WLAN and Short Range Radio Communication

R. K. Ghosh

January, 2008

5.1 Introduction

All radio based communication technologies are based on cellular architecture. However, the major technological hurdle in use of radio communication is the ability to build seamless convergent solutions for mobile users. Accessing services across heterogeneous networks is still problematic for mobile users. The challenges encountered in this respect are enormous mainly due to 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 traffic delivery.

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

The focus of this chapter is on wireless data networks that are relevant to computer networks. Therefore, we do not plan to cover wireless data networks, like CDPD, HSCSD, PDC-P, etc, which run over wireless voice networks or mobile telephones. Wireless data networks can be categorized broadly into four different categories based on their intended use.

1. *Wide area networks* (WANs) are created and maintained by cellular carriers. In fact, older WANs can be viewed connectionless extensions to circuit switched networks, created in order to facilitate communication between persons and groups belonging to geographically dispersed locations such as between cities and countries. However, most modern WANs are based on packet switched networks such as UMTs.
2. *Metropolitan area networks* (MANs) are created and maintained as a backbone network technology for interconnecting a number of local area networks or LANs. 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 concerning professional interactions between persons and groups working for an institution or an organization.

4. *Personal area networks* (PANs) are created by individuals, usually self-maintained, and for person centric communication with interfaces to local neighborhood and the rest of the world.

Both WLAN and PAN are based on short range radio transmissions. However, the two have distinct application domains. Over the years, many interesting applications have been developed for PAN independent of WLANs. PAN applications typically require low volume transmission compared to WLAN. PANs are based on short range radio transmission technologies such as Bluetooth or ZigBee which appear to be ideally suited for small space privacy preserving person centric data services.

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

We plan to study PAN and WAN separately in this text while limiting our current focus to the principles and the theories on which wireless LANs function. In order to organize this chapter as a precursor to subsequent discussion on wireless networks, we also take closer look at how mobility affects the data rates and details of standards developed for different wireless networks.

5.2 Mobility Support and Wireless Networks

We begin with a brief introduction on the relationship of achievable data rates with mobility support. Figure 5.1 illustrates the relationship. WLAN supports only slow mobility while WAN (GSM/wideband cellular) supports

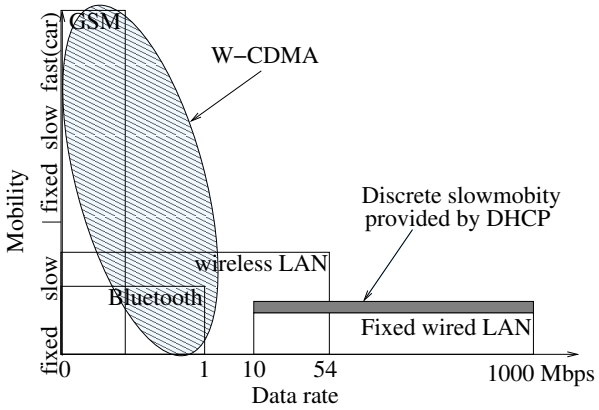


Figure 5.1: Mobility supports on LAN and WAN

range of mobilities starting from discrete and slow to continuous fast (vehicular). PAN implemented over Bluetooth, for example, 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 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 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 is 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 (Worldwide Interoperability for

Microwave Access) as it works on Microwave band. There are two variants of WiMAX; one operating in unlicensed frequency band 2-11GHz while the other operates on licensed band 10-66GHz. WMAN offers a range upto 50Km and data rate up to 80Mbps.

Wireless LAN is supported usually by wired infrastructure and provide one-hop wireless connectivities to clients within a small distance. The typical coverage area could be a university, small enterprise, hospital, airport, etc. Considering the requirements of clients, wireless LAN should support high data transfer rates as opposed to WANs. WLANs operate on unregulated part of the wireless communication spectrum. Its range may spill over to 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. 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., can be connected to 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 dependent 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.

In summary, the usage of different wireless communication technologies characterized by speed, range and applications as follows:

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

5.3 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 meters or so 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 to 54 Mbps. The latest WLAN standard IEEE 802.11n could offer speed up to 300 Mbps. As opposed to WLANs, Wired LANs can support data rates between 100 to 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.

5.3.1 IEEE Standards

WLANs mostly use wireless Ethernet technology based on IEEE 802.11 standards [5]. 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, known popularly as WiFi, was released. It uses 2.4 GHz unlicensed spectrum, and supports the transfer rates in the range of 5 to 11 Mbps. IEEE 802.11a was also released around the same time. The industry name for the implementation of 802.11a is WiFi5 because it uses regulated 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 Figure 5.2. Since each channel width is 22 MHz, and the center frequency of channel 1 is 2.412 GHz, the upper frequency of channel 1 must be 2.423 GHz. This means

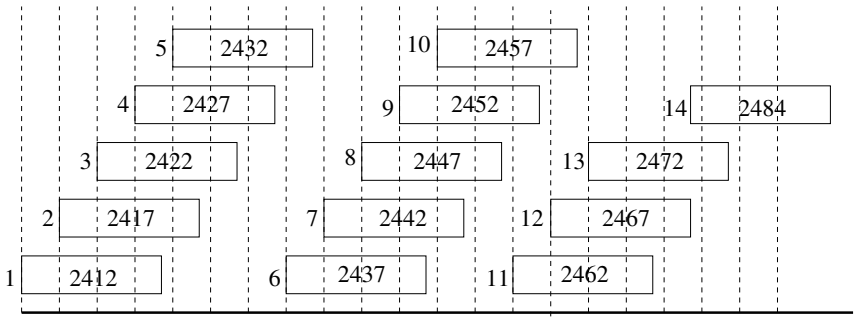


Figure 5.2: Channelization of 2.4 GHZ band for WLAN.

any channel whose lower frequency is highter than 2.423 GHz would be non-overlapping with channel 1. The lower frequency of channel 6 is 2.426 GHz. So, channels 1 and 6 are non-overlapping. The upper frequency of channel 6 is 2.448 GHz. Channel 11 have lower frequency 2.451 which is greater than 2.448. So channel 11 is non-overlapping with 6. Therefore, in 802.11b we have just three non-overlapping channels, namely 1, 6 and 11. 802.11b uses transmit spectrum mask to limit power leakage to adjacent channels. It causes the energy outside ± 11 MHz around the center frequency f_c to drop down by 30 dB with relative to the peak energy at f_c. Similarly, the signal must attenuate by at least 50 dB outside ± 22 MHz around f_c with relative to peak energy at f_c. This may still cause interference in adjacent channelr.

