Newnes

Third Edition

SHORT-RANGE WIRELESS COMMUNICATION

Alan Bensky

Short-range Wireless Communication

This page intentionally left blank

Short-range Wireless Communication

Alan Bensky

ELSEVIER

Newnes
An imprint of Elsevier

Newnes is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-815405-2

For information on all Newnes publications
visit our website at https://www.elsevier.com/books-and-journals

Publisher: Jonathan Simpson Acquisition
Acquisition Editor: Tim Pitts Editorial
Editorial Project Manager: Ana Claudia A. Garcia
Production Project Manager: Kamesh Ramajogi
Cover Designer: Mark Rogers

Typeset by SPi Global, India

This page intentionally left blank

CHAPTER

Wireless local area networks

11

An important factor in the widespread penetration of short-range devices into the office and the home is the basing of the most popular applications on industry standards. In this chapter and the next, we take a look at some of these standards and the applications that have emerged from them. Those covered pertain to Wi-Fi, Bluetooth, Zigbee and others based on IEEE 802.15.4. In order to be successful, a standard has to be built so that it can keep abreast of rapid technological advancements by accommodating modifications that don't obsolete earlier devices that were developed to the original version. A case in point is the competition between the WLAN (wireless local area network) standard that was developed by the HomeRF Working Group based on the SWAP (shared wireless access protocol) specification, and IEEE specification 802.11, commonly known as Wi-Fi. The former used frequency-hopping spread-spectrum exclusively, and although some increase of data rate was provided for beyond the original 1 and 2 Mbps, it couldn't keep up with Wi-Fi, which incorporated new bandwidth efficient modulation methods to increase data rates 50-fold while maintaining compatibility with first generation DSSS terminals.

Most of the pervasive WLANs are designed for operation on the 2.4 GHz ISM band, available for license-free operation in North America and Europe, as well as virtually all other regions in the world. However, The 5 GHz band has become a favorite for advanced systems because of its higher bandwidth and reduced interference from other unlicensed users. Most systems have provisions for handling errors due to interference, but when the density of deployment of one or more systems is high, throughput, voice intelligibility, or quality of service (QoS) in general is bound to suffer. We will look at some aspects of this problem and methods for solving it. This chapter will also describe multi-antenna systems—MIMO, communication security, and location awareness, as they apply to IEEE 802.11. Wi-Fi is the term adopted by the Wi-Fi Alliance association in year 2000 to identify its technical work and we use it herein synonymously with the generic IEEE 802.11 WLAN. From its self-identification, the Wi-Fi Alliance "defines innovative, standards-based Wi-Fi technologies and programs, certifies products that meet quality, performance, security, and capability standards, provides industry thought leadership, and advocates globally for fair spectrum rules"[1] By promoting compatibility of products from different manufacturers, the organization has contributed, together with IEEE, to making Wi-Fi/IEEE 802.11 the most widely deployed wireless communication system in the world.

Short-range Wireless Communication. https://doi.org/10.1016/B978-0-12-815405-2.00011-7

11.1 Introduction

One of the most prevalent deployments of short-range radio communication is WLANs. While the advantage of a wireless versus wired LAN is obvious, the early versions of WLAN had considerably inferior data rates making conversion to wireless not necessarily worthwhile, particularly when portability is not an issue. However, advanced modulation techniques have allowed wireless throughputs to approach and even exceed those of wired networks, and the popularity of highly portable laptop and handheld computers, along with the decrease in device prices, have made computer networking a common occurrence in multi-computer offices and homes.

There are still three prime disadvantages of wireless networks as compared to wired: range limitation, susceptibility to electromagnetic interference, and security. Direct links may be expected to perform at a top range of 50 to 100 m depending on frequency band and surroundings. Longer distances and obstacles will reduce data throughput. Greater distances between network participants are achieved by installing additional access points (APs) to bridge remote network nodes. Reception of radio signals may be interfered with by other services operating on the same frequency band and in the same vicinity.

Wireless transmissions are subject to eavesdropping, and a standardized security implementation in Wi-Fi called WEP (wired equivalent privacy) was found to be compromised with relative ease by persistent and knowledgeable hackers. More sophisticated encryption techniques have been instituted that greatly increase, but do not eliminate absolutely, the security risk of wireless communication although they may be accompanied by reduction of convenience in setting up connections and possibly in performance.

Various systems of implementation are used in wireless networks. They may be based on an industrial standard which facilitates compatibility between devices by different manufacturers, or a proprietary design. The latter would primarily be used in a special purpose network, such as in an industrial application where all devices are made by the same manufacturer and where performance may be improved without the limitations and compromises inherent in a widespread standard. In this chapter we deal with Wi-Fi, based on IEEE 802.11 with amendments and revisions.

As mentioned above, the Wi-Fi Alliance promotes Wi-Fi, and certifies devices to ensure their interoperability. The original link specification is continually updated by IEEE working groups to incorporate technical improvements and feature enhancements that are agreed upon by a wide representation of potential users and industry representatives. 802.11 is the predominant industrial standard for WLAN and products adhering to it are acceptable for marketing all over the world, albeit with features and characteristics conforming to the various regulatory organizations.

IEEE 802.11 covers the data link layer of lower-level software, the physical layer hardware definitions, and the data flow and management interfaces between them. The connection between application software and the wireless hardware is the MAC (medium access control). It is built so that the upper application software doesn't have to know what wireless technique is being used—the MAC interface firmware takes care of that. In fact, application software doesn't have to know that a wireless connection is being used at all and mixed wired and wireless links can coexist in the same network. The original basic specification defined three types of wireless communication techniques: DSSS (direct sequence spread spectrum), FHSS (frequency-hopping spread spectrum) and IR (infra-red). FHSS and IR early fell by the wayside, and DSSS has given way to OFDM, although specification amendments and revisions have maintained compatibility with earlier DSSS modes.

Wireless communication according to 802.11 is conducted on the 2.400 to 2.4835 GHz frequency band and on frequencies between 5 and 5.8 GHz that are authorized for unlicensed equipment operation in the United States and Canada and most European and other countries. A few countries allow unlicensed use in only in portions of these bands. Amendments to the original document add increased data rates and other features while retaining compatibility with equipment using the DSSS physical layer of the basic specification. Amendment 802.11a specified considerably higher rate operation in bands of frequencies between 5.2 and 5.8 GHz. The higher data rates were made available on the 2.4 GHz band by 802.11g that has backward compatibility with 802.11b.

Changes to 802.11 which reflect technological improvements and expansion of application areas are issued from time to time in the form of amendments to the current specification. Every four years or so amendments are consolidated into the current specification as a revision. The revision which serves as a reference for this edition of the book is IEEE 802.11-2016, which includes the basic performance amendments through 802.11ac [2].

11.2 Network architecture

Wi-Fi architecture is very flexible, allowing considerable mobility of stations and transparent integration with wired IEEE networks. The transparency comes about because upper application software layers (see below) are not dependent on the actual physical nature of the communication links between stations. Also, all IEEE LAN stations, wired or wireless, use the same 48-bit addressing scheme so an application only has to reference source and destination addresses and the underlying lower level protocols will do the rest.

Three Wi-Fi network configurations are shown in Figs. 11.1–11.3. Fig. 11.1 shows two unattached basic service sets (BSS), each with two stations (STA). The BSS is the basic building block of an 802.11 WLAN. A station can make ad hoc connections with other stations within its wireless communication range but not with those in another BSS that is outside of this range. In order to interconnect terminals that are not in direct range one with the other, the distributed system shown in Fig. 11.2 is needed. Here, terminals that are in range of a station designated as an AP can communicate with other terminals not in direct range but who are associated with the same or another AP. Two or more such APs communicate between

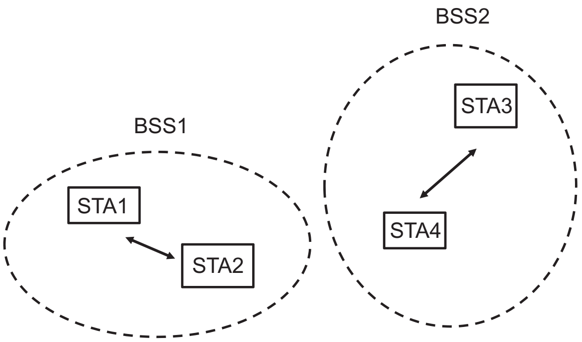


FIG. 11.1

Basic service set.

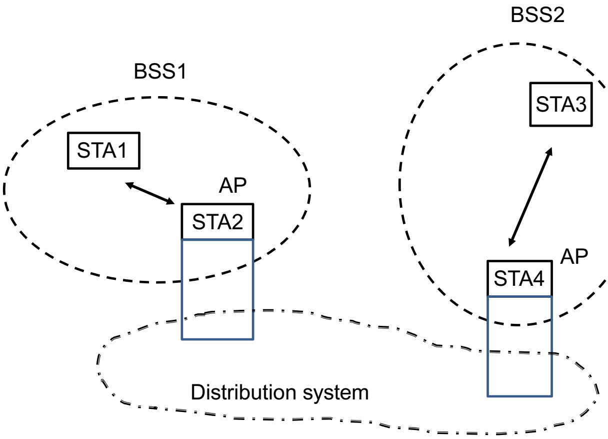


FIG. 11.2

Distribution system and access points.

themselves either by a wireless or wired medium, and therefore data exchange between all terminals in the network is supported. The important thing here is that the media connecting the STAs with the APs, and connecting the APs among themselves are totally independent. Note that the STA is an addressable destination, not necessarily at a fixed location. STA's may have varied characteristics and functions. A STA may be, for example, an AP terminal, a mobile terminal, or it may have another specified function.

