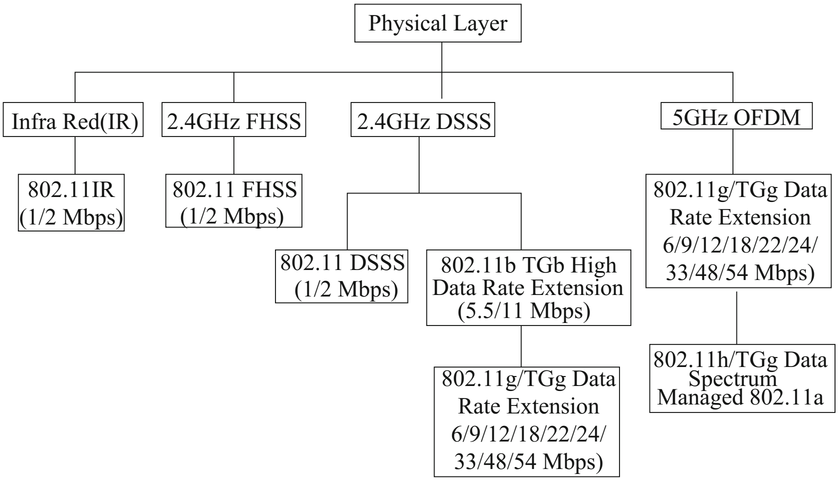

Physical Layer
Infra Red(IR)
2.4GHz FHSS
2.4GHz DSSS
5GHz OFDM
802.11IR (1/2 Mbps)
802.11 FHSS (1/2 Mbps)
802.11 DSSS (1/2 Mbps)
802.11b TGb High Data Rate Extension (5.5/11 Mbps)
802.11g/TGg Data Rate Extension 6/9/12/18/22/24/ 33/48/54 Mbps)
802.11g/TGg Data Rate Extension 6/9/12/18/22/24/ 33/48/54 Mbps)
802.11h/TGg Data Spectrum Managed 802.11a

Fig. 4.7 IEEE standard architecture for PHY and MAC layers

can fill enclosed area like ordinary light, so it offers a better option for operating in baseband. For diffused IR, the adapters can be fixed on ceiling or at an angle, so that signals can bounce off the walls, and consequently changing the location of the receiver will not disrupt the signal.

4.5.2 Spread Spectrum

Spread spectrum uses radio frequency transmission as physical layer medium. Two spread spectrum strategies are Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). FHSS is an intra building communication technology whereas DSSS is for inter building communication. Spread spectrum essentially spreads a signal, so that it can be transmitted over a wider frequency band than the minimum bandwidth required by the signal. The transmitter spreads the energy initially concentrated on a narrow band across a number of frequency band channels using a pseudo-random sequence known to both the transmitter and the receiver. It results in increased privacy, lower interference, and increased capacity. The generic technique of spread spectrum transmission is as follows:

1. Input is fed into channel encoder, it produces analog signal with narrow bandwidth.
2. Signal is then modulated using spreading code or spreading sequence. The spreading code is generated by pseudo-noise whereas spreading sequence is obtained by pseudo-random number generator.

The modulation increases the bandwidth of the signal to be transmitted.

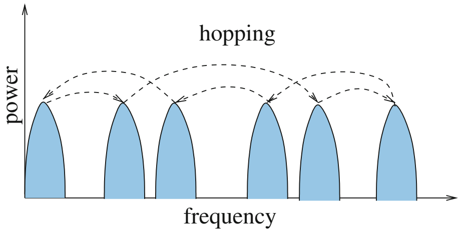


Fig. 4.8 Frequency hopping spread spectrum

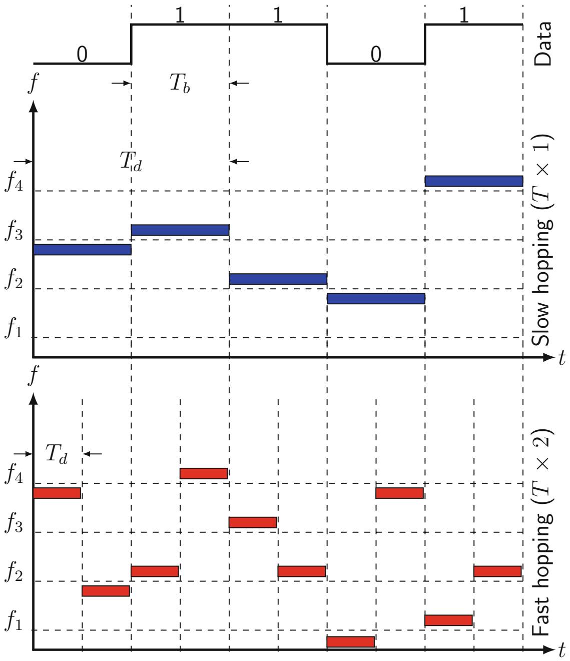
Figure 4.8 illustrates the transmission pattern of a FHSS radio. FHSS changes transmission frequency periodically. The hopping pattern of frequency is determined by a pseudo-random sequence as indicated by the figure. FHSS partitions the 2.4 GHz band into 79 channels, each of 1 MHz wide, ranging from 2.402 to 2.480 GHz. It allocates a different frequency hopping patterns for every data exchange. The signal dwell time cannot exceed 400 ms in a particular frequency. A maximum length packet takes about 30 ms. Thus, a small amount of data is sent on each channel for a designated time period before FHSS radio hops to a different frequency. After hopping, the transmitter resynchronizes with the receiver to be able to resume the transmission. The pseudo-random sequence of hopping pattern minimizes probability of interference. The radio spends only a small amount of time in any single carrier frequency. So, it would experience interference, if at all, only for that duration. The chance of experiencing interference in every carrier frequency is low. It is virtually impossible to design any jammer for FHSS radios. FHSS comes in three variants, namely, slow frequency hopping (SFH), intermediate (rate) frequency hopping (IFH) and fast frequency hopping (FFH).

Let T_h be the hop period and T_b be the bit period. A SFH transmitter uses a frequency for several bit periods. Equivalently, T_b is smaller than T_h in a SFH, i.e., $T_b = T_h/k$, for $k = 1, 2, 3, \ldots$. Thus, in a SFH the base band message rate $R_b = 1/T_b \geq R_h$. As shown in Fig. 4.9, the transmitter $Tx1$ uses frequency $f3$ for $2T_b$ periods. The period for which a transmitter uses the same frequency is referred to as *dwell time* T_d. For slow hopping, $T_d \geq T_b$. Figure 4.9 also shows hopping pattern for transmitter $Tx2$. It dwells in a particular frequency for half the T_b period. In general, for FHF $T_d < T_b$, and $T_b = kT_h$ for $k = 1, 2, 3, \ldots$. The number of frequency hopping for $Tx2$ is twice the number for $Tx1$. Bluetooth system uses frequency hopping spread spectrum.