IEEE 802.11a is particularly well suited for multiple users running applications that require high data rates. It supports a maximum raw 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 every 20 MHz channel spans over 4 channel numbers. The lower and middle subbands have total of 8 carriers of width 40 MHz at 20 MHz spacing. The upper subband has 4 carriers also at 20 MHz spacing. The outermost channels in lower and middle subands are at 30 MHz spacing from band edges. Figure 5.3 illustrates the the channelization scheme. However, outermost channels in upper subband are at 20 MHz spacing from band edges. Channelization for upper subband is illsutrated by Figure 5.4. A spectral mask is used in 802.11a to limit power leakage into adjacent channels. The power output drops down sharply after a spacing of 9 MHz on both sides of central frequency. After 11 MHz spacing from the central frequency, the power output goes down steadily and

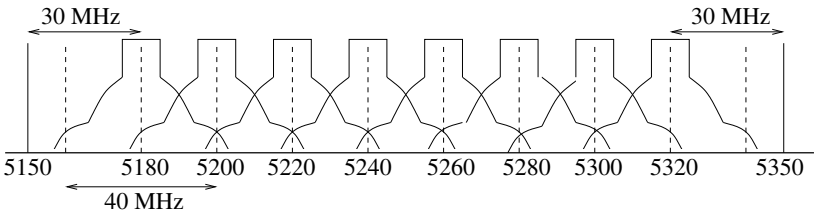


Figure 5.3: Lower and middle subband channelization scheme for 802.11a

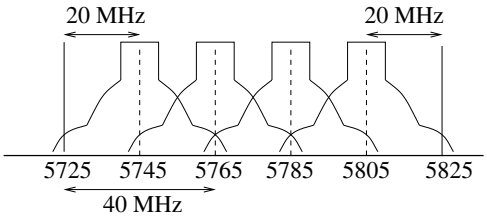


Figure 5.4: Upper subband channelization scheme for 802.11a

becomes as low as -40dB at ±30 MHz from the central frequency as shown in Figure 5.5. In Europe lower and middle segments are free, so only a total of 8 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

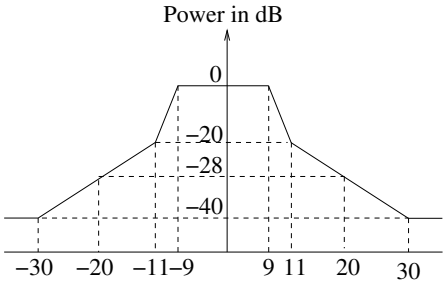


Figure 5.5: Transmit spectrum mask

the other due to the property of orthogonality. However, 802.11a was not as popular as 802.11b. Due to higher frequency, the range of 802.11a networks is shorter compared to that of 802.11b. It covers just about one fourth of the area covered by 802.11b. Furthermore, 802.11a signals can not penetrate walls and other obstructions due to shorter range. The use of 802.11a, thus, never really caught on.

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 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 4 (10-13) and Spain allows only 2 (10-11) channels for WLAN. The channels are overlapping. For avoiding adjacent channels rejection at 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 demands, there should be 5 channels in-between to avoid interference caused by the neighboring access points. So, out of 14 at most three are non-overlapping channels. This implies that at most three access points can be placed adjacent to one another.

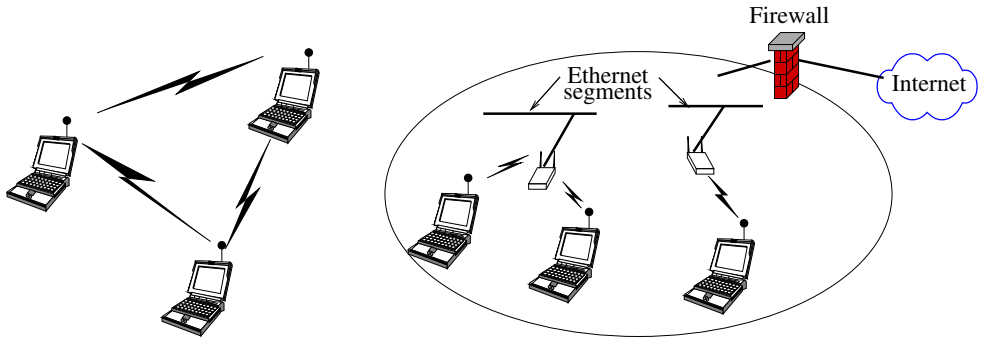
IEEE 802.11n is a relatively new standard (finalized in 2009). It could achieve higher transfer rate by relying on multiple input and mupltiple output (MIMO) antennas. It operates on both 2.4GHz and 5GHz bands. IEEE 802.11n allows up to 4 transmit and 4 receive antennas. The allowable number of simultaneous data streams is restriced by minimum number of antennas used on both end of a connection. The notation $n_1 \times n_2 : n_3$, where $n_3 \leq \max\{n_1, n_2\}$, a MIMO antenna's capabilities. The first number n_1 gives the maximum number of transmit antennas, the second number n_2 specifies the maximum number of receive antennas that can be used by the radio. The third number 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 $2\times2 : 2$ radio a device have 2 receive and 2 transmit antenna, however, only 2 simultaneous data streams can be supported.

5.4 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 to this access point together define a Basic Service Set (BSS). Note that BSS is different from coverage area of an access point which is referred to as Basic Service Area (BSA). A Basic Service Set IDentifier (BSSID) uniquely identifies each BSS. So, 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. So, a user friendly name known as Service Set IDentifier (SSID) is used to identify a BSS. SSID is referred to as a name of a WLAN or the network. Typically, a client can receives SSID of a WLAN from its access point. However, for security reason, some wireless access point may disable automatic SSID broadcast. In that case client has to set 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 IBSS every station should be 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 5.6 depicts the two basic topologies described above. Independent network services are available to stations for communication within a small geographical coverage area called 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 this chapter. 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 sender to its AP, and the other from the AP of the receiver to itself when both sender and receiver wireless enabled. Both receiver and sender could be linked to same AP or two different APs. APs essentially act as relay points and vital to WLAN architecture. The placement of APs should be planned in advance to provide coverage to wireless stations. The planning should consider issues such as maximizing coverage, minimizing interferences, restricting blind spots (no wireless coverage), minimizing unwanted signal spillovers, and maximizing opportunities for implementing the Extend Service Set (ESS) for mobile



(a) Independent network topology.

(b) Infrastructured network topology.

Figure 5.6: WLAN basic topologies

nodes to be able to connect to the Internet.