A network of arbitrary size and complexity can be maintained through the architecture of the extended service set (ESS), shown in Fig. 11.3. Here, STAs have full mobility and may move from one BSS to another while remaining in the network. Fig. 11.3 shows another element type—a portal. The portal is a gateway between

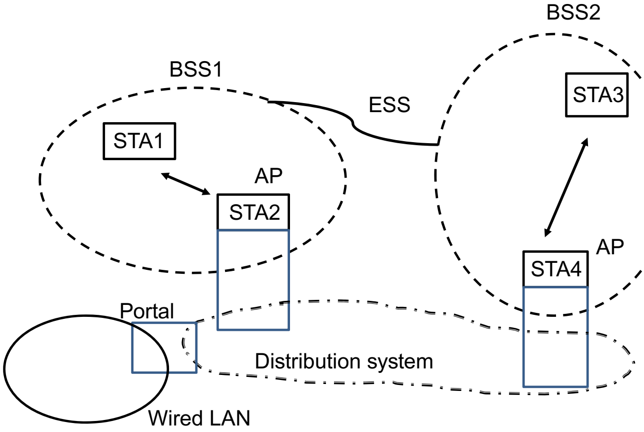


FIG. 11.3

Extended service set.

the WLAN and a wired LAN. It connects the medium over which the APs communicate to the medium of the wired LAN—coaxial cable or twisted pair lines, for example.

In addition to the functions Wi-Fi provides for distributing data throughout the network, two other important services, although optionally used, are provided. They are authentication and encryption. Authentication is the procedure used to establish the identity of a station as a member of the set of stations authorized to associate with another station. Encryption applies coding to data to prevent an eavesdropper from intercepting it. 802.11 details the implementation of these services in the MAC. Further protection of confidentiality may be provided by higher software layers in the network that are not part of 802.11.

The operational specifics of WLAN are described in IEEE 802.11 in terms of defined protocols between lower-level software layers. In general, networks may be described by the communication of data and control between adjacent layers of the Open System Interconnection Reference Model (OSI/RM), shown in Fig. 11.4, or the peer-to-peer communication between like layers of two or more terminals in the network. The bottom layer, physical, represents the hardware connection with the transmission medium that connects the terminals of the network—cable modem, radio transceiver and antenna, infrared transceiver, or power line transceiver, for example. The software of the upper layers is wholly independent of the transmission medium and in principle may be used unchanged no matter what the nature of the medium and the physical connection to it. IEEE 802.11 is concerned only with the two lowest layers, physical and data link.

IEEE 802.11 prescribes the protocols between the MAC sublayer of the data link layer and the physical layer, as well as the electrical specifications of the physical layer. Fig. 11.5 illustrates the relationship between the physical and MAC layers

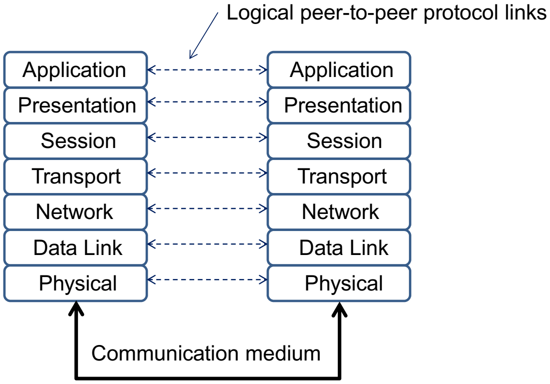


FIG. 11.4

Open system interconnection reference model.

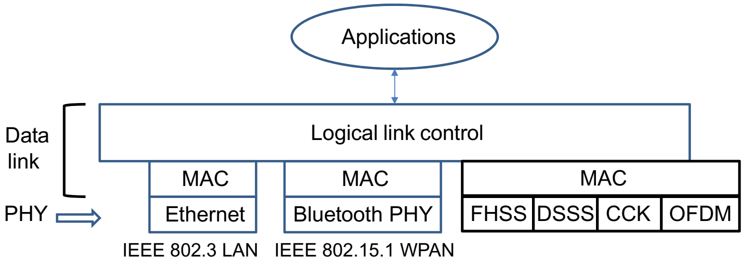


FIG. 11.5

Data link and physical layers (PHY).

of several types of networks with upper-layer application software interfaced through a commonly defined logical link control (LLC) layer. The LLC is common to all IEEE local area networks and is independent of the transmission medium or medium access method. Thus, its protocol is the same for wired local area networks and the various types of wireless networks.

The MAC service is the essence of the WLAN. Its implementation may be by high-level digital logic circuits or a combination of logic and a microcontroller or a digital signal processor. While the PHY of IEEE 802.11 describes wireless signal characteristics such as data rates and modulation techniques (DSSS, CCK, OFDM), the MAC station service consists of the following functions:

- Authentication
- Deauthentication
- Data confidentiality

- Delivery of data packets to and from higher protocol levels, which includes control of access to the physical medium
- Dynamic frequency selection (DFS)
- Transmit power control (TPC)
- QoS support
- Radio measurement

11.3 Medium access

An important attribute of any communications network is the method of access to the medium. 802.11-2016 prescribes three possibilities: distributed coordination function (DCF), hybrid coordination function (HCF), and mesh coordination function (MCF). A point coordination function (PCF) which is an optional polling method prescribed for 802.11, is now obsolete.

The fundamental access method in IEEE 802.11 is the DCF, which is known as CSMA/CA (carrier sense multiple access with collision avoidance). It is based on a procedure during which a station wanting to transmit may do so only after listening to the channel and determining that it is not busy. If the channel is busy, the station must wait until the channel is idle. In order to minimize the possibility of collisions when more than one station wants to transmit at the same time, each station waits a random time-period, called a back off interval, before transmitting, after the channel goes idle. Fig. 11.6 shows how this method works. Figure sections are shown as a numeral in a circle.

In the figure, a previous transmission is recognized by a station that is attempting to transmit. The station may start to transmit if the channel is idle, determined by a carrier sense mechanism, for a period of at least a duration of an interframe space (IFS) since the end of any other transmission (section 1 of the figure). Several different duration IFS's are defined, in order to give access priority to different types of frame exchanges. Data frame and management frame exchanges require the use of the DIFS (distributed coordination function interframe space), shown in the figure. If the channel is busy, as shown in section 2 of the figure, it must defer access and enter

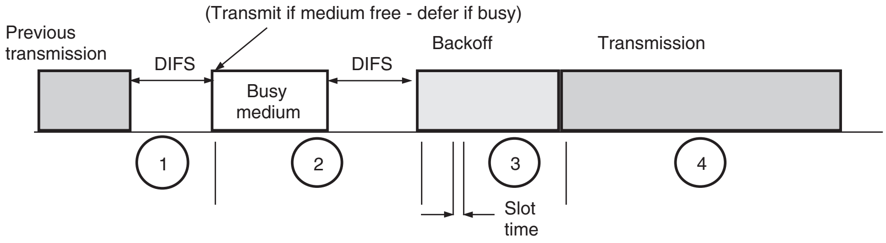


FIG. 11.6

CSMA/CA access method.

a back off procedure. The station waits until the channel is idle, and then waits an additional period of DIFS. Now it computes a time-period called a back off window that equals a pseudo-random number multiplied by a constant called the “slot time.” As long as the channel is idle, as it is in section 3 of the figure, the station may transmit its frame at the end of the back off window, section 4. During every slot time of the back off window the station senses the channel, and if it is busy, the counter that holds the remaining time of the back off window is frozen until the channel becomes idle and the back off counter resumes counting down.

At the conclusion of a received frame and ascertaining through a frame check sequence field (FCS) that it is not in error, the receiving station sends a short acknowledgement (ACK) to the sender. The waiting period for sending the ACK is a short interframe space (SIFS) of less duration than the DIFS, thereby giving priority to the acknowledgement. If the sender does not hear an ACK during a specified waiting period after concluding his transmission, he assumes the frame was not received and must send it again.

In waiting for a channel to become idle, a transmission contender doesn’t have to listen continuously. When one station hears another station access the channel, it notes the frame length field that is transmitted on every frame and updates a memory location called a network allocation vector (NAV) which gives the total occupation time for the station presently using the channel. After taking into account the time of the acknowledgement transmission that replies to a data transmission, the time until the channel will become idle is known even without physically sensing it. This is called a virtual carrier sense mechanism.