FHSS uses only a small portion of bandwidth at any time. As opposed to FHSS, DSSS uses a fixed carrier frequency for the transmission. But instead of using a narrow band, it spreads the data over a wide frequency band using a specific encoding scheme called PN (pseudo-noise) code. The justification of spread spectrum is provided by Shannon-Hartley channel capacity equation [12]

$$C = B \times \log_2(1 + S/N).$$

Fig. 4.9 Frequency hopping spread spectrum



In the above equation, C represents the capacity in bits per second which is the maximum data rate for a theoretical bit error rate (BER). B is the bandwidth and S/N is signal to noise ratio. Since, S/N represents environmental condition, and the frequency is limited, the equation essentially means that B is the cost to be paid if the performance, C, is to be increased. Another way to look at the equation is that even in difficult environmental condition, i.e., when S/N is low, it is possible to increase performance (C) by injecting more bandwidth. Now let us try to eliminate $\log_2$ term from the above equation. Converting the log term in base 2, and assuming $S/N \ll 1$,

$$\begin{aligned} C/B &= (1/\ln 2) \times \ln(1 + S/N) \\ &= 1.443 \times ((S/N) - (1/2) \times (S/N)^2 + (1/3) \times (S/N)^3 - \dots \\ &= 1.443 \times (S/N), \text{ neglecting higher order terms.} \\ &\approx S/N \end{aligned}$$

The above simplified equation implies that for a given noise to signal ratio, error free transmission can be ensured by spreading which is equivalent to increasing bandwidth. As along as, the PN codes are orthogonal, data of users can be distinguished from one another on the basis their respective PN codes even if these data occupy the same spectrum all the times. The pseudo-noise code is more popularly referred to as chipping sequence. To transmit each bit of actual data, a redundant bit pattern of bits or *chips* is generated. For example, as shown in Fig. 4.10 a single bit of data

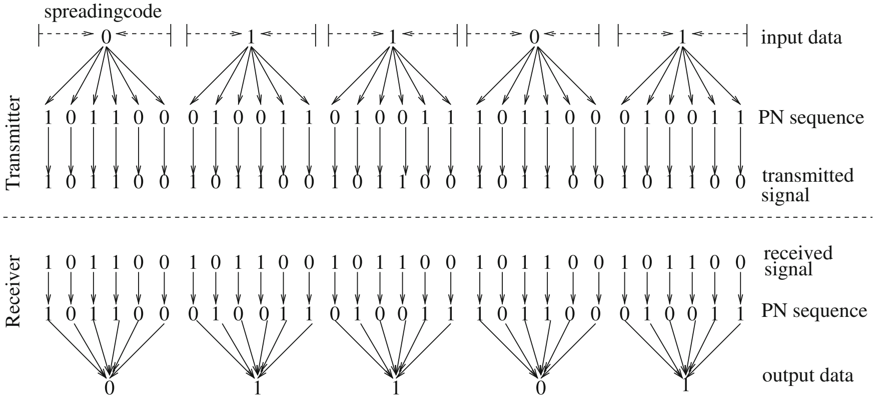


Fig. 4.10 DSSS using with spreading factor 6

is represented by six chips.This implies that each user's bit has a duration T_b, while the chipping sequence consists of smaller pulses or "chips" such that each chip has a duration of T_c ($\leq T_b$).

Instead of using 0 and 1 for chips, a bipolar notation where -1 replaces 0 and $+1$ replaces 1, is more commonly used for denoting the chip sequence. The ratio T_b/T_c is called *spreading factor*, which represents the number of chips used for one bit of actual data. Longer the spreading ratio, more resistent is the transmitted data to interference. Equivalently, the probability of recovering the actual data is high. In most applications involving private/public communication, a spreading factor between 10 and 100 is used. As opposed to that, the applications related to military and security may use spreading factors upto 10,000. IEEE 802.11, for example, employs Barker code [2] sequence 10110111000, which has a spreading factor of 11. Barkar code is short, have a good balance (difference between 1s and 0s is small) and exponentially decreasing number of run lengths ($1/2^k$ of the runs have length 2^k, $k = 0, 1, \ldots$). and exhibit good correlation properties. Since adjacent bit correlation is very low, Barkar codes are ideal for CDMA [10]. Also Shanon-Hartley's equation tells us that lower the spreading factor, higher is the bandwidth available to the user.

It may be noted that the chipping code is related to a user, and independent of data or signal. If a sequence such as 101100 is used for encoding 0 then the 1's complement of the sequence, 010011 is used for encoding 1 as depicted in Fig. 4.10. The product (bitwise XOR) of the spreaded data is transmitted. Since the radio transmission is analog, the spreaded data should be modulated with a radio carrier before transmitter can actually send it. For example, if a user's signal requires a bandwidth of 1 MHz, employing 11-chip Barker code would result in a signal of 11 MHz bandwidth. After converting the digital data to analog signal, the radio carrier has to shift this resulting signal to the carrier frequency, i.e., 2.4 GHz band.

For recovering data at the receiver end, the two step modulations of transmitted data is reversed using the same carrier as the transmitter. It results in the signal which is of the same bandwidth as the original spreaded signal. Some additional filters may be used to generate this signal. The receiver must use the same chipping sequence as employed by the transmitter's end in order to recover the spreaded data by one XOR operation. The receiver should be synchronized precisely with the transmitter in order to know this chipping sequence and bit period. During a bit period, an integrator adds all these products. The process of computing products of chips and signals, and the adding of the products in an integrator is known as the *correlation*. The device executing the process is called a *correlator*. After the sum of products are made available by the integrator, a decision unit samples these sums for each period and decides if a sum represents a 0 or an 1.