5.5 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, can not fully utilize the bandwidth. Secondly, the noise due to external interference and electronic circuits reduce the signal to noise ratio at receiver. Thus, receiver can not receive the transmission properly. If 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 [**?**] tells us that any conducting material can function as an antenna on any frequency. Furthermore, the height antenna would 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 reduce the length of 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 communication.

5.5.1 Modulation

Modulation is defined as a process by which information signal is superimposed on a carrier. It essentially modifies certain parameters of the carrier in proportion to signal or message.

IEEE 802.11g standard, supports the raw data rates of 54 Mbps (same as 802.11a) but operates in 2.4 MHz band. It is, therefore, backward compatible with 802.11b equipments. But like 802.11a, it uses Orthogonal Frequency Division Multiplexing (OFDM). Therefore, it offers enhanced data rate in 2.4 GHz band. It could offer some resistance to radio frequency interference and multipath distortion. However, it suffers from interference from other devices operating in 2.4 MHz frequency. 802.11g standard also includes the use of Packet Binary Convolution Code (PBCC), and a hybrid of Complementary Code Keying (CCK) and OFDM for optional modulation techniques.

5.5.2 Physical Layer Standards

IEEE standards focus on bottom two layers, physical (PHY) and medium access control (MAC) of the OSI model [12]. The Logical Link Layer specification is available in IEEE 802.2 standard. The architecture is designed to provide a transparent interface to higher level layers for the clients. The client terminals may roam about in WLAN yet appear stationary to 802.2 LLC sub-layer and above. So existing TCP/IP is remains unaffected and need not be retooled for wireless networks. Figure 5.7 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 (FH or FHSS) and Direct Sequence Spread Spectrum (DS or DSSS) are meant for radio based connectivity. Both IR and FHSS operate in 2.4 GHz band, while DSSS operates in 5 GHz band.

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

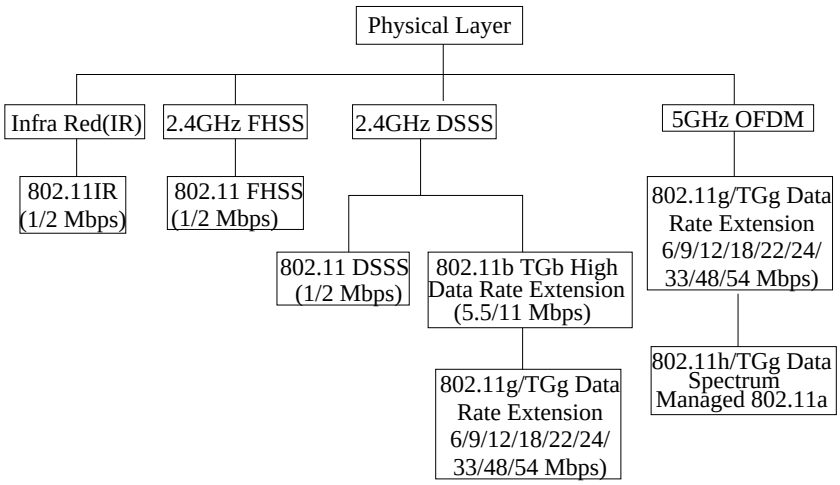


Figure 5.7: IEEE standard architecture for PHY and MAC layers.

off the walls, and consequently changing the location of the receiver will not disrupt the signal.

5.5.3 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 modulated using spreading code or spreading sequence. The

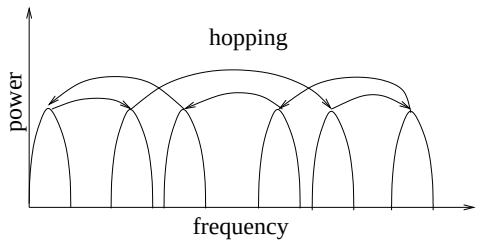


Figure 5.8: Frequency hopping spread spectrum.

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.

Figure 5.8 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 GHz to 2.480 GHz. It allocates a different frequency hopping patterns for every data exchange. The signal dwell time can not exceed 400 ms in a particular frequency. A maximum length packet takes about 30 ms. Thus a small amount of data is sent before 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 for 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).

Assuming a bit period T_b, and hop period T_h, for SFH $T_b = T_h/k$, for $k = 1, 2, 3, \ldots$. It implies that the hop rate $R_h = 1/T_h$ is less than the base band message rate $R_b = 1/T_b$. Equivalently, in SFH, the transmitter uses a frequency for several bit periods. As shown in figure 5.9, 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, $T_d \geq T_b$.

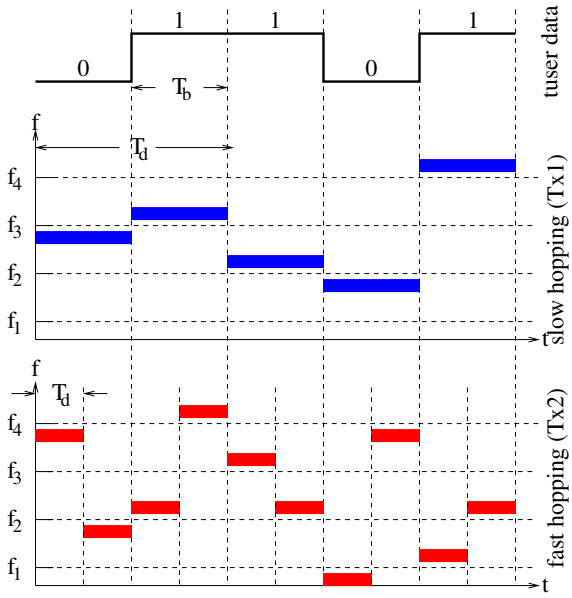


Figure 5.9: Frequency hopping spread spectrum.