The procedure shown in Fig. 11.6 may not work well under some circumstances. For example, if several stations are trying to transmit to a single AP, two or more of them may be positioned such that they all are in range of the AP but not of each other. In this case, a station sensing the activity of the channel may not hear another station that is transmitting on the same network. To get around this “hidden node” problem, a refinement of the described CSMA/SA procedure can be used. A station thinking the channel is clear sends a short RTS (request to send) control frame to the AP. It then waits to receive a CTS (clear to send) reply from the AP, which is in range of all contenders for transmission, before sending its data transmission. RTS and CTS transmissions access the channel after an SIFS, so other stations waiting to transmit cannot interfere because they have to wait the longer DIFS time after the previous transmission and by then the channel is already occupied. If the originating station doesn’t hear the CTS it assumes the channel was busy and so it must try to access the channel again. This RTS/CTS procedure is also effective when not all stations on the network have compatible modulation facilities for high rate communication and one station may not be able to detect the transmission length field of another. RTS and CTS transmissions are always sent at the lowest rate that is common to all participants in the network. Data frame duration is included in the RTS/CTS messages so stations waiting to access a channel can set their NAV and defer transmissions even when they do not hear both sides of the communication.

Use of RTS/CTS is optional and its use depends on frame length. For short data or management frames it would not be used because the overhead of the RTS/CTS transmissions reduces the benefit of priority access to the medium. Above a certain frame length threshold, the RTS/CTS option can increase throughput.

11.3.1 Hybrid coordination function

The HCF is a medium access procedure associated with QoS requirements that gives differentiated priorities to transmitted traffic through four different access classes. It works essentially by defining backoff times within an IFS that is shorter than the DIFS and can give controlled access to applications that require regular time slots, for example voice and multimedia streaming while maintaining protection against transmission collisions. HCF controlled channel access (HCCA) is an aspect of HCF that gives higher priority channel access to non-AP stations. It works essentially as a polling mechanism. Stations may transmit multiple frames during a polling period.

11.3.2 Mesh coordination function (MCF)

The MCP is a MAC mechanism for mesh networks. It has a contention based channel access procedure and controlled channel access where management frames are used to make reservations for future transmissions. Neighboring stations hear these reservations and do not transmit during the reserved periods, thereby reducing potential congestion.

11.4 Physical layer

The discussion so far on the services and the organization of the WLAN did not depend explicitly on the details of the wireless connection between the members of the network but those details affect the nature and quality of the services that the network can provide. 802.11 and its amendments specify various bit rates, modulation methods, and operating frequency channels on three frequency bands (plus TV white space), which we discuss in this section. The distinctions of the types of physical layers covered by IEEE 802.11-2016 are shown in Table 11.1.

Details are given below.

11.4.1 IEEE 802.11 basic

The original version of the 802.11 specification prescribes three different air interfaces, each having two data rates. One is infrared and the others are based on FHSS and direct-sequence spread-spectrum, each supporting raw data rates of 1 and 2 Mbps. Below is a short description of the IR and FHSS links, for historical interest since these modes are now obsolete. A more detailed review of DSSS follows.

Table 11.1 IEEE 802.11-2016 physical layers

Name	Amendment	Frequencies (GHz)	Bandwidth (MHz)	Modulation	MIMO streams	Data rate (Mb/s)
DSSS	—	2.4	20	DSSS	—	1, 2
HR/DSSS (high rate)	802.11b	2.4	20	CCK complementary code keying	—	5.5, 11
OFDM	802.11a	5	20 (also 10, 5)	OFDM	—	Up to 54
ERP (extended rate)	802.11g	2.4	20	OFDM, CCK, DSSS	—	Up to 54
HT (high throughput)	802.11n	5, 2.4	20, 40	OFDM + backward compatible	4	600
DMG (directional multi-gigabit)	802.11ad	60	2160	SC Single carrier	Beam forming	8,085 max
VHT (very high throughput)	802.11ac	5	20, 40, 80, 160	OFDM	8, MU-MIMO 4 × 4 (8 max)	6,933.3 max
TVHT (television VHT)	802.11af	0.540-0.790 TV white space	6, 7, 8; × 1, 2, 4	OFDM	4	568.9 max

11.4.1.1 Infrared PHY

Infrared communication links have some advantages over radio wave transmissions. They are completely confined within walled enclosures and therefore eavesdropping concerns are greatly relieved, as are problems from external interference. Also, they are not subject to intentional radiation regulations. The IEEE 802.11 IR physical layer is based on diffused infrared links, and the receiving sensor detects radiation reflected off ceilings and walls, making the system independent of line-of-site. The range limit is on the order of 10 m. Baseband pulse position modulation is used, with a nominal pulse width of 250 nsec. The IR wavelength is between 850 and 950 nM. The 1 Mbps bit rate is achieved by sending symbols representing 4 bits, each consisting of a pulse in one of 16 consecutive 250 ns slots. This modulation method is called 16-PPM. Optional 4-PPM modulation, with four slots per two-bit symbol, gives a bit rate of 2 Mbps.

Although part of the original IEEE 802.11 specification and having what seems to be useful characteristics for some applications, products based on the infrared physical layer for WLAN were not generally commercially available. However, point-to-point, very short-range infrared links using the IrDA (infrared data association) standard were widespread. These links worked reliably line-of-site at 1 m and may be still found, for example, in desktop and notebook computers, handheld PC's, printers, cameras and toys. Data rates range from 2400 bps to 16 Mbps. Bluetooth devices have taken over many of the applications but for some cases IrDA imbedding still has an advantage because of its much higher data rate capability. We may expect that 802.11 DMG (see table) will fill the role that IR has had for very short range high speed connections to computer peripherals but with data rates several orders of magnitude greater.

11.4.1.2 FHSS PHY

While overshadowed by the DSSS PHY, acquaintance with the FHSS option in 802.11 may still be of interest. In FHSS WLAN, transmissions occur on carrier frequencies that hop periodically in pseudo-random order over almost the complete span of the 2.4 GHz ISM band. This span in North America and most European countries is 2.400 to 2.4835 GHz, and in these regions there are 79 hopping carrier frequencies from 2.402 to 2.480 GHz. The dwell on each frequency is a system-determined parameter, but the recommended dwell time is 20 ms, giving a hop rate of 50 hops per second. In order for FHSS network stations to be synchronized, they must all use the same pseudo-random sequence of frequencies, and their synthesizers must be in step, that is, they must all be tuned to the same frequency channel at the same time. Synchronization is achieved in 802.11 by sending the essential parameters—dwell time, frequency sequence number, and present channel number—in a frequency parameter set field that is part of a beacon transmission sent periodically on the channel. A station wishing to join the network can listen to the beacon and synchronize its hop pattern as part of the network association procedure.

The FHSS physical layer uses GFSK (Gaussian frequency shift keying) modulation, and must restrict transmitted bandwidth to 1 MHz at 20 dB down (from peak carrier).

This bandwidth holds for both 1 Mbps and 2 Mbps data rates. For 1 Mbps data rate, nominal frequency deviation is ±160 kHz. The data entering the modulator is filtered by a Gaussian (constant phase delay) filter with 3 dB bandwidth of 500 kHz. Receiver sensitivity must be better than −80 dBm for a 3% frame error rate. In order to keep the same transmitted bandwidth with a data rate of 2 Mbps, four-level frequency shift-keying is employed. Data bits are grouped into symbols of two bits, so each symbol can have one of four levels. Nominal deviations of the four levels are ±72 and ±216 kHz. A 500 kHz Gaussian filter smoothes the four-level 1 megasymbols per second at the input to the FSK modulator. Minimum required receiver sensitivity is −75 dBm.

Although development of Wi-Fi for significantly increased data rates has based on DSSS, FHSS does have some advantageous features. Many more independent networks can be collocated with virtually no mutual interference using FHSS than with DSSS. As we will see later, only three independent DSSS networks can be collocated. However, 26 different hopping sequences (North America and Europe) in any of three defined sets can be used in the same area with low probability of collision. Also, the degree of throughput reduction by other 2.4 GHz band users, as well as interference caused to the other users is lower with FHSS. FHSS implementation may at one time also have been less expensive. However, the updated versions of 802.11—specifically 802.11a, 802.11b, and 802.11g—have all based their methods of increasing data rates on the broadband channel characteristics of DSSS in 802.11, while being downward compatible with the 1 and 2 Mbps DSSS modes (except for 802.11a which operates on a different frequency band). Bluetooth has some of the characteristics of 802.11 FHSS but has advanced well beyond the capabilities of the earlier standard.

11.4.1.3 DSSS PHY

The channel characteristics of the DSSS physical layer in 802.11 are retained in the high data rate updates of the specification. This is natural, since systems based on the newer versions of the specification must retain compatibility with the basic 1 and 2 Mbps physical layer. The channel spectral mask is shown in Fig. 11.7, superimposed on the simulated spectrum of a filtered 1 Mbps transmission. It is 22 MHz wide at the −30 dB points. Fourteen channels are allocated in the 2.4 GHz ISM band, whose center frequencies are 5 MHz apart, from 2.412 to 2.484 GHz. The highest channel, number fourteen, is designated for Japan where the allowed band edges are 2.471 and 2.497 GHz. In the United States and Canada, the first eleven channels are used. Fig. 11.8 shows how channels one, six and eleven may be used by three adjacent independent networks without co-interference. When there are no more than two networks in the same area, they may choose their operating channels to avoid a narrow-band transmission or other interference on the band.