For the output at the receiver end to be identical to actual data, the following equation must hold:

$$s_i(t).c_i(t).c_i(t) = s_i(t),$$

where $s_i(t)$ is signal, $c_i(t)$ is the spreading code for ith mobile. In other words, the spreading code must be such that $c_i(t).c_i(t) = 1$. After recovering the spreaded data, it is multiplied (bitwise XOR) with the chip sequence corresponding to transmitter and integrated. To illustrate this, let us take a small example with 11-bit Barker code 10110111000. Let the actual data be 011. Barker code spread binary 0 to 10110111000 and binary 1 to 01001000111. So the spreaded code for actual data 011 is equal to:

[10110111000 **01001000111 01001000111**]

The XOR operation of spreaded data with Barker chipping sequence followed by the integrator's sum at the end of each bit-stream interval will be shown below.

$$\begin{array}{r l}
\text{spreaded data:} & [10110111000\ \mathbf{01001000111}\ \mathbf{01001000111}] \\
\text{chip sequence:} & [10110111000\ \mathbf{10110111000}\ \mathbf{10110111000}] \\ \hline
\text{XOR:} & [00000000000\ \mathbf{11111111111}\ \mathbf{11111111111}] \\ \hline
\text{sums over } T_b, 2T_b, 3T_b : & \quad (0)_{10} \qquad\qquad (11)_{10} \qquad\qquad (11)_{10}
\end{array}$$

The sum over a chip interval would map either to binary 0 or 1. In the above example, sum $(0)_{10}$ maps to 0, whereas sum $(11)_{10}$ maps to 1. So, the data received is 011. In general, integration does not result in a clear distinction between 0 and 1 as shown above. This necessitates use of a threshold comparator to take care of the worst case scenario with maximum number of channels in the system. With the above technique, even if one or more chips are flipped in transmission due to noise, it would be possible to get the correct information. As an example, suppose we use 11 bit Barkar code and the information received is such that

- two of the bits were flipped in the first and the third blocks, and
- one of the bits was flipped in the second block,

as shown below:

$$\begin{array}{r|ccc}
\text{spreaded data:} & [10110111000 & \mathbf{01001000111} & \mathbf{01001000111}] \\
\text{received:} & [00100001000 & \mathbf{11110111111} & \mathbf{11011110111}] \\
\hline
\text{sums over } T_b, 2T_b, 3T_b: & (2)_{10} & (9)_{10} & (11)_{10}
\end{array}$$

Then the threshold comparator can still map the information received to 011.

DSSS uses more bandwidth than FHSS, yet considered to be more reliable and rejects interference. The processing gain G is provided by the ratio of spreading bandwidth against the information rate R, i.e., $G = B/R$. Note that the information rate R is the inverse of bit stream interval T_b. Consequently, the signal to noise ratios for input and output are related by the processing gain as follows.

$$(S/N)_{out} = G \times (S/N)_{in}.$$

Similarly, the bandwidth requirement is $1/T_c$, where T_c is chip interval. So, processing gain G can be alternatively expressed as the ratio T_c/T_b.

Since, distinct orthogonal scrambling codes are used, the user data can be distinguished from the data mix at the receiver end. Spreading introduces redundancy in data, so even if some bits are damaged in transmission user data can be recovered without the need for the retransmission of signal.

4.5.3 Protocol Stack

The physical layer corresponds more or less to the OSI physical layer. Physical layer has a variety of implementation options, namely, IR, Bluetooth or FHSS, 802.11a OFDM, 802.11b DSSS, 802.11g OFDM, etc. Each one will also have a MAC sublayer. Together with logical link layer, MAC sublayer constitutes the Data Link Layer as indicated in Fig. 4.11.

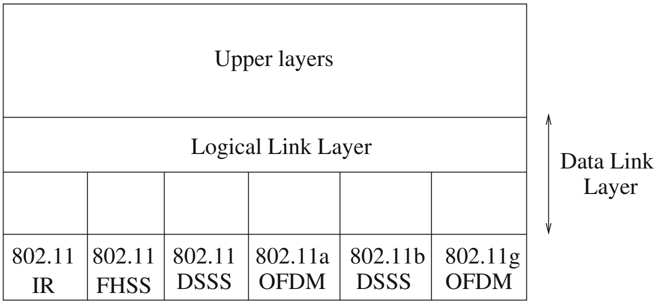


Fig. 4.11 Protocol stack for 802.11

4.6 MAC Sublayer

The responsibility of medium access control (MAC) layer is to ensure that radio systems of different nodes share the wireless channels in a controlled manner, i.e., with mutual fairness and without collisions. The two resources of a radio system are (i) frequency, and (ii) time. So, the radio access methods of wireless channels can be classified either in frequency domain or in time domain. In frequency domain, sharing is ensured by using non-overlapping frequency bands within the allocated communication spectrum. On the other hand, sharing in time domain is made possible by allowing entire bandwidth to each node for a short period of time called *slot*. Since, data transmission can be carried out in bursts, sharing is possible among multiple nodes in both frequency and time domains. In this type of sharing scheme, each user can use a certain frequency on certain time slots. The idea of two dimensional sharing is extended to a third dimension where multiple senders use orthogonal code sequences to send data at the same time in full bandwidth. Orthogonal codes ensures that concurrent communications can be separated at the receiving ends using the respective orthogonal codes employed by the transmitters. The sharing of wireless channels in this way can be referred to as sharing in code domain.

4.6.1 Radio Access Technologies

Thus, in summary the different access technologies used by the radio systems are:

1. FDMA: assigns channels using distinct frequencies in frequency domain.
2. CDMA: assigns orthogonal code sequences in code domain.
3. TDMA: assigns time slots for transmission in time domain.
4. CSMA: assigns transmission opportunities on statistical basis on time domain.

In FDMA, a frequency is allocated to a transmission on demand. It will remain engaged until the transmission is over. A frequency can be reallocated for another transmission only when the ongoing transmission on that band is complete. But, a channel sits idle when not in use. Normal channel bandwidth is 30 kHz with guard band of 30 kHz. FDMA is best suited for analog transmission. Since transmission is continuous, it does not require any framing or synchronization. But tight filtering is required to reduce interferences.

TDMA supports multiple transmissions by allocating frequency for a specified time slot to each transmission. Once the slot time is over, the same frequency may be assigned to another transmission. TDMA allocates further time slots to an unfinished transmission in future to complete the communication. It may, thus, be viewed as enhancements over FDMA achieved by dividing spectrum into channels by time domain. Only one user is allowed in a time slot either to receive or to transmit. Slots are assigned cyclically.