Figure 5.9 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 $T_b = (1/k)T_h$, 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 [11]

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

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 required to be paid if C (performance) is to sought be increased. Another way to look at the equation is that even in difficult environmental

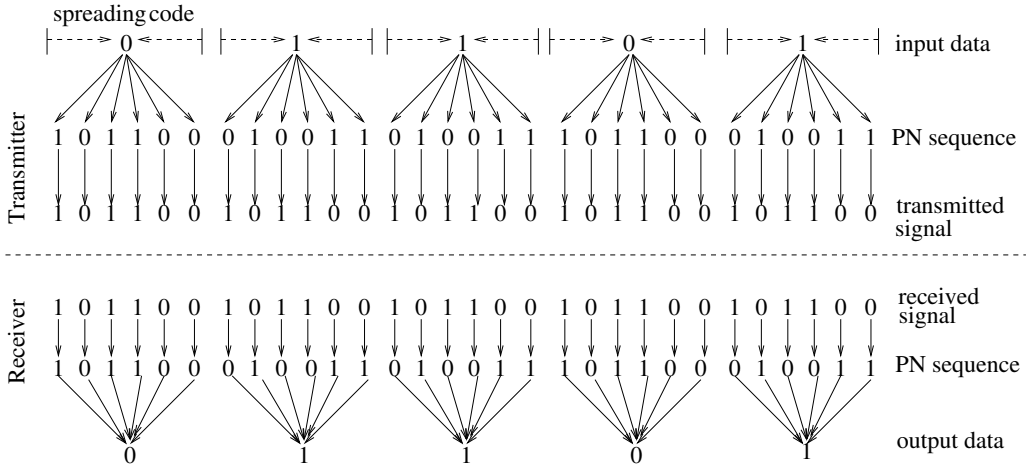


Figure 5.10: DSSS using with spreading factor 6.

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 $S/N \ll 1$,

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

The above simplified equation implies that for a given noise to signal ratio, error free transmission can be ensured by performing spreading which is equivalent to increasing bandwidth. So 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, in figure 5.10 depicts 1 data bit is represented by 6 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 represent 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 to 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 are short, have good balance (difference between 1s and 0s is small), 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 [7]. Also from Shanon-Hartley's equation, 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 figure 5.10. 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 actual 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 of the same bandwidth as the original spreaded signal. Some additional filters may be used to generate this signal. The receiver then has to use the same chipping sequence as was employed at the transmitter's end to recover spreaded data by one XOR operation. The receiver has to be precisely synchronized 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 signal, and the adding of the products in an integrator is known as *correlation* and the device executing the process known as *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.

The output at the receiver end to be identical to actual data, 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 data for actual data 011 is

[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.

spreaded data:	[10110111000	**01001000111**	**01001000111**]
chip sequence:	[10110111000	**10110111000**	**10110111000**]
XOR:	[00000000000	**11111111111**	**11111111111**]
sums over $T_b, 2T_b, 3T_b$:	$(0)_{10}$	$(11)_{10}$	$(11)_{10}$

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 have been indicated 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. For example, suppose we use 11 bit Barkar code as previously 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.

spreaded data:	[10110111000	**01001000111**	**01001000111**]
received:	[00100001000	**11110111111**	**11011110111**]
sums over $T_b, 2T_b, 3T_b$:	$(2)_{10}$	$(9)_{10}$	$(11)_{10}$

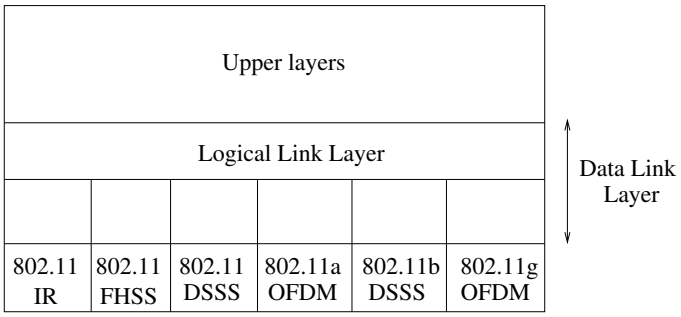


Figure 5.11: Protocol stack for 802.11

Then threshold comparator could 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., $G = B/R$. Consequently, the signal to noise ratios for input and output are related by the processing gain as follows.

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

Note that the information rate R is the inverse of bit stream interval T_b. Similarly, the bandwith 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.

5.5.4 Protocol Stack

We now have a fairly good idea about the physical layer of 802.11 networking protocol suite. As discussed in previous section, the physical layer corresponds more or less to the OSI physical layer. Physical layer have a variety of implementation options, namely, Infrared, 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 Figure 5.11.

5.6 MAC Layer

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 are allowed to send at the same time using the full bandwidth by use of orthogonal code sequences. Orthogonal codes ensures that concurrent communication can be separated at the receiving end 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.

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: by assigning time slots for transmission in time domain.
4. CSMA: by assigning transmission opportunities on statistical basis on time domain.

In FDMA, a frequency is allocated to a transmission on demand. It will remain engaged until 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

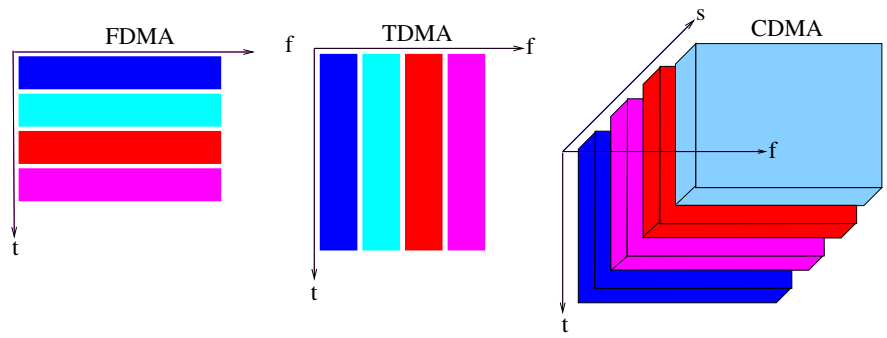


Figure 5.12: Contrasting different access technologies

bandwidth is 30KHz with guard band of 30KHz. 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.

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 mix of different transmissions by different senders in the same time span. Figure 5.12 shows hows multiple transmissions are carried out using different access technologies.

CSMA/CD (carrier sense multiple access/collision detection), a MAC method used in a wired LAN, is a clever sharing in time domain where channel access by a device gets suspended on detection of an ongoing transmission. The access is granted on the basis of a statistical fairness. A wired LAN can detect collision whereas a wireless LAN can not. Wireless LAN uses backoff to avoid collision. Collision is never noticed by contending stations, it

is implied by receipt of an erroneous frame or non-receipt of an acknowledgement. Therefore, the protocol is known as CSMA/CA, CSMA with Collision Avoidance.

5.7 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 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 which solve multiple of access issues 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 protocol operate by prevent any occurrence of a collision.