In 802.11 DSSS, a pseudo-random bit sequence phase modulates the carrier frequency. In this spreading sequence, bits are called chips. The chip rate is 11 megachips per second (Mcps). Data is applied by phase modulating the spread carrier. There are eleven chips per data symbol. The chosen pseudo-random sequence is a

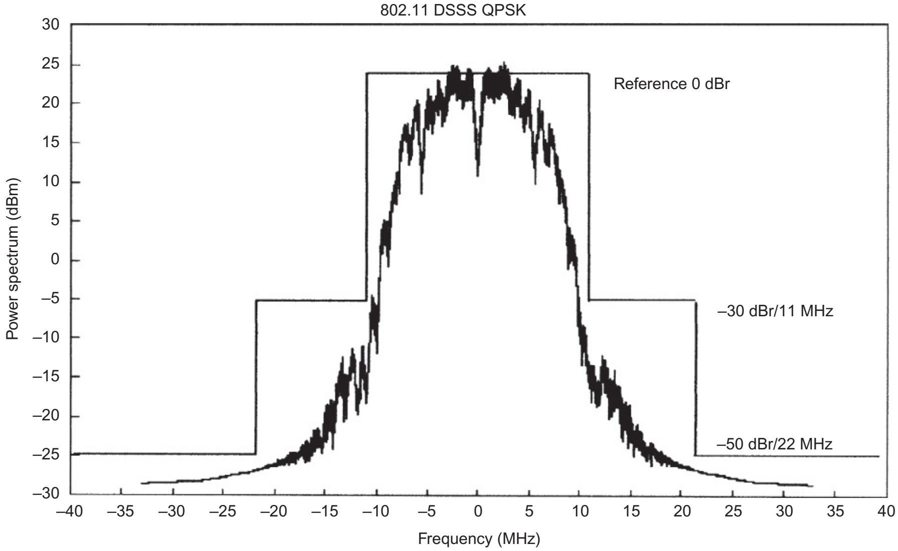


FIG. 11.7

802.11 DSSS spectral mask and example spectrum.

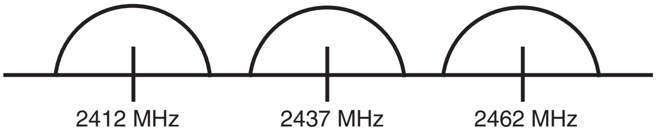


FIG. 11.8

DSSS non-interfering channels.

Barker sequence, represented as 1,−1,1,1,−1,1,1,1,−1,−1,−1. Its redeeming property is that it is optimally detected in a receiver by a matched filter or correlation detector. Fig. 11.9 is one possible implementation of the modulator. The DSSS PHY specifies two possible data rates—1 and 2 Mbps. The differential encoder takes the data stream and produces two output streams at 1 Mbps that represent changes in data polarity from one symbol to the next. For a data rate of 1 Mbps, differential binary phase shift keying is used. The input data rate of 1 Mbps results in two identical output data streams that represent the changes between consecutive input bits. Differential quadrature phase shift keying handles 2 Mbps of data. Each sequence of two input bits creates four permutations on two outputs. The differential encoder outputs the differences from symbol to symbol on the lines that go to the inputs of the exclusive OR gates shown in Fig. 11.9. The outputs on the *I* and *Q* lines are the Barker sequence of 11 Mcps inverted or sent straight through, at a rate of 1 Msps (mega-symbols per second), according to the differentially encoded data

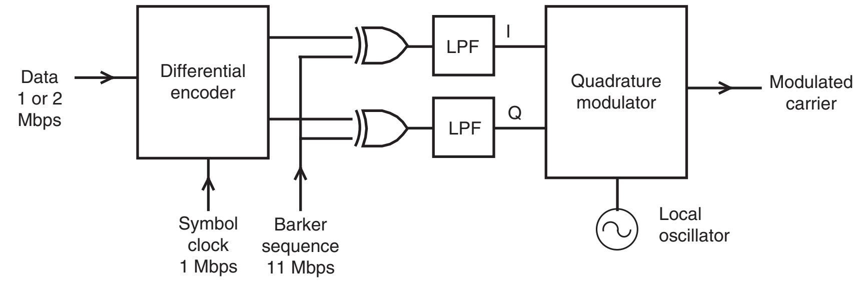


FIG. 11.9

IEEE 802.11 DSSS modulation.

at the exclusive OR gate inputs. These outputs are spectrum shifted to the RF carrier frequency (or an intermediate frequency for subsequent upconversion) in the quadrature modulator.

Reception of DSSS signals is represented in Fig. 11.10. The downconverted *I* and *Q* signals are applied to matched filters or correlation detectors. These circuits correlate the Barker sequence with the input signal and output an analog signal that represents the degree of correlation. The following differential decoder performs the opposite operation of the differential encoder described above and outputs the 1 or 2 Mbps data.

The process of despreading the input signal by correlating it with the stored spreading sequence requires synchronization of the receiver with transmitter timing and frequency. To facilitate this, the transmitted frame starts with a synchronization field (SYNC), shown at the beginning of the physical layer protocol data unit in Fig. 11.11. Then a start frame delimiter (SFD) marks out the commencement of

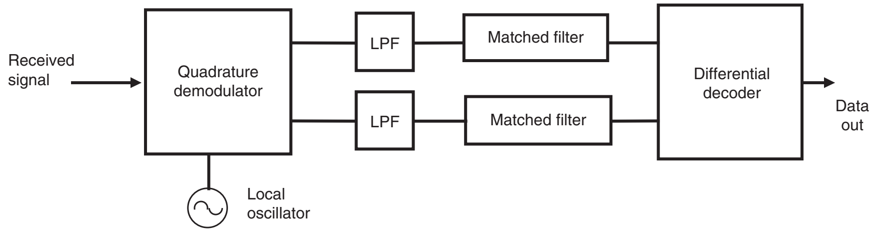
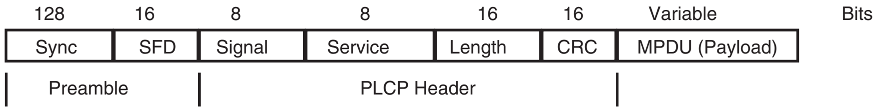


FIG. 11.10

IEEE 802.11 reception.



128	16	8	8	16	16	Variable	Bits
Sync	SFD	Signal	Service	Length	CRC	MPDU (Payload)	
Preamble		PLCP Header					

FIG. 11.11

IEEE 802.11 frame format.

the following information bearing fields. All bits in the indicated preamble are transmitted at a rate of 1 Mbps, no matter what the subsequent data rate will be. The signal field specifies the data rate of the following fields in the frame so that the receiver can adjust itself accordingly. The next field, SERVICE, contains all zeros for devices that are only compliant with the basic version of 802.11, but some of its bits are used in devices conforming with updated versions. The value of the length field is the length, in microseconds, required to transmit the data-carrying field labeled MPDU (MAC protocol data unit). An error check field, labeled CRC, protects the integrity of the SIGNAL, SERVICE, and LENGTH fields. The last field MPDU (MAC protocol data unit) is the data passed down from the MAC to be sent by the physical layer, or to be passed up to the MAC after reception. All bits in the transmitted frame are pseudo-randomly scrambled to ensure even power distribution over the spectrum. Data are returned to its original form by descrambling in the receiver.

11.4.2 High rate DSSS

The “b” amendment to the original 802.11 specification supports a higher rate physical layer for the 2.4 GHz band. It is this 802.11b version that provided the impetus for Wi-Fi proliferation. With it, data rates of 5.5 and 11 Mbps were enabled, while retaining downward compatibility with the original 1 and 2 Mbps rates. The slower rates may be used not only for compatibility with devices that aren’t capable of the extended rates, but also for fall back when interference or range don’t provide the required signal-to-noise ratio for communication using the higher rates.

As previously stated, the increased data rates specified in 802.11b do not entail a larger channel bandwidth. Also, the narrow-band interference rejection, or jammer resisting qualities of direct sequence spread-spectrum are retained. The classical definition of processing gain for DSSS as being the chip rate divided by the data bandwidth doesn’t apply here. In fact, the processing gain requirement that for years was part of the FCC Rules paragraph 15.247 definition of DSSS was deleted in an update from August 2002, and at the same time reference to DSSS was replaced by “digital modulation.”

The mandatory high-rate modulation method of 802.11b is called complementary code keying (CCK). An optional mode called packet binary convolutional coding (PBCC) was also described in the specification but it is no longer applicable. Although there are similarities in concept, the two modes differ in implementation and performance. First the general principle of high-rate DSSS is presented below, applying to both CCK and PBCC, then the details of CCK are given.