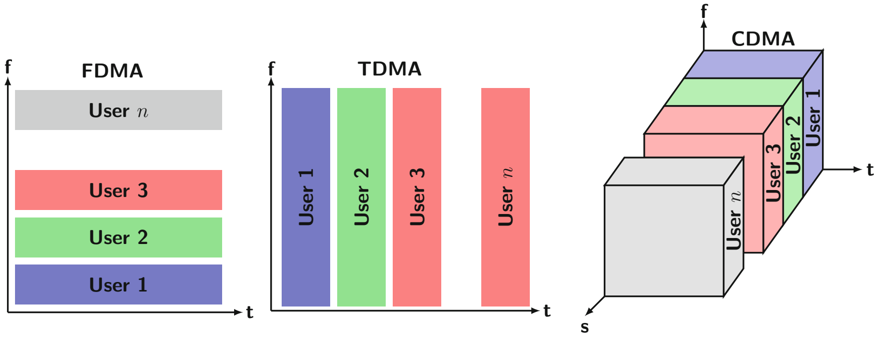


Fig. 4.12 Contrasting different access technologies

CDMA utilizes entire spectrum for each transmission. Each transmission is uniquely coded using a randomly generated code sequence which are known before hand to both sender and the receiver (they synchronize). Then the data is encoded using random code sequence before transmission. Since code sequences are orthogonal, transmitted data can be recovered at receiver end even if the receiver gets a combination of different transmissions by different senders in the same time span. Figure 4.12 shows hows multiple transmissions are carried out using different access technologies.

CSMA (Carrier Sensing and Multiple Access) is a statistical based technique for allowing opportunity of radio access for transmission to competing station. The idea is derived from human way of carrying out conversation. Listening to channel before initiating a transmission could save unnecessary efforts in retransmissions by avoiding probable collisions. Before initiating a transmission, a station senses the channel, and if a signal is detected then the initiating station defers its transmission.

4.6.2 Multiple Access Protocols

Each mobile station has a wireless interface consists of transmitter unit and receiver unit. These units communicate via a channel shared among other different mobile stations. Transmission from any node is received by all nodes. This creates the problems of contentions. If more than one station transmit at the same time on the same channel to a single node then the collisions occur. Thus, a protocol must be in place for the nodes to determine whether it can transmit on a specific channel. Such a protocol is referred to as a multiple access protocol. Multiple access protocols are of two different types, namely,

1. Contention protocols: these protocols function optimistically, and try to resolve contention by executing a collision resolution protocols after each collision.
2. Conflict-free protocols: these protocols operate by preventing any occurrence of a collision.

4.6.3 ALOHA

ALOHA is a simple minded contention type MAC protocol developed at the University of Howaii [1, 3]. There is no explicit allocation of a shared channel for communication under the pure ALOHA scheme. The transmitting stations start sending whenever they have data. Under this scenario, collisions do occur and the received frames are often damaged. Since wireless transmissions are broadcast based, the sending stations can determine the collisions by listening to the channel. When a collision is detected the sending station backs off for a random time before attempting a retransmission. In absence of possibility of listening, acknowledgements are needed to determine if the sent data were received correctly.

A possible scenario of transmission of frames in pure ALOHA involving three transmitting stations is depicted in Fig. 4.13. There is just one receiver and many senders. Each sender may send new frames and also retransmit the frames which were damaged due to collisions. It implies there may be attempts to transmit several frames per frame time, taking into account both new and old (due to retransmissions) frames. The question one would ask is why this simple scheme may work at all? This can be answered best by analyzing its performance.

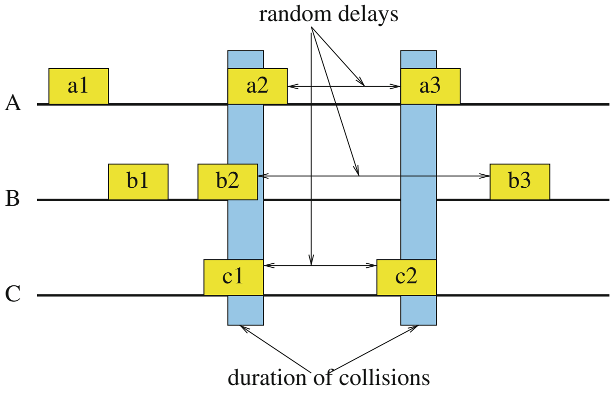


Fig. 4.13 Frames generation and transmission under pure ALOHA

For the convenience of analysis, following assumptions are used:

1. Total number of stations is N.
2. Frames are of equal length, i.e., frame time is t.
3. All user transmits with a probability p during time t.

According to the above assumptions, the average number of frames in a pure ALOHA system is Np. The stations are assumed to operate independently. So, the frame transmissions are independent events which can be modeled by Poisson distribution

$$P(k) = \frac{\lambda^k e^{-\lambda}}{k!},$$

where $\lambda = Np$ is the frame transmission rate, and $P(k)$ is the probability of k transmission occurring in a frame time t.

Let the time be divided into slots of frame time t. So, frame transmission started by a station at time $t_0 + t$ suffers a collision if some other station generates a frame in time intervals $(t_0, t_0 + t)$ and $(t_0 + t, t_0 + 2t)$. It implies that the period of vulnerability of a frame in transmission is $2t$. In other words, a generated frame always gets successfully transmitted provided there is no other frame available for transmission during its vulnerable period of $2t$. The probability $P_0[2t]$ for no traffic being generated during time $2t$ is obtained from the Poisson distribution with rate $\lambda' = 2Np$:

$$P_0[2t] = \frac{(2Np)^0 e^{-2Np}}{0!} = e^{-2Np},$$

Throughput is obtained by multiplying $P_0[2t]$ and the mean number of frames available for transmission during a frame time, which is:

$$P[success] = Np.P_0[2t] = Np.e^{-2Np}.$$

The maximum value of $P[success]$ occurs at $Np = 1/2$, i.e., $P_{max}[success] = 1/2e$ = 0.184. Equivalently, throughput is just 18.4%. Though the performance is bad, ALOHA does work.

A variation of pure ALOHA is slotted ALOHA which doubles the capacity. In this protocol, the time is divided into slots of size equal to frame time. A station has to agree to align each transmission with a slot boundary. So, whenever a station has a packet to send, it wait till the beginning of the next slot boundary. So the collision can occur only during the interval of a slot. It leads to cutting down the period of vulnerability to half as compared to pure ALOHA. So, the probability that no other frame is generated during a frame time $P_0[t] = e^{-Np}$. Therefore, the probability that a frame will not suffer a collision during its transmission is $P[success] = Np.e^{-Np}$. This implies that the maximum throughput achievable in slotted ALOHA is $1/e$, i.e., 36.8%.