5.7.1 ALOHA

ALOHA is a simple minded contention type MAC protcol 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 resend. 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 a few stations is depicted in Figure 5.13. The question one would ask is why this simple scheme would work at all? This can be answered best by analyzing its

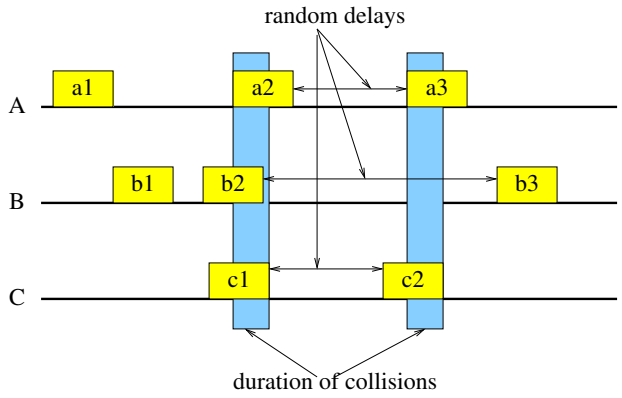


Figure 5.13: Frames generation and transmission under pure ALOHA.

performance. The initial ALOHA scheme was for transmitting data from a number of earth stations to a satellite. So there is one receiver and a number of senders. Each sender sends new frame as well retransmits the frames which were damaged due to collisions. Suppose there is an infinite population of transmitters, and new frames are generated by this population according to Poisson distribution with a mean N per frame time. If $N > 1$, then the system is generating frame at a rate greater than what the system can handle. So, $0 < N < 1$ must hold. Apart from new frames, the retransmission of damaged frames also should be taken into account. So, there may be attempts to transmit several frames per frame time taking into account both new and old (due to retransmissions) frames. Let the probability of k frames being transmitted in a frame time be also distributed according to Poisson with a mean of G frames per frame time t. Clearly, $N \leq G$. At low traffic conditions, N is close to 0, there will be few collisions, so G is very close to N. But if there are many collisions (with high traffic load), $G > N$. If P_0 be the probability of a transmission becomes successful. Then throughput under all traffic conditions will be $S = GP_0$.

Now let us analyze how collisions will affect the transmissions. Suppose a frame is being transmitted. Since, a ALOHA station does not listen to the channel before commencing a frame transmission, a frame will not suffer from a collision provided no other frame is transmitted during the frame time from the starting time of the first frame. Let the time be divided into slots of frame time t. So, frame started at time $t_0 + t$ will suffer from collision if any

other user has generate a frame in time intervals (t_0, t_0+t) and (t_0+t, t_0+2t). So the period of vulnerability of a frame in transmission is $2t$.

According to Possion distribution, the probability of generating k frames in a frame time t is: $\frac{G^k e^{-G}}{k!}$. The average number of frames generated in two consecution frame time is $2G$. Therefore, the probability that k transmission attempts are made during the two consecutive frame time is $\frac{(2G)^k e^{-2G}}{k!}$. Notice that a frame will not suffer a collision if no transmission attempt is made for two consecutive frame time. The probability that no frame transmission attempt will be made in the time interval $2t$ is $P_0 = e^{-2G}$. This implies that probability of a frame not suffering a collision or its transmission becomes successful is $S = G.P_0 = Ge^{-2G}$. The maximum value of S occurs at $G = 1/2$, i.e., $S_{max} = 1/2e = 0.184$. So, though performance is bad ALOHA does work.

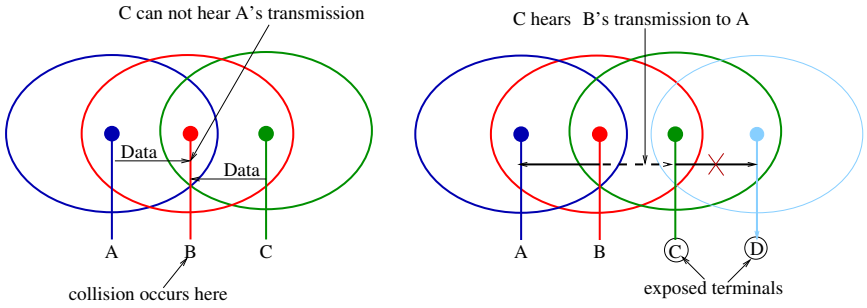
A variation of pure ALOHA is slotted ALOHA which double the capacity. In this protocol, time is divided into slots of size equal to frame time. A station has to agree to align transmission with a slot boundary. So, whenever a station has a packet to send it wait till the beginning of next slot boundary. So the collision can occur only during the interval of a slot. It leads to cutting down the period of vulnerability to half of that of pure ALOHA. So, the probability that no other frame is generated during a frame time $P_0 = e^{-G}$. Therefore, the probability that a frame will not suffer a collision during its transmission is $S = GP_0 = Ge^{-G}$. This implies that the maximum throughput achieveable through slotted ALOHA is $1/e$ twice of that of pure ALOHA.

5.7.2 IEEE standards

IEEE standard specifies two ways to resolve contention in medium access when multiple nodes attempt to transmit simultaneously:

1. Distributed Coordination Function (DCF) is a mechanism for resolving contention without the need for a central arbiter when access attempts were made independently by a multiple number of stations to gain access of medium. The protocol resolves contention by employing virtual carrier sensing. If the carrier is busy the station trying to gain access backs off.

2. Point Coordination Function (PCF) is restricted resolution of contention within infrastructure BSS. It does so with help of a coordinator residing in access point itself.



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

Figure 5.14: Hidden and exposed terminal problems.

Two transmission modes are also supported, viz., asynchronous and synchronous. 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 can not operate 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 Figure 5.14(a), 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. Therefore, the crux of the problem is that the absence carrier does not necessarily mean idle medium.

The exposed terminal case, as indicated by Figure 5.14(b), 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.

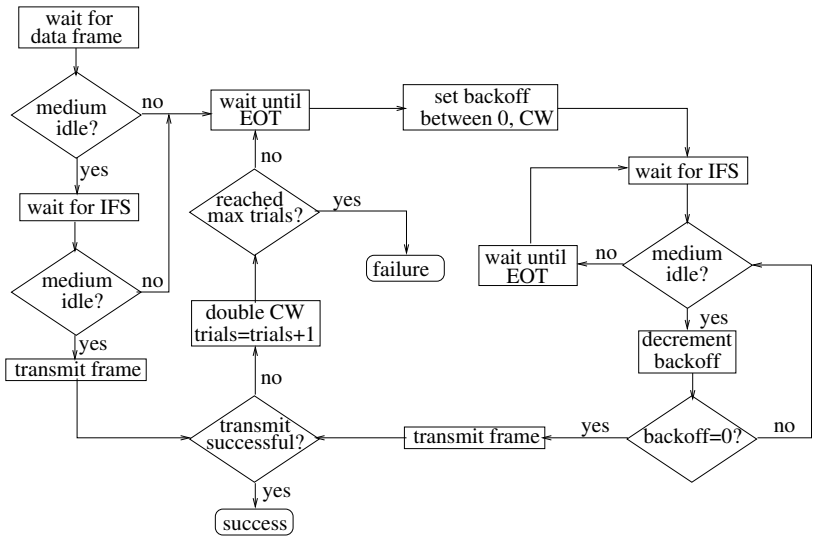


Figure 5.15: DCF basic mode when collisions do not occur.