As in the original 802.11, a pseudo-random noise sequence at the rate of 11 Mcps is the basis of high-rate transmission in 802.11b. It is this 11 Mcps modulation that gives the 22 MHz null-to-null bandwidth. However, in contrast to the original specification, the symbol rate when sending data at 5.5 or 11 Mbps is 1.375 Msps. Eight chips per symbol are transmitted instead of eleven chips per symbol for data rates of 1 or 2 Mbps. In “standard” DSSS as used in 802.11, the modulation, BPSK or QPSK, is applied to the group of eleven chips constituting a symbol. The series of eleven chips in the symbol is always the same (the Barker sequence previously defined) while their phase as a whole is modified in accordance with the data. In contrast, high-rate DSSS uses a different 8-chip sequence in each symbol, depending on the sequence of data bits that each symbol represents. Quadrature modulation is used, and each chip has an I value and a Q value which represent a complex number having a normalized amplitude of one and some angle, α, where α = arctangent (Q/I). α can assume one of four values divided equally around 360 degrees. Since each complex bit has four possible values, there are a total of $4^8 = 65536$ possible 8-bit complex words. For the 11 Mbps data rate, 256 out of these possibilities are actually used—which one being determined by the sequence of 8 data bits applied to a particular symbol. Only 16-chip sequences are needed for the 5.5 Mbps rate, determined by four data bits per symbol. The high-rate algorithm describes the manner in which the 256 code words, or 16 code words, are chosen from the 65536 possibilities. The chosen 256 or 16 complex words have the very desirable property that when correlation detectors are used on the I and Q lines of the received signal, down converted to baseband, the original 8-bit (11 Mbps rate) or 4-bit (5.5 Mbps rate) sequence can be decoded correctly with high probability even when reception is accompanied by noise and other types of channel distortion.

The concept of CCK modulation and demodulation is shown in Figs. 11.12 and 11.13. It's explained below in reference to a data rate of 11 Mbps. The multiplexer of Fig. 11.12 takes a block of eight serial data bits, entering at 11 Mbps, and outputs them in parallel, with updates at the symbol rate of 1.375 MHz. The six latest data bits determine 1 out of 64 (2^6) complex code words. Each code word is a sequence of eight complex chips, having phase angles α_1 through α_8 and a magnitude of unity. The first two data bits, d_0 and d_1, determine an angle, α'_8, which, in the code rotator (see Fig. 11.12), rotates the whole code word relative to α_8 of the previous code word. This angle of rotation becomes the absolute angle α_8 of the present code word. The normalized I and Q outputs of the code rotator, which after filtering are input to a quadrature modulator for up conversion to the carrier (or intermediate) frequency, are:

$$I_i = \cos(\alpha_i), Q_i = \sin(\alpha_i)\ i = 1\ldots8$$

Fig. 11.13 is a summary of the development of code words a for 11 Mbps rate CCK modulation. High rate modulation is applied only to the payload—MPDU in Fig. 11.11. The code word described in Fig. 11.13 is used as shown for the first symbol and then every other symbol of the payload. However, it is modified by adding 180° to each element of the code word of the second symbol, fourth symbol, and so on.

The development of the symbol code word or chip sequence may be clarified by an example worked out per Fig. 11.13. Let's say the 8-bit data sequence for a symbol is $\boldsymbol{d} = d_0 \ldots d_7 = 1\,0\,1\,0\,1\,1\,0\,1$. From the phase table of Fig. 11.13 we find the angles $\varphi : \varphi_1 = 180°$, $\varphi_2 = 180°$, $\varphi_3 = -90°$, $\varphi_4 = 90°$. Now summing up these values to

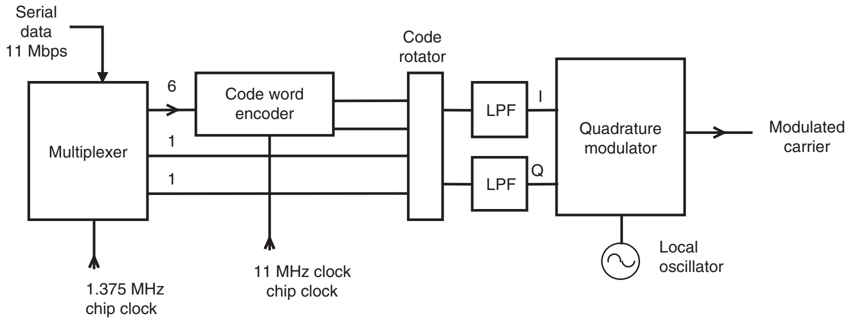


FIG. 11.12

High-rate modulator—11 Mbps.

Data symbol: $d_0\, d_1\, d_2\, d_3\, d_4\, d_5\, d_6\, d_7$

Phase table

d_i	d_{i+1}	φ
0	0	0^0
1	0	180^0
0	1	90^0
1	1	-90^0

Phase $(d_0,d_1) = \varphi_1$
Phase $(d_2,d_3) = \varphi_2$
Phase $(d_4,d_5) = \varphi_3$
Phase $(d_6,d_7) = \varphi_4$

$$\begin{aligned}
\alpha_1 &= \varphi_1 + \varphi_2 + \varphi_3 + \varphi_4\\
\alpha_2 &= \varphi_1 + \varphi_3 + \varphi_4\\
\alpha_3 &= \varphi_1 + \varphi_2 + \varphi_4\\
\alpha_4 &= \varphi_1 + \varphi_4 + 180^0\\
\alpha_5 &= \varphi_1 + \varphi_2 + \varphi_3\\
\alpha_6 &= \varphi_1 + \varphi_3\\
\alpha_7 &= \varphi_1 + \varphi_2 + 180^0\\
\alpha_8 &= \varphi_1
\end{aligned}$$

$$\begin{aligned}
I_i &= \cos(\alpha_i)\\
Q_i &= \sin(\alpha_i)\\
i &= 1\ldots8
\end{aligned}$$

FIG. 11.13

Derivation of code word.

get the angle α_i of each complex chip, then taking the cosine and sine to get I_i and Q_i, we summarize the result in the following table:

i	1	2	3	4	5	6	7	8
α	0	180	90	90	−90	90	180	180
I	1	−1	0	0	0	0	−1	−1
Q	0	0	1	1	−1	1	0	0

The code words for 5.5 Mbps rate CCK modulation are a subset of those for 11 Mbps CCK. In this case, there are four data bits per symbol which determine a total of 16 complex chip sequences. Four 8-element code words (complex chip sequences) are determined using the last two data bits of the symbol, d_2 and d_3. The arguments (angles) of these code words are shown in Table 11.2. Bits d_0 and d_1 are used to rotate the code words relative to the preceding code word as in 11 Mbps modulation and shown in the phase table of Fig. 11.13. Code words are modified by 180° every other symbol, as in 11 Mbps modulation.

The concept of CCK decoding for receiving high rate data is shown in Fig. 11.14. For the 11 Mbps data rate, a correlation bank decides which of the 64 possible codes best fits each received 8-bit symbol. It also finds the rotation angle of the whole code relative to the previous symbol (one of four values). There are a total of 256 (64 × 4) possibilities and the chosen one is output as serial data. At the 5.5 Mbps rate there are four code words to choose from and after code rotation a total of 16 choices from which to decide on the output data.

To maintain compatibility with earlier non-high-rate systems, the DSSS frame format shown in Fig. 11.11 is retained in 802.11b. The 128-bit preamble and the

Table 11.2 5.5 Mbps CCK decoding

d_3, d_2	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8
00	90	0	90	180	90	0	−90	0
10	−90	180	−90	0	90	0	−90	0
01	−90	0	−90	180	−90	0	90	0
11	90	180	90	0	−90	0	90	0

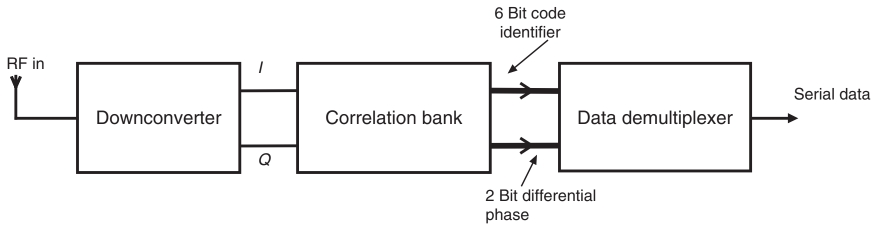


FIG. 11.14

CCK decoding.

header are transmitted at 1 Mbps while the payload MPDU can be sent at a high rate of 5.5 or 11 Mbps. The long and slow preamble reduces the throughput and cancels some of the advantage of the high data rates. 802.11b defines an optional short preamble and header which differ from the standard frame by sending a preamble with only 72 bits and transmitting the header at 2 Mbps, for a total overhead of 96 μs instead of 192 μs for the long preamble and header. Devices using this option can only communicate with other stations having the same capability.

Use of higher data rates entails some loss of sensitivity and hence range. The minimum specified sensitivity at the 11 Mbps rate is −76 dBm for a frame-error rate of 8% when sending a payload of 1024 bytes, as compared to a sensitivity of −80 dBm for the same frame-error rate and payload length at a data rate of 2 Mbps.