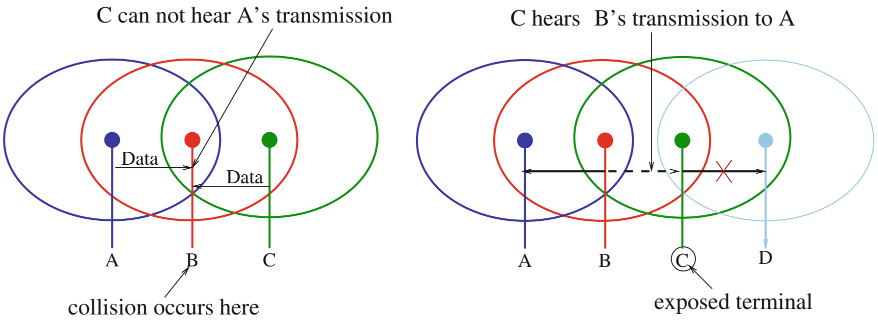
4.6.4 CSMA/CA

As explained in Sect. 4.6.1, CSMA is a probability based multiple access scheme for radio resources for WLAN. IEEE standard specifies two ways to resolve contention in medium access through CSMA when multiple nodes attempt to transmit simultaneously. It supports two transmission modes, viz., asynchronous and synchronous:

1. Distributed Coordination Function (DCF) is a mechanism for resolving contention without a central arbiter when access attempts were made independently by a multiple number of stations. The protocol resolves contention by employing virtual carrier sensing.
2. Point Coordination Function (PCF) is a mechanism for restricted resolution of contention within infrastructure BSS. It does so with help of a coordinator residing in access point itself.

DCF supports asynchronous mode while synchronous mode is supported by PCF. Since PCF supports synchronized mode, it provides a connection oriented mode. Implementation of DCF is mandatory in all 802.11 equipment, but PCF's implementation is optional. Furthermore, implementation of PCF relies on DCF. It cannot operate in ad hoc mode, while DCF can operate in both independent and infrastructure modes.

Since, PCF depends on DCF, let us examine DCF first. DCF supports asynchronous mode of transmission. The major problem in design of DCF is in handling hidden and exposed terminals. The hidden terminal problem, as shown in Fig. 4.14a, occurs if the transmitting station accesses the medium even when another station is actually using the medium. Using carrier sensing, station A is not able to detect presence of carrier as A is not in the range of C. So, it accesses medium for transmitting to B when C is actually transmitting data to B. A and C are hidden from each other. The crux of the problem is that the absence carrier does not necessarily mean idle medium.


C can not hear A's transmission
Data
Data
A
B
C
collision occurs here
C hears B's transmission to A
A
B
C
D
exposed terminal

(a) Hidden terminal. (b) Exposed terminal.

Fig. 4.14 Hidden and exposed terminal problems

The exposed terminal case, as indicated by Fig. 4.14b, occurs when stations A and B are already talking, and station C, which is within B's range, wrongly concludes the carrier to be busy overhearing the ongoing transmission between A and B, and refrains from initiating exchanges with D. Stations C and D are exposed terminals. So, in the context of exposed terminals, the problem is other way round, i.e., the presence of carrier does not necessarily mean busy medium.

4.6.5 Distributed Coordination Function

DCF solves both hidden and exposed terminals problems by getting rid of carrier sensing. The protocol CSMA/CD is modified as CSMA/CA. That is, collision detection (CD) is replaced with the mechanism of collision avoidance (CA). In CSMA/CA, a transmitting station first checks to ensure that channel is free for a fixed duration of time. Each station then chooses to wait for a randomly chosen period of time. From among the contending stations, the station whose waiting time expires first gains access to the channel. The randomly chosen waiting time for a station is known as its backoff timer. As soon as the channel is occupied by a station, the countdown of back timer in each unsuccessful station is suspended until the channel becomes free again.

To understand the role of backoff timer and collision avoidance, a more detailed examination of DCF protocol is needed. DCF consists of a basic mode and an optional RTS/CTS access mode. In the basic mode, sending station senses channel before transmitting. If the medium is free for a DIFS interval it is assumed to be free. The sender then waits for backoff period and starts sending. The backoff period is set from an interval $[0, W - 1]$, where W is set to a pre-specified value, and is known as contention window.

4.6.5.1 DCF Basic Mode

For the basic DCF mode, the MAC frame transmission logic is provided in Fig. 4.15.

When a station wishes to transmit multiple number of packets, the protocol forces every subsequent packet except the first one to have a minimum of one random backoff even if the channel is free. Therefore, the generation of a random backoff is enforced after the transmission of the first packet. If by chance backoff timer is set to 0 every time the attempt to transmit a new packet is made then the sender could cause other contending stations to wait for indefinite time.

Once a station gains the access of the medium, the countdown of backoff timers of all other contending stations is suspended. The countdown is resumed when the medium becomes idle again for DIFS period. The use of backoff timers has three important uses:

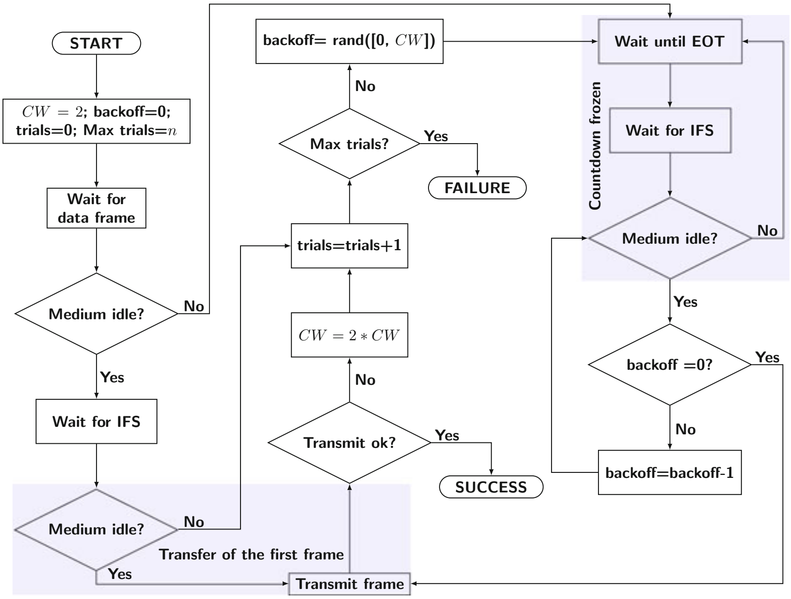


Fig. 4.15 Logic of DCF basic transmission mode

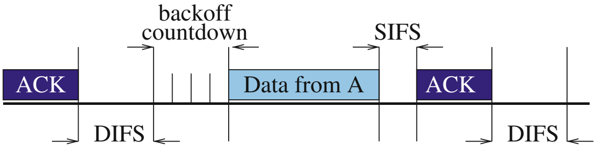


Fig. 4.16 Data transmission from one station to another

1. *Collision avoidance*: avoid collision among contending stations,
2. *No starvation*: no waiting station will be blocked from gaining access of medium indefinitely,
3. *Bounded wait*: the stations waiting for a longer time gain priority over other waiting stations.