DCF solves the hidden and the exposed terminals problems by getting rid of carrier sensing. The protocol CSMA/CD is modified as CSMA/CA. That is, it uses the mechanism of collision avoidance (CA) instead of using collision detection (CD). In CDMA/CA, transmitting station first checks to ensure that channel is free. If the channel is indeed free, then the station waits for a chosen period of time, and checks once again to see if the channel is clear. The waiting time between the two checkings is known as backoff time. When the backoff timer becomes zero, and the channel is clear the station begins transmission. The backoff timer is reset once it reaches zero.

5.7.3 Distributed coordination function

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. Figure 5.15 depicts the transmission process in basic DCF mode. 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, generation of a random backoff is enforced after the transmission of the first packet.

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 not only helps to avoid collision among contending stations but also ensures that no waiting station will be blocked from gaining access of medium indefinitely. Furthermore, the stations waiting for a longer time also gain priority over other waiting stations. An unlikely event of occurrence of collisions happens due to the case when backoff timers of two or more contending stations simultaneously reach countdown of 0. In this case, each sending station once again chooses a random backoff value to avoid repeated collision. The random backoff value 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 20μs. The contention window is set dynamically, when a station successfully complete 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 ACK. ACK has a higher priority because if a station is made aware of successful transfer, it won't retransmit the data. It would help 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 10μs, whereas DIFS $= 2 \times slotTime$ + SIFS $= 50\mu$s. In DCF basic access mode ACK transmission occurs as shown in Figure 5.16.

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

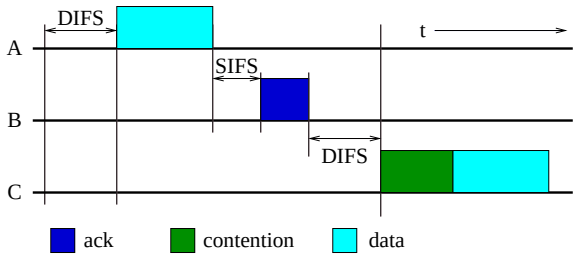


Figure 5.16: ACKs for DCF unicast data transmission.

1. for sending CTS (clear to send),

2. for sending actual data, and

3. for 3 SIFS intervals.

Note that CTS is sent by the receiver to the sender signaling the latter to access the medium. CTS is considered as a short high priority message much like ACK. So, before gaining access of 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 senser 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 of medium would know the duration for which 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 Figure 5.17. As indicated in the figure, once A has been cleared by B for sending, C has to wait till DIFS + NAV(RTS) + *contention interval* before it can try to gain access of the medium.

DCF with RTS/CTS mode solve both hidden and exposed terminal problems. The solution to hidden and exposed terminal problem is illustrated by figure 5.18. In hidden terminal problem, station C hears the CTS sent by B on RTS request from A. So, C becomes aware of medium access by A and differs the attempt to access medium by retrieving the NAV from CTS. The possibility of collision becomes restricted to RTS because C not being in the range of A may not be able to hear RTS as shown in figure 5.19. Exponential backoff is applied when RTS collisions occur.

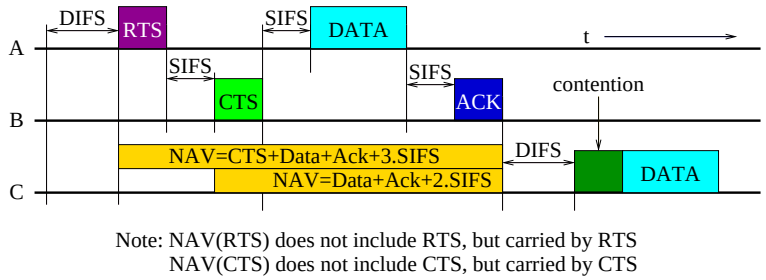
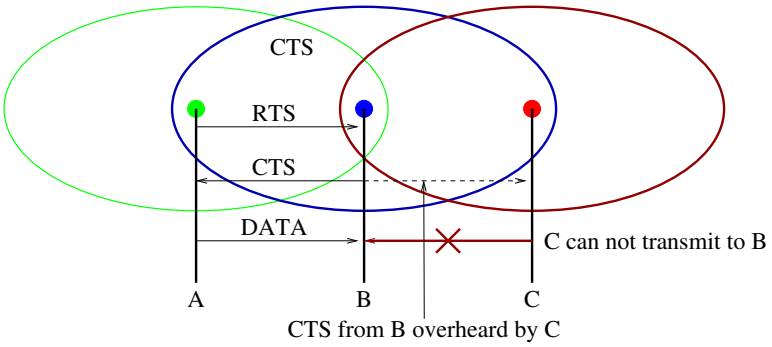
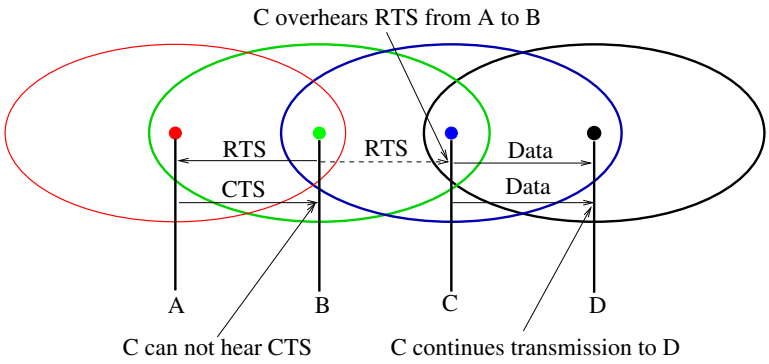


Figure 5.17: DCF RTS/CTS mode of transmission.



(a) Hidden terminal.



(b) Exposed terminal.

Figure 5.18: Solutions to hidden/exposed terminal problem.

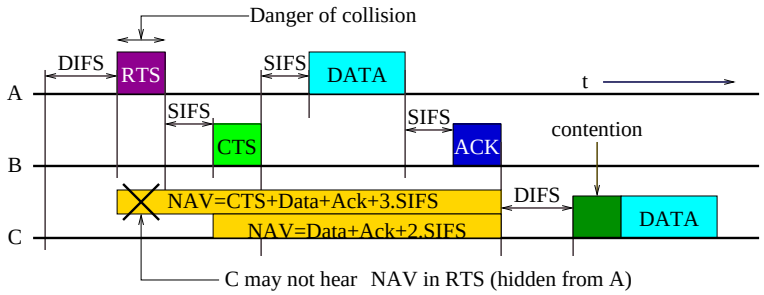


Figure 5.19: Collision problem in RTS transmission.