11.4.3 802.11a and OFDM

In the search for ways to communicate at even higher data rates than those applied in 802.11b, a completely different modulation scheme, OFDM (orthogonal frequency division multiplexing) was adopted for 802.11a. It is not DSSS yet it has a channel bandwidth similar to the DSSS systems already discussed. The 802.11a amendment is defined for channel frequencies between 5.2 and 5.85 GHz, obviously not compatible with 802.11b signals in the 2.4 GHz band. However, since the channel occupancy characteristics of its modulation are similar to that of DSSS Wi-Fi, the same system was adopted in IEEE 802.11g for enabling the high data rates of 802.11a on the 2.4 GHz band, while allowing downward compatibility with transmissions conforming to 802.11b.

802.11a specifies data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s. As transmitted data rates go higher and higher, the problem of multipath interference becomes more severe. Reflections in an indoor environment can result in multipath delays on the order of 100 ns but may be as long as 250 ns, and a signal with a bit rate of 10 Mbps (period of 100 ns) can be completely overlapped by its reflection. When there are several reflections, arriving at the receiver at different times, the signal may be mutilated beyond recognition. The OFDM transmission system goes a long way to solving the problem. It does this by sending the data partitioned into symbols whose period is several times the expected reflected path length time differences. The individual data bits in a symbol are all sent in parallel on separate subcarrier frequencies within the transmission channel. Thus, by sending many bits during the same time, each on a different frequency, the individual transmitted bit can be lengthened so that it won't be affected by the multipath phenomenon. The higher bit rates are accommodated by representing a group of data bits as the phase and amplitude of a symbol sent on a particular subcarrier. A subcarrier modulated using quadrature phase shift keying (QPSK) can represent two data bits per symbol and 64-QAM (quadrature amplitude modulation) can present six data bits as a single symbol on a subcarrier.

Naturally, transmitting many subcarriers on a channel of given width brings up the problem of interference between those subcarriers. There will be no interference between them if all the subcarriers are orthogonal—that is, if the integral of any two different subcarriers over the symbol period is zero. It is easy to show that this condition exists if the frequency difference between adjacent subcarriers is the inverse of the symbol period.

In OFDM, the orthogonal subcarriers are generated mathematically using the inverse Fourier transform (IFT), or rather its discrete equivalent, the inverse discrete Fourier transform (IDFT). The IDFT may be expressed as:

$$x(n) = \frac{1}{N}\sum_{m=0}^{N-1} X(m)[\cos(2\pi mn/N) + j\sin(2\pi mn/N)]$$

$x(n)$ are complex sample values in the time domain, $n = 0 \ldots N-1$, and $X(m)$ are the given complex values, representing magnitude and phase, for each subcarrier frequency in the frequency domain. N is the number of subcarriers. The IDFT expression indicates that each sample of the time domain signal is the sum of N harmonically related sine and cosine waves each of whose magnitude and phase is given by $X(m)$. We can relate the right side of the expression to absolute frequency by multiplying the arguments $2\pi mn/N$ by f_1/f_s to get

$$x(n) = \frac{1}{N}\sum_{m=0}^{N-1} X(m)[\cos(2\pi m f_1 n t_s) + j\sin(2\pi m f_1 n t_s)] \tag{11.1}$$

where f_1 is the fundamental subcarrier and the difference between adjacent subcarriers, and t_s is the sample time $1/f_s$. In 802.11a OFDM, the sampling frequency f_s is 20 MHz and $N = 64$, so $f_1 = 312.5$ kHz. Symbol time is $Nt_s = 64/f_s = 3.2$ µs.

In order to prevent intersymbol interference, 802.11a inserts a guard time of 0.8 µs in front of each symbol, after the IDFT conversion. During this time, the last 0.8 µs of the symbol is copied in front of its beginning, so the guard time is also called a circular prefix. Thus, the extended symbol period that is transmitted is 3.2 + 0.8 = 4 µs. The guard time segment is deleted after reception and before reconstruction of the transmitted data.

Although Eq. (11.1), where $N = 64$, indicates 64 possible subcarriers, only 48 are used to carry data, and four more for pilot signals to help the receiver phase lock to the transmitted carriers. The remaining carriers that are those at the outside of the occupied bandwidth, and the DC term ($m = 0$ in Eq. 11.1), are null. It follows that there are 26 ((48 + 4)/2) carriers on each side of the nulled center frequency. Each channel width is 312.5 kHz, so the occupied channels have a total width of 53 × 312.5 kHz = 16.5625 MHz.

For accommodating a wide range of data rates, four modulation schemes are used—BPSK, QPSK, 16-QAM and 64-QAM, requiring 1, 2, 4, and 6 data bits per symbol, respectively. Forward error correction (FEC) coding is employed with OFDM, which entails adding code bits in each symbol. Three coding rates: 1/2, 2/3, and 3/4, indicate the ratio of data bits to the total number of bits per symbol for different degrees of coding performance. FEC permits reconstruction of the correct message in the receiver, even when one or more of the 48 data channels have selective interference that would otherwise result in a lost symbol. Symbol bits are

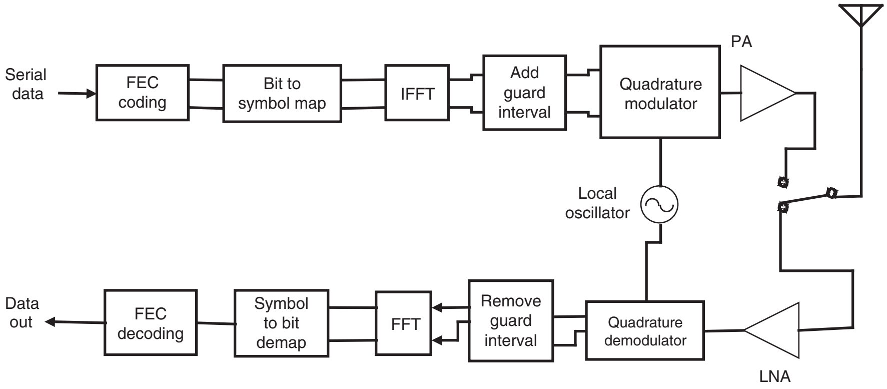


FIG. 11.15

OFDM system block diagram.

interleaved so that even if adjacent subcarrier bits are demodulated with errors, the error correction procedure will still reproduce the correct symbol. A block diagram of the OFDM transmitter and receiver is shown in Fig. 11.15. Blocks FFT and IFFT indicate the fast Fourier transform and its inverse instead of the mathematically equivalent (in terms of results) discrete Fourier transform and IFDT that we used above because it is much faster to implement. Table 11.3 lists the modulation type and coding rate used for each data rate, and the total number of bits per OFDM symbol, which includes data bits and code bits. The data rate in the first column is the result of multiplying the data bits per OFDM symbol (last column) by the transmitted symbol rate which is the inverse of the extended symbol period of 4 μs.

The frequency ranges in the 5 GHz band in accordance with FCC paragraphs 15.401–15.407 for unlicensed national information infrastructure (U-NII) devices

Table 11.3 OFDM characteristics according to data rate

Data rate (Mbps)	Modulation	Coding rate	Coded bits per subcarrier	Coded bits per OFDM symbol	Data bits per OFDM symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

are given in Section 10.2.2.10. Channel allocations are 5 MHz apart and 20 MHz spacing is needed to prevent co-channel interference.

Extension of the data rates of 802.11b to those of 802.11a, but on the 2.4 GHz band is covered in amendment 802.11g. The OFDM physical layer defined for the 5 GHz band is applied essentially unchanged to 2.4 GHz. Equipment complying with 802.11g must also have the lower-rate features and the CCK modulation technique of 802.11b so that it will be downward compatible with existing Wi-Fi systems.

11.4.3.1 HIPERLAN/2

While 802.11b was designed for compliance with regulations in the European Union and most other regions of the world, 802.11a was relevant to the regulations of the FCC. ETSI (European Telecommunications Standards Institute) developed a high-speed wireless LAN specification, called HIPERLAN/2 (high performance local area network), which met the European regulations and in many ways went beyond the capabilities of 802.11a. HIPERLAN/2 defined a physical layer essentially identical to that of 802.11a, using coded OFDM and the same data rates up to 54 Mbps. However, its second layer software level is very different from the 802.11 MAC and the two systems are not compatible. Features of HIPERLAN/2 that were necessary to meet European regulations, specifically DFS and TPC, as well as QoS features and high data security, have since been incorporated into IEEE 802.11 which has become the leading technology for WLAN the world over.

11.4.4 IEEE 802.11 throughput improvements

Two parameters of the 802.11 communication link that were modified for performance improvements are bandwidth and number of data streams. Both are responsible for the significantly increased data rate of the high throughput (HT) physical layer, the 802.11n amendment, over the basic OFDM specifications, 802.11a and 802.11g. HT PHY doubled bandwidth to 40 MHz and introduced MIMO, with a maximum of 4 signal streams. A third contributor to increased data rate is the modulation level. The VHT PHY, 802.11ac, uses up to 256-QAM, for 8 data bits per symbol, compared to 64-QAM, 6 bits per symbol, in the HT PHY. An increase in modulation level also increases susceptibility to noise and interference. The later amendments specified improved FEC, which also facilitated a higher code rate, which is the ratio of data bits to total bits (including code bits) in a code block. Still another factor in increased throughput is reduced overhead. Maintaining backward compatibility requires longer preambles and transmitting the frame header at the basic low data rate, needed for collision avoidance when a network is open to older devices conforming to older versions of the specification. HT PHY and VHT PHY have provision for “greenfield” operational mode, where a more streamlined frame header is used, assuming all devices on the network comply with the latest specification revision. Another way to reduce overhead is by using a shorter cyclic prefix on the OFDM symbol. HT and VHT PHY can optionally have a cyclic prefix of 400 ns instead of the legacy length of 800 ns.