The process of transmitting data from a station A to another station B is illustrated in Fig. 4.16.

A collision may still occur in the case when backoff timers of two or more contending stations simultaneously reach zero countdown. In this case, each sending station must choose a random backoff value to avoid repeated collision. The value of the random backoff is:

$$backoff = \lceil rand() \times slotTime \rceil,$$

where i is number of consecutive failures, *rand*() is chosen from interval $[0, W - 1]$, and slot time is 20 µs. The contention window is set dynamically, when a station successfully completes a data transfer it restores the window value W to W_{min}. The value of contention window is doubled, each time a station fails to transmit a frame, until it reaches the maximum value W_{max}. It implies the value $W \in [W_{min}, W_{max}]$. The failure of data transmission is determined by non-receipt of acknowledgement within specified time interval.

For unicast data transfer, the receiver sends an ACK. An ACK packet has a higher priority because if a station is made aware of successful transfer, it would not retransmit the data. This helps to cut down the pressure on the available bandwidth. To ensure that transmission of ACK is not cut in the race among the contending stations trying to access of the medium, the receiving station (which wishes to send ACK) waits only for a Short InterFrame Spacing (SIFS). The typical value of SIFS is 10 µs, whereas DIFS = 2 × $slotTime$ + SIFS = 50 µs.

4.6.5.2 DCF Advanced (RTS/CTS) Mode

In RTS/CTS mode, at first a dialogue is initiated between the sender and the receiver. The sender sends RTS (request to send) which is a short message. RTS contains NAV (network allocation vector) that includes times for

1. Sending CTS (clear to send),
2. Sending actual data, and
3. Three SIFS intervals.

A CTS is sent by a receiver to a sender in order to signal the latter to access the medium. CTS is considered as a short high priority packet much like ACK. So, before gaining access to medium, for sending CTS, the receiver waits for SIFS time. After the CTS is received by the sender, it just waits for SIFS time before accessing the medium, and following which the sender starts to send data. Finally, when the data have been received, the receiver waits for a SIFS time before sending the ACK. This explain why 3 SIFS are needed along with the time for sending CTS and data. CTS also includes NAV, so that other station trying to gain access to medium would know the duration for which the medium will remain busy between the sender and the receiver. But NAV of CTS does not include CTS itself unlike NAV of RTS. The RTS/CTS mode of DCF is illustrated in Fig. 4.17. As indicated in the figure, once A has been cleared by B for sending, C has to wait till

$$\text{DIFS} + \text{NAV(RTS)} + contention\ interval$$

before it can try to gain access to the medium.

By including NAVs, the stations involved in exchange of RTS and CTS inform other stations in their respective neighborhood about the duration of time the conversation would continue. In other words, these stations receive carrier busy information in advance.

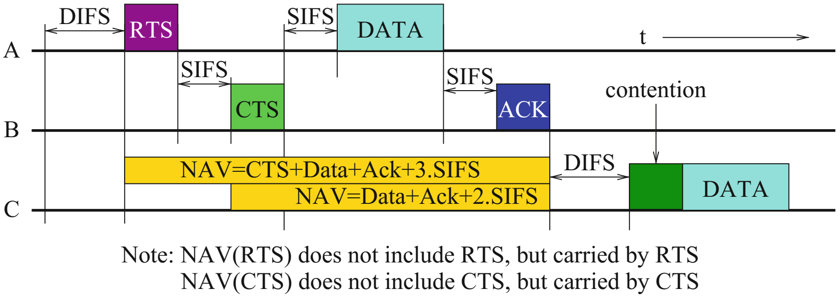
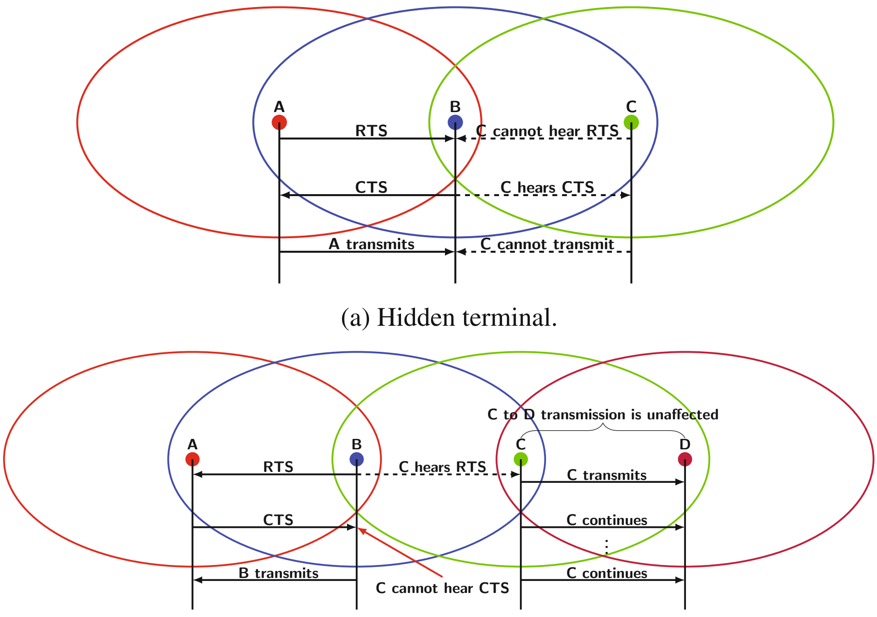

DIFS
RTS
SIFS
DATA
t
A
SIFS
CTS
SIFS
ACK
contention
B
NAV=CTS+Data+Ack+3.SIFS
DIFS
NAV=Data+Ack+2.SIFS
DATA
C
Note: NAV(RTS) does not include RTS, but carried by RTS
NAV(CTS) does not include CTS, but carried by CTS