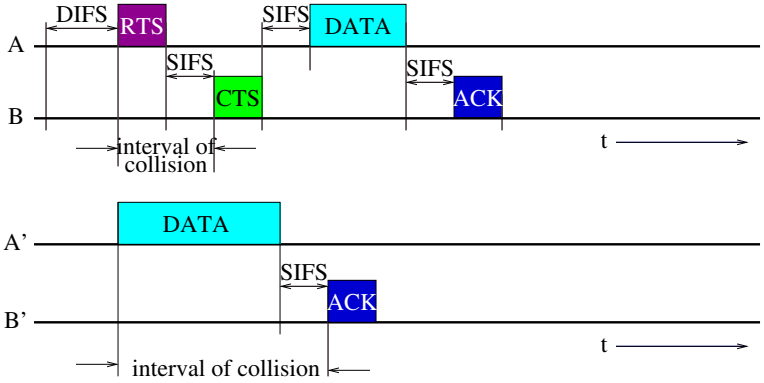


Figure 5.20: Reducing collision interval by RTS.

As shown in figure 5.18(b), station B sends RTS to A which is overheard by C. However, C cannot overhear the CTS sent by A to B as it is not in the wireless range of station A. Therefore, C would conclude that the medium is free and could continue transmission to D. Clearly, the use of RTS/CTS restricts the duration of collision. As shown in figure 5.20, if the interval of collision is determined by data, then the interval of collision will be for the duration of data transmission plus the SIFS interval. On the other hand, if RTS/CTS mode of DCF is used, then the interval of collision would be determined by the length of RTS plus the SIFS interval.

There may a smart station which uses a number of tricks to increase its chance of medium access and 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 [6, 13]:

- 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 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 larger than required.

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 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 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. Receiver side solution looks better. The access point can monitor each sender's behavior. The receiver side solution could as follows.

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

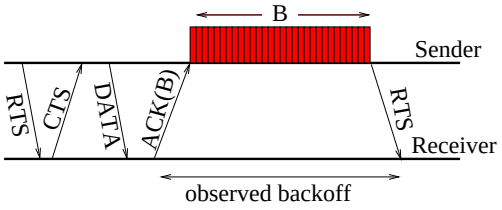


Figure 5.21: Receiver side solution to check LAN misbehavior.

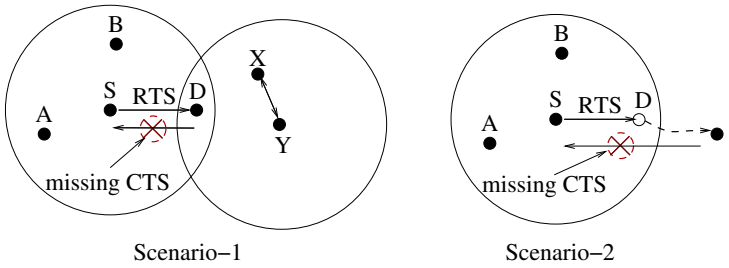


Figure 5.22: Effects of missing CTS

The receiver side monitoring process is explained in figure 5.21.

The use of 4-way handshaking through RTS-CTS handshake was proposed mainly for solving hidden and exposed terminal problem through virtual carrier sensing mechanism. It also improved throughput by reducing the probability of packet collision by limiting the period of collision to a short interval bounded by RTS+SIFS interval. However, the stations involved in RTS collision fail to get CTS, and prevented from sending data. However, the network incurs 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 figure 5.22. In the first case, there is an ongoing communication between stations X and Y. So, station D concludes that carrier is busy and would not send CTS to S's RTS. However, 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. 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.

5.7.4 Point coordination function

The Access Point (AP) works as coordinator for PCF. The time is divided into superframes each consisting of a contention period (CP) and a contention free period (CFP). The maximum duration of CFP 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 CP and PCF is used during CFP. PCF polls individual nodes in its polling list, which is arranged according to 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 frames which is shorter than DCF InterFrame Spacing (DIFS). To prevent starvation of stations not allowed to send during CFP there should be space for at least one maximum length frame to be sent during CFP.

The access point which acts as coordinator, polls the stations in round robin fashion. The polled station must always respond. If there is no data to be sent then a polled station must respond with null frame with no payload. If all stations can not be polled during a CFP, then 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 5.23 below provides the structure of the superframe. At the beginning of every contention free period, AP sends beacon frame to all station in basic service area (BSA) after it finds the medium to be be idle for PIFS interval. PIFS is shorter than DIFS but longer than SIFS. The beacon frame contains CFP_{max}, beacon interval, and BSS identifier. All stations in BSS set their network allocation vector (NAV) accordingly for not sending a packet

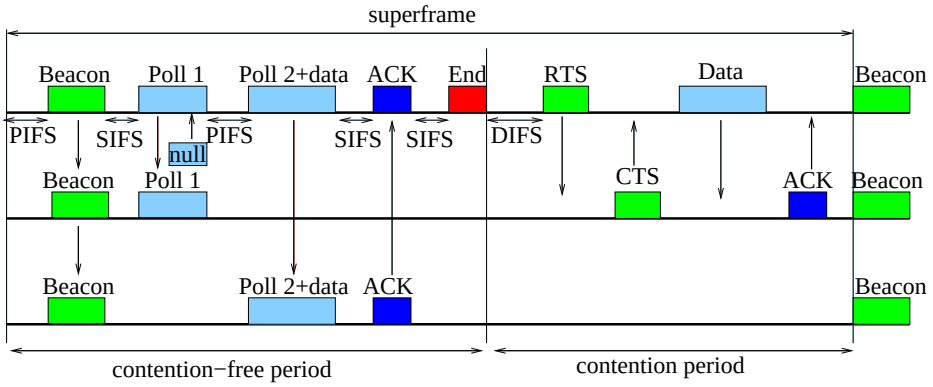


Figure 5.23: Superframe structure and PCF.

in CFP after receiving a beacon.

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 receiving station responds AP with Data or null frame as explained above. AP continue the polling of each station until it reaches CFP_{max} time. Whe time bound is reached AP terminates contention free period by sending a CF-end frame.