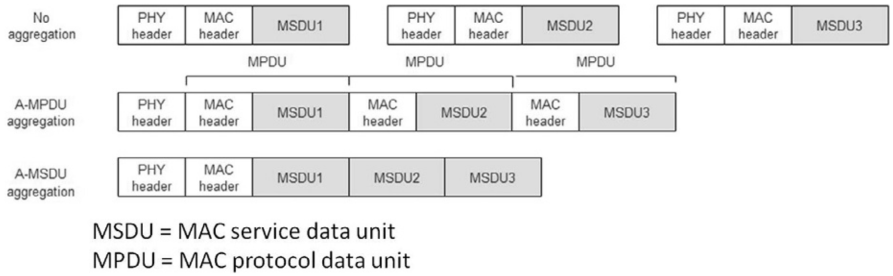


FIG. 11.16

Frame aggregation.

Still another throughput improvement technique in HT and VHT is packet aggregation, where data packets are combined in a single frame to substantially increase the data to header size ratio as shown in Fig. 11.16 [3]. The data, handed down to the data link layer from applications is designated MSDU (MAC Service Data Unit). MPDU (MAC Protocol Data Unit) is a subframe that includes the MSDU and a MAC header. The MAC sub-layer adds the MAC header, which includes addressing information and other functional fields relating to the data. Every transmitted frame must have a PHY header, which consists of synchronization and MIMO streaming fields. Not shown in Fig. 11.16 are the acknowledgement transmissions which follow each frame, so the impact on throughput is greater than is apparent in the figure. Although A-MSDU aggregation appears to yield the highest throughput, its advantage is reduced when frame errors occur. The whole A-MSDU frame must be retransmitted when there is an error, whereas in A-MPDU aggregation, only the MSDU and its header (the MPDU) that contained the error has to be retransmitted, with a lower reduction in throughput.

Table 11.4 shows a selection of parameters for the OFDM, HT, and VHT specifications and how they affect data rate. The difference between throughput and data rate should be noted. Throughput depends on frame length, header length, network

Table 11.4 Comparison of some OFDM, HT, and VHT parameters

PHY	Modulation	Code rate	Bandwidth (MHz)	MIMO streams	Data rate (Mb/s)
OFDM	16-QAM	1/2	20	—	24
OFDM	64-QAM	3/4	20	—	54
HT	16-QAM	1/2	20	1	26
HT	64-QAM	5/6	20	1	65
HT	64-QAM	5/6	20	2	130
HT	64-QAM	5/6	40	2	270
HT	64-QAM	5/6	40	4	540
VHT	256-QAM	5/6	40	4	720
VHT	256-QAM	5/6	80	4	1560

Note: cyclic prefix is 800 ns for all entries.

congestion, and acknowledgements, whereas data rate is the net rate of data bits in an OFDM symbol—the symbol bit rate times the code rate [3, 4].

It should be remembered that use of high level modulation and a high code rate requires a relatively high signal to noise ratio, which usually means short range. In order to gain full advantage of multiple MIMO data streams there must be low correlation of antenna elements which is generally not obtainable in small devices like smartphones. However, through MU-MIMO (multi-user MIMO), independent data streams can be transmitted simultaneously to several separated devices.

11.4.5 MIMO in 802.11

11.4.5.1 Estimating channel state at the receiver

The key to reaping the advantages of multiple antenna elements on the transmitter side, receiver side, or both, is knowledge of the propagation medium, represented by matrix **H** in Chapter 2 (Eqs. 2.20, 2.21). A receiver can construct this matrix by comparing received symbols at each of its receiving antenna elements with known symbols transmitted in turn from each of the transmitting antenna elements. For example, consider three transmitting antennas and two receiving antennas. Fig. 11.17 shows the propagation path constants when only antenna TX1 is transmitting a symbol

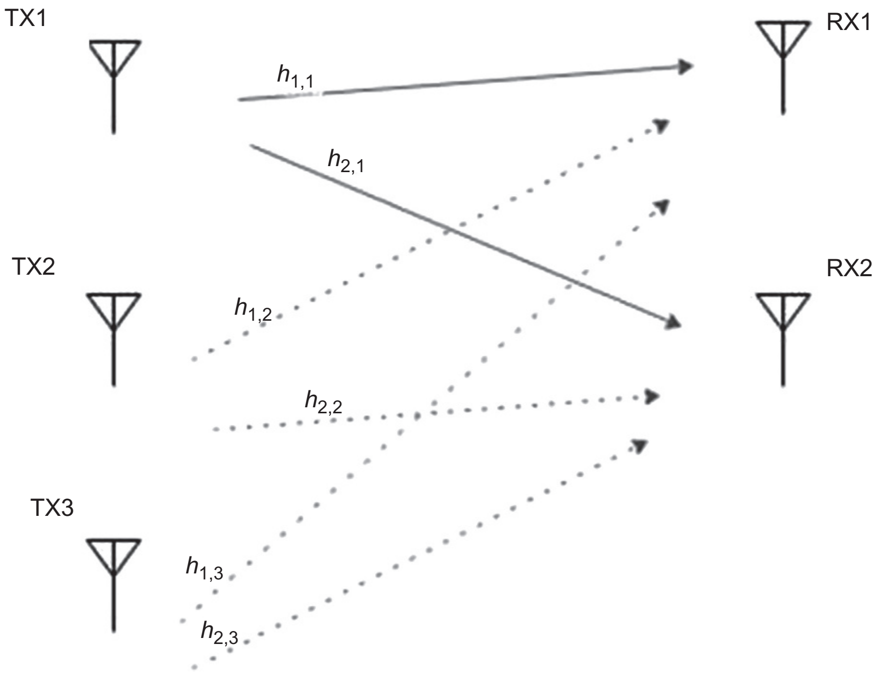


FIG. 11.17

Channel matrix. Solid line paths show channel coefficients when only TX1 is transmitting.

stream that is known to the receiver. In general, for each antenna element transmitting individually, the received signal r at each receiving antenna element is:

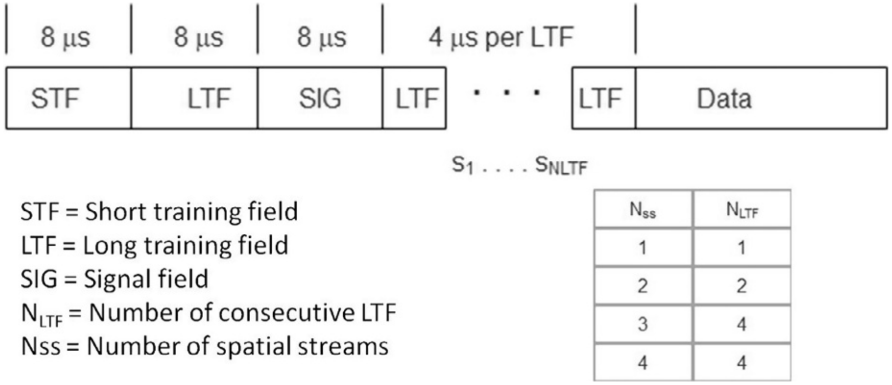
$$r_i = h_{i,j}s + n_i \tag{11.2}$$

where subscripts i and j refer to the specific receiver and transmitter antenna element respectively, s is the transmitted symbol and n is noise. This, and the following expressions, refer to the channel of one OFDM subcarrier, since h is a function of frequency and is different in each subchannel.

From sequential transmissions over each antenna element of a training symbol known to the receiver, the receiver can estimate each element of **H** without interference from the signals from the other antenna elements as

$$\hat{h}_{i,j} = r_i s^{-1} = h_{i,j}s \cdot s^{-1} + n_i s^{-1} = h_{i,j} + n_i s^{-1} \tag{11.3}$$

However, in IEEE 802.11 HT and VHT physical layers which use MIMO, the channel matrix **H** is found by sending a sequence of training symbols over all antenna elements at the same time yet avoiding interference between the spatial streams [2, 5, 6]. Fig. 11.18 shows a simplified PPDU (PHY protocol data unit) frame, taken from HT but applying in principle to VHT as well. The first two fields, labeled STF (short training field) and LTF (long training field) are used for synchronizing the frame to allow OFDM demodulation of the following SIG (signal) field, which gives the parameters, including the modulation and coding scheme, bandwidth, and frame length, that are needed to interpret the whole frame. Following SIG, one, two, or four long training field symbols for HT (up to eight for VHT), corresponding to the number of space-time streams (with the exception of four symbols for three spatial streams), are sent over all MIMO antenna elements. They are labeled s_1 through s_{NLTF}. Each of these LTF symbols is a modification of a long training symbol, which we label as a vector **S**, which has a value of "1" or "−1" for each of 56 sub-carrier data elements of the OFDM symbol. Fig. 11.19 shows the flow of the training


8 µs
8 µs
8 µs
4 µs per LTF
STF
LTF
SIG
LTF
. . .
LTF
Data
S1 . . . . SNLTF
STF = Short training field
LTF = Long training field
SIG = Signal field
NLTF = Number of consecutive LTF
Nss = Number of spatial streams

N_{ss}	N_{LTF}
1	1
2	2
3	4
4	4

FIG. 11.18

IEEE 802.11 HT PPDU frame showing training sequences.