Fig. 4.17 DCF RTS/CTS mode of transmission

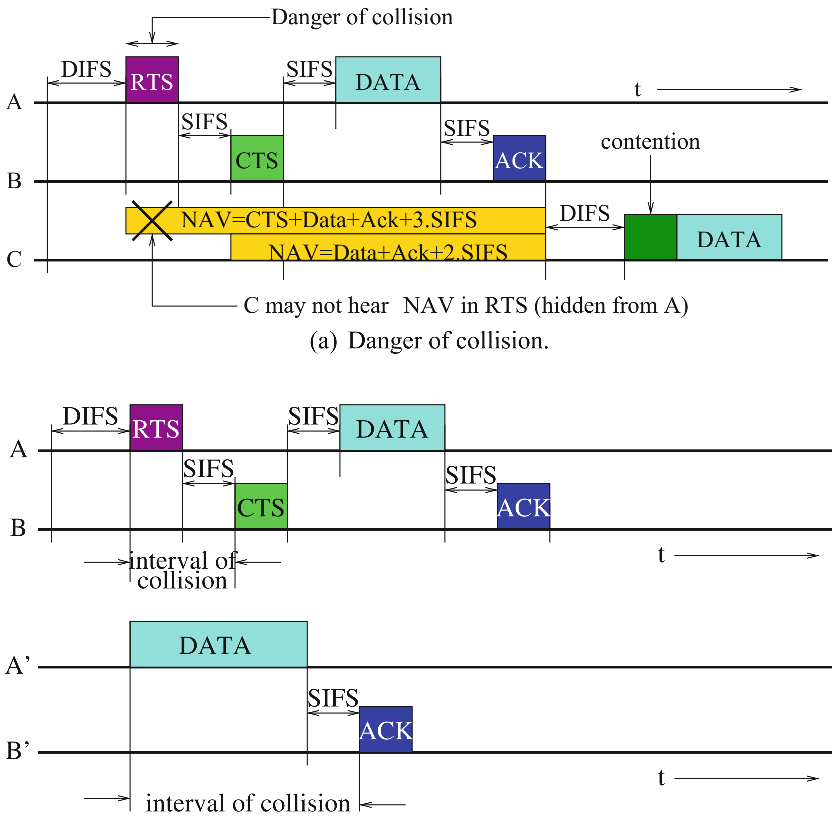


(a) Hidden terminal.

(b) Exposed terminal.

Fig. 4.18 Solutions to hidden/exposed terminal problem

DCF with RTS/CTS mode solve both hidden and exposed terminal problems. The solution to hidden and exposed terminal problem is illustrated by Fig. 4.18. In hidden terminal problem (see Fig. 4.18a) station *C* becomes aware of medium being busy when it hears the CTS from *B* in response to RTS request from *A*. So, *C* defers its attempt to access the medium until NAV set in CTS from *B* expires. To understand how RTS/CTS mode solves exposed terminal problem refer to Fig. 4.18b. The RTS sent by station *B* to station *A* is heard by station *C*. However, *C* being not in range of *A*, does not hear the CTS from A. Therefore, *C* would conclude that the carrier is free, and may initiate a RTS/CTS dialogue with *D*.



(a) Danger of collision.

(b) Collision interval.

Fig. 4.19 RTS/CTS mode shortens interval of collision in DCF

Still there is a possibility of a collision even in RTS/CTS mode. This is exhibited by Fig. 4.19a, where a station C, not being in the range of station A, is unable to hear RTS sent to station B. However, the interval of collision in RTS/CTS mode is limited to RTS plus the SIFS interval as indicated by Fig. 4.19b. The figure also provides a comparison of the intervals of collision in two modes of DCF. In DCF basic mode, the interval of collision is equal to the duration of data transmission plus the SIFS interval which may at times be unpredictably long.

4.6.5.3 Monitoring of Misbehaving Stations

There may be a smart station which uses a number of tricks to increase its chance of accessing the medium in order to increase its throughput. If traffic is known to be bursty, then a misbehaving station could send burst of packets ignoring MAC rules and minimize its average delay. Some of these tricks could be [4, 8]:

- Node may choose backoff timer from a smaller range of values than the contention window range $[0, W - 1]$.
- Contention window is not doubled after a collision.
- DIFS, SIFS and PIFS are not used properly. For example, a node may delay CTS and ACK; or instead of waiting for DIFS time, the node may transmit when it senses the channel to be idle.
- When exchanging RTS-CTS, NAV can be set to a value much larger than actually needed.

By using the first trick, a station gets an unfair advantage in accessing the medium ahead of other contending stations, since countdown of backoff timer of the misbehaving station reaches 0 faster than that of others. With the second trick, a misbehaving station can always outsmart other well-behaved stations when a collision occurs.

We need some solutions to block the unfair advantages that a misbehaving station might gain by resorting to trick mentioned above. Some possible approaches could be

1. Monitor throughput of each sender.
2. Monitor the distribution of per packet backoff for each sender.
3. Receiver side detection mechanisms.

Monitoring requires a delay. Because the relevant meta data must be logged for a while before an analysis can be done. Furthermore, sending station can choose a random backoff but send burst of traffic in a bursty traffic environment to ward off monitoring mechanism. The receiver side solution looks better. The access point can monitor each of the sender's behavior. The receiver side monitoring process is explained in Fig. 4.20. The receiver side solution is summarized as follows.

1. The receiver assigns a backoff b to the sender. So, the receiver can control the backoff behavior and the monitoring becomes simple.
2. The receiver then verifies whether the sender has actually backed off for an interval exceeding assigned backoff.
3. If observed backoff is less than assigned backoff then the receiver adds extra penalty to new backoff.

The use of RTS-CTS handshake was proposed mainly for solving hidden and exposed terminal problem through virtual carrier sensing mechanism. It also improves throughput by reducing the probability of collisions by limiting the period of collision to a short interval (bounded by RTS+SIFS). However, the stations involved in RTS collision fail to get CTS, and prevented from sending data. The network also incurs

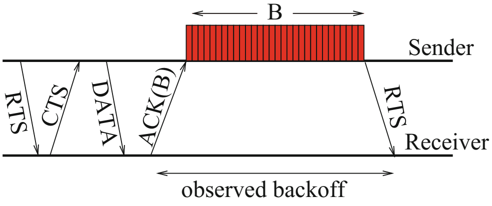


Fig. 4.20 Receiver side solution to check LAN misbehavior

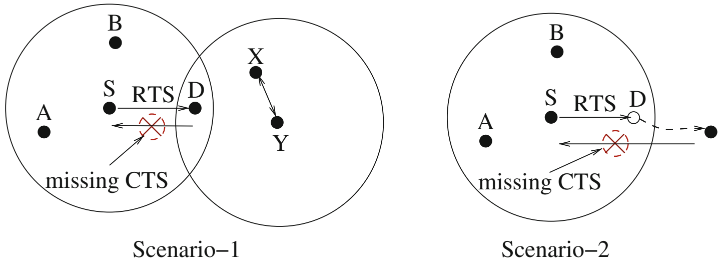


Fig. 4.21 Effects of missing CTS

an overhead due to increase in number of RTS-CTS control packets. As the number of RTS-CTS packets increases, the probability of RTS collision also increases. Though an analysis of overhead is difficult due to complexity and unpredictability of wireless environments, there is a possibility of under-utilization of channel capacity due to implementation of virtual carrier sensing mechanism. It may occur due to non-receipt of a CTS. Two scenarios involving missing CTSs and their effects have been illustrated in Fig. 4.21. In the first case, there is an ongoing communication between stations$X$ and Y. On overhearing the above exchange, station D concludes that carrier is busy and would not send CTS to S's RTS. The problem may get aggravated further, as stations A and B which are in range of S on hearing RTS set their NAVs. So, A and B would be prevented from communicating until their NAVs expire. In the second case, the destination node D simply has moved to a new location and unable to respond to RTS from S. However, A and B set their NAVs on hearing RTS from S. The CTS never materializes from D, but the NAVs set by A and B prevent both from engaging into a conversation.