Standard	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Bandwidth/ Channel width in 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	1m
Protocol stack size	4-32kB	$>$ 250kB	$\approx$425kB
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

5.7.5 Review questions

1. In DSSS, what does spreading factor represent?
2. What is the advantage of using orthogonal chipping sequence in DSSS?
3. What are the basic differences between FHSS and DSSS?
4. How FDMA, CDMA, TDMA and CSMA differ each other?
5. How the radio technologies FDMA and TDMA can be combined?
6. What are two basic network topologies supported by IEEE 802.11?
7. Explain how the use of NAV in DCF helps in controlling multiple accesses?

5.7.6 Exercises

1. Suppose a chipping sequence 10111001 is used to represent 0 bit in DSSS, find the spreaded data if the actual data is 0101.
2. Derive a closed form expression for bandwidth in terms of channel capacity and signal to noise ratio (SNR), assuming SNR to be less than 0.1. Calculate bandwidth requirement for a DSSS transmission system which operates an RF link with data information rate being 30 Kbps and S/N ratio is 0.05.
3. Let the available channel bandwidth on a telephone link be 4kHz, and average signal to noise ration on the channel be 40dB. What is the maximum error free data rate that can be supported on this channel?
4. The signal loss over a communication link is such that the maximum E_b achievable at the required range is only -0.5dB. Determine the maximum bandwidth efficiency for this link at the extreme of range, and the information throughput that can be delivered in a bandwidth of 3kHz?
5. Suppose 1000 frames transmitted using pure ALOHA protocol through a shared 2Mbps satellite link. Each frame is of 1K bits and all stations taken together produce 500 frames per second. Find the number of frames that are transmitted without collision?

6. Solve the previous problem by replacing pure ALOHA with slotted ALOHA.

7. Explain the differences between CSMA/CD and CSMA/CA protocols.

8. Suppose DCF operating in RTS-CTS mode eventually allows station A to transmits data to station B. Stations D is able to set its NAV from RTS, while C is able to set its NAV by hearing CTS from B. Then which station between C and D is closer to A? Explain why? Also show likely locations of the stations, assuming D can also communicate with C.

9. Why the update of backoff timer is delayed until the DIFS contention period? Explain how the use of backoff timer allows a station to raise its priority when many contending stations try to access the channel.

10. Assume that one mobile station (MS) has opened a UDP connection with an access point (AP). The UDP data packets has following parameters:

    i. SIFS duration: 10μs,

    ii. DIFS duration: 50μs;

    i. 802.11 preamble: 264 bytes

    ii. UDP header: 8 bytes.

    iii. MAC header: 36 bytes.

    iv. UDP payload: 1192 bytes.

    Find the maximum throughput for the above transmission assuming link capacity to be 20 Mbps.

11. Find the maximum throughput when UDP connection is replaced by a TCP connection under the previous problem settings. The parameters specific to TCP transmission are:

    i. 802.11 ACK frame: 14 bytes.

    ii. TCP header: 40 bytes.

    iii. TCP payload: 1160 bytes

    iv. TCP ACK packet payload: 40 bytes.

12. Suppose a mobile station (MS) is sending data to the access point (AP) at a rate of 1 Mbps. The MS operates under saturation conditions, i.e., it always has data ready to send once the previous transmission is complete. Assume also that no other stations contend for channel access, and that transmissions are ideal (i.e. no data frame is lost due to channel errors). The parameters concerning this transmission are:

    i. The PHY preamble duration: 144μs,
    ii. SIFS duration is 10μs,
    iii. DIFS duration is 50μs;
    iv. RTS packet: 20 bytes,
    v. CTS packet: 14 bytes,
    vi. ACK packet: 14 bytes;
    vii MAC packet header: 34 bytes,
    viii The maximum (payload) frame size: 2312 bytes.

    Also assume that the initial backoff is uniformly distributed between 20μs and 620μs. Determine the actual average throughput (considering the overheads due to both to the PHY and the MAC layer) under the above-mentioned conditions, in the case where the data to send is mapped into a single packet of the maximum payload size.

13. It is possible for a pair of smart mobile stations (MSs) to cheat in order get a higher share of uplink traffic to an Access Point. Apart from the ways of cheating discussed in the text, MSs may adopt following techniques:

    i. The destination scramble CTS and ACK packets and the source scrambles data packets. So, it is not possible to figure out whether data sent has been received. Then taking advantage of this source can fake retransmissions to send further data, and at the end sends unscrambled packets.
    ii. By mutual collusion source and destination may send oversized NAV, and prevent other contending stations from attempting transmission.

    Find solutions for detection of such cheatings.

Bibliography

[1] Abramson, N. The ALOHA system - another alternative for computer communications. In *Fall Joint Computer Conference* (1970), AFIP Press, p. 281=285.

[2] Barker, R. H. Group synchronizing of binary digital sequences. *Communication Theory* (1953), 273–287.

[3] Binder, R., Abramson, N., Kuo, F., Okinaka, A., and Wax, D. ALOHA packet broadcasting - a retrospect. In *1975 National Computer Conference* (1975), AFIPS Press, pp. 203–215.

[4] Deering, S. ICMP router discovery messages. `http://www.ietf.org/rfc/rfc1256.txt`, 1991.

[5] Gast, M. S. *802.11 Wireless Networks*. O'Reilly & Associates Inc., Gravenstein Highway North, Sebastopol, California, 2002.

[6] Kyasanur, P., and Vaidya, N. H. Selfish MAC layer misbehavior in wireless networks. *IEEE Transaction on Mobile Computing 4*, 5 (2005), 502–518.

[7] Mitra, A. On pseudo-random and orthogonal binary spreading sequences. *International Journal of Information and Communication Engineering 4*, 6 (2008), 447–454.

[8] Perkins, C. IP encapsulation within IP. `http://tools.ietf.org/html/rfc2003`, 1996.

[9] Perkins, C. Minimal encapsulation within IP. `http://tools.ietf.org/html/rfc2004`, 1996.

[10] Perkins, C. *Mobile IP: Design, Principles and Practice.* Addison-Wesley Longman, Reading, Massachusetts, 1998.

[11] Shannon, C. E. Mathematical theory of communication. *Bell System Technical Journal 27* (July and October 1948), 379–423, 623–656.

[12] Tanenbaum, A. S. *Computer Networks.* Prentice Hall, 2003.

[13] Xu, M., Zhan, Y., Cao, J., and Liu, Y., Eds. *Selfish MAC Layer Misbehavior Detection Model for the IEEE 802.11-Based Wireless Mesh Networks* (2007), vol. 4847 of *Lecture Notes in Computer Science.*