It may be noted that IEEE 802.11 standard specifies use of the same MAC layer for different physical layer implementations like IR, FHSS and DSSS. However, the numerical values of MAC parameters such as slot time, SIFS, DIFS, frame size, etc., are different for different physical layer implementations.

4.6.6 Point Coordination Function

The Access Point (AP) works as the coordinator for PCF. The time is divided into superframes each consisting of a Contention Allowed Period (CAP) and a Contention Free Period (CFP). The maximum duration of a superframe should be bounded to allow both contention and contention free traffic to co-exist. The contention period should give sufficient time to send at least one data frame. The maximum duration for CFP is denoted by CFP$_{max}$. DCF is used during CAP and PCF is used during CFP. PCF polls individual nodes in its polling list, which is arranged according to the priorities, to find when they can access the medium. To block DCF stations from interrupting CFP, PCF uses a PCF InterFrame Spacing (PIFS) between PCF data

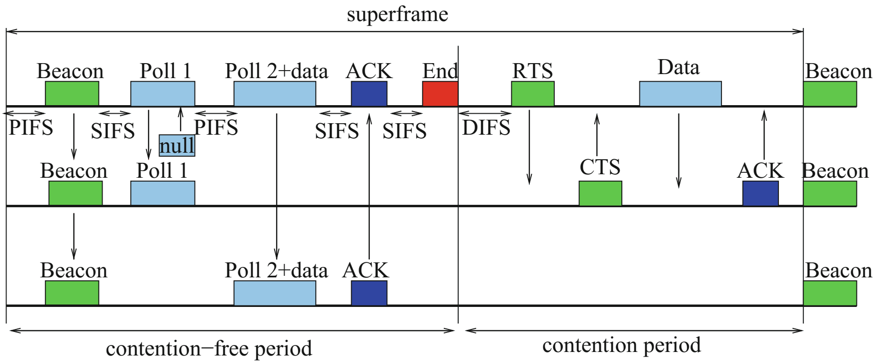


Fig. 4.22 Superframe structure and PCF

frames which is shorter than DCF InterFrame Spacing (DIFS). In order to prevent starvation during CFP, there should be space for at least one maximum length frame to be sent during CFP. It ensures that every station is allowed to send at least one frame.

The access point which acts as the coordinator, polls the stations in the round robin fashion. The polled station must always respond. If there is no data to be sent then a polled station must respond with a null frame. If all stations cannot be polled during a CFP, then the polling is resumed at the next station during next CFP. If a polled station is unsuccessful in sending data then it may retransmit data during subsequent CFP when polled.

Figure 4.22 provides the structure of the superframe. At the beginning of every contention free period, the AP sends beacon frame to all station in basic service area (BSA) after it finds the medium to be idle for PIFS interval. The beacon frame contains CFP$_{max}$, beacon interval, and the BSS identifier. All stations in the BSS set their network allocation vector (NAV) appropriately, and do not attempt to initiate CAP communication during CFP after a CFP-begin beacon has been received.

AP polls each station in its polling list by sending a data and CF-poll frame. When a station receives Data and a CF-poll frame, it responds after waiting for SIFS period. The response would consist of Data and CF-ACK frame or only CF-ACK frame (with no payload). AP after receiving frames from the station may again send Data, CF-ACK, a CF-poll frame or just Data and a CF-poll frame. Notice that if CF-ACK not received from AP then it indicates that data has not been received. Once again the receiving station responds to AP with Data or null frame as explained above. AP continues the polling of each station until it reaches CFP$_{max}$ time. When time bound is reached the AP terminates contention free period by sending a CF-end frame.

References

1. N. Abramson, The ALOHA system—another alternative for computer communications, *Fall Joint Computer Conference* (AFIP Press, 1970), pp. 281–285
2. R.H. Barker, Group synchronizing of binary digital sequences. Commun. Theor. 273–287 (1953)
3. R. Binder, N. Abramson, F. Kuo, A. Okinaka, D. Wax, ALOHA packet broadcasting—a retrospect, *1975 National Computer Conference* (AFIPS Press, 1975), pp. 203–215
4. H. Li, M. Xu, Y. Li, Selfish MAC layer misbehavior detection model for the IEEE 802.11-based wireless mesh networks, *The 7th International Symposium, APPT 2007*, vol. LNCS-4847 (2007), pp. 381–391
5. Y. Huang, K. Boyle, *Antennas: From Theory to Practice* (Wiley, 2008)
6. S. Kerry and The Author Team IEEE-SA, Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications (2007)
7. B.P. Kraemer and The Author Team IEEE-SA, Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications (2009)
8. P. Kyasanur, N.H. Vaidya, Selfish MAC layer misbehavior in wireless networks. IEEE Trans. Mobile Comput. **4**(5), 502–518 (2005)
9. B.G. Lee, S. Choi, *Broadband Wireless Access and Local Networks: Mobile WiMAX and WiFi* (Artech House, 2008)
10. A. Mitra, On pseudo-random and orthogonal binary spreading sequences. Int. J. Inf. Commun. Eng. **4**(6), 447–454 (2008)
11. E.L. Oschmann, J.P. Welch, Wireless diffuse infrared LAN system (1994)
12. C.E. Shannon, The mathematical theory of communication. Bell Syst. Techn. J. **27**, 379–423 (1948)
13. IEEE-SA standard board, Part 11: Wireless LAN medium access control (mac) and physical layer (phy) specifications: higher-speed physical layer extension in the 2.4 Ghz band (1999)
14. A.S. Tanenbaum, *Computer Networks*, 6th edn. (Prentice Hall, 2015)
15. The Author Team-IEEE-SA, IEEE 802.11n-2009-amendment 5: enhancements for higher throughput (2009)