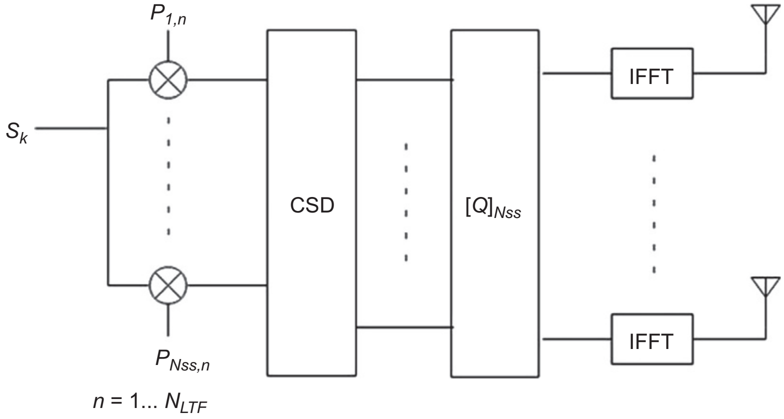


FIG. 11.19

Flow of training signals to antenna elements.

symbols for a particular subcarrier, subscript k. The parallel paths are the spatial streams in the frequency domain of the particular k symbol. The vector composed of all 64 subcarrier elements (56 data element and 8 null elements) for each spatial stream are inverse fast Fourier transformed (IFFT) to the time domain, then upconverted to the carrier frequency and transmitted on an antenna element. The block labeled CSD (cyclic shift diversity) shifts the phase of each symbol in each spatial stream in order to prevent unintentional beamforming. Block $[Q]$ produces intentional beamforming, which is optionally used, by adjusting phases and magnitudes of the spatial streams. Otherwise, that block passes each data stream to the IFFT block unchanged. The multiplying factors, elements of a matrix **P**, are what allows the receiver to obtain an estimation of each element in the channel matrix for each sub-carrier. The matrix **P** for HT 802.11 is:

$$\mathbf{P} = \begin{bmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \end{bmatrix} \tag{11.4}$$

This is an orthogonal matrix with the characteristic that the sum of corresponding product terms of any two rows is zero, whereas the sum of the product terms of any row times itself equals the number of columns. The same holds for the columns. A possibly truncated version of **P**, henceforth designated as $\mathbf{P}_{\mathrm{Nss}}$, has Nss rows and N_{LTF} columns (see table in Fig. 11.18).

The signal flow diagram in Fig. 11.19 should be regarded in two dimensions—time and space. As shown in Fig. 11.18, there are N_{LTF} consecutive long training field symbols of duration 4 μs each. In Fig. 11.19 the nth training element in time s_n of the kth subcarrier, with a value of $S_k =$ “1” or “−1” depending on k, enters on the left and is used to create Nss spatial streams after multiplication by an element of matrix $\mathbf{P}_{\mathrm{Nss}}$. A column of $\mathbf{P}_{\mathrm{Nss}}$ holds multipliers for each spatial stream. For example, for the first LTF, $n=1$, s_1 is multiplied by "1" for the first three spatial streams and "-1" for the last (the first column of $\mathbf{P}_{\mathrm{Nss}}$).

The frequency domain sub-carrier symbol detected at each receiver antenna element for a given LTF is

$$r_{i,n} = [h_{i,1}, \ldots, h_{i,\mathrm{NTX}}] \cdot S_k \cdot [\mathbf{P}_{\mathrm{Nss}}]_{(:,\,n)} + n_i \tag{11.5}$$

where i is the index of the receiver antenna element, NTX is the number of transmitting antennas (here the number of spatial streams), n is the index of the training frame and n_i is the noise at the ith receiving antenna. $[\mathbf{P}_{\mathrm{Nss}}]_{(:,\mathrm{n})}$ means the nth column of $\mathbf{P}_{\mathrm{Nss}}$. Note that the path coefficient h is constant from one symbol period (4 μs) to the next and is expected to be constant for the whole frame.

The total training information for a particular subcarrier symbol at all receiver antenna elements and over all training symbol time sequences can be expressed in matrix form as

$$\mathbf{r}_k = \mathbf{H}_k \cdot S_k \cdot \mathbf{P}_{\mathrm{Nss}} + \mathbf{N}_k \tag{11.6}$$

where $\mathbf{r}_k$ and $\mathbf{N}_k$ are matrices whose rows correspond to the number of receiver antenna elements and columns correspond to the number of symbols in a training sequence.

In order to estimate $\mathbf{H}_k$, $\mathbf{r}_k$ is multiplied by the inverse (or pseudo inverse if the matrix is not square) of the matrix of the training signals $S_k\mathbf{P}_{\mathrm{Nss}}$, Because of the orthogonal nature of $\mathbf{P}_{\mathrm{Nss}}$ and the fact that its elements are real, its inverse can be expressed as $\mathbf{P}^{\mathrm{T}}_{\mathrm{Nss}}$ times a scaling factor of $1/N_{\mathrm{LTF}}$. Superscript T stands for *transpose*. The estimate of $\mathbf{H}$ is then, comparable to Eq. (11.3)

$$\hat{\mathbf{H}}_k = \mathbf{r}_k \cdot \frac{\mathbf{P}^{\mathrm{T}}_{\mathrm{Nss}}}{S_k \cdot N_{\mathrm{LTF}}} = \mathbf{H}_k + \mathbf{N}_k \cdot \frac{\mathbf{P}^{\mathrm{T}}_{\mathrm{Nss}}}{S_k \cdot N_{\mathrm{LTF}}} \tag{11.7}$$

As an example, consider three transmitter antenna elements and two receiver antenna elements as depicted in Fig. 11.17. For the three spatial streams, $N_{\mathrm{LTF}} = 4$. Let $S_k = 1$. From Eqs. (11.4), (11.6) (after truncation of $\mathbf{P}$):

$$\mathbf{r}_k = \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} \\ h_{2,1} & h_{2,2} & h_{2,3} \end{bmatrix} \cdot 1 \cdot \begin{bmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} + \begin{bmatrix} n_{1,1} & n_{1,2} & n_{1,3} & n_{1,4} \\ n_{2,1} & n_{2,2} & n_{2,3} & n_{4,4} \end{bmatrix}$$

Inserting $\boldsymbol{r}_k$ in Eq. (11.7):

$$\hat{\mathbf{H}}k = \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} \\ h_{2,1} & h_{2,2} & h_{2,3} \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix} \cdot \frac{1}{4}$$

$$+ \begin{bmatrix} n_{1,1} & n_{1,2} & n_{1,3} & n_{1,4} \\ n_{2,1} & n_{2,2} & n_{2,3} & n_{2,4} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix} \cdot \frac{1}{4}$$

$$\hat{\mathbf{H}}_k = \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} \\ h_{2,1} & h_{2,2} & h_{2,3} \end{bmatrix} \cdot \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

$$+\frac{1}{4} \cdot \begin{bmatrix} n_{1,1}-n_{1,2}+n_{1,3}+n_{1,4} & n_{1,1}+n_{1,2}-n_{1,3}+n_{1,4} & n_{1,1}+n_{1,2}+n_{1,3}-n_{1,4} \\ n_{2,1}-n_{2,2}+n_{2,3}+n_{2,4} & n_{2,1}+n_{2,2}-n_{2,3}+n_{2,4} & n_{2,1}+n_{2,2}+n_{2,3}-n_{2,4} \end{bmatrix}$$

$$\mathbf{H}_k = \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} \\ h_{2,1} & h_{2,2} & h_{2,3} \end{bmatrix} + \text{noise}$$

This result shows that the channel state has been estimated without interchannel interference. The noise statistics are not changed by this procedure [7, p. 214].

11.4.5.2 Transmitter channel state information (T-CSI)

For some MIMO modes including beamforming and spatial division multiplexing (SDM) discussed in Chapter 2, channel state information (CSI) represented by the channel matrix H is needed by the transmitter to predistort the emitted signals in order to obtain the MIMO advantage [2, 8]. We have just seen how the channel propagation matrix H is estimated in the receiver. There are two ways for the transmitter to get this information: implicit feedback and explicit feedback. Both ways are used for HT; VHT uses only explicit feedback. For implicit feedback, Fig. 11.20, the transmitter requests sounding frames, which contain a sequence of training symbols but no data, from the receiver. Through these signals, the transmitter can determine the channel state represented by the propagation matrix. For explicit feedback, Fig. 11.21, the receiver estimates the channel state as described in the previous section and sends this information to the transmitter. The problem with implicit feedback is that the resulting raw CSI is not the same as what would be measured by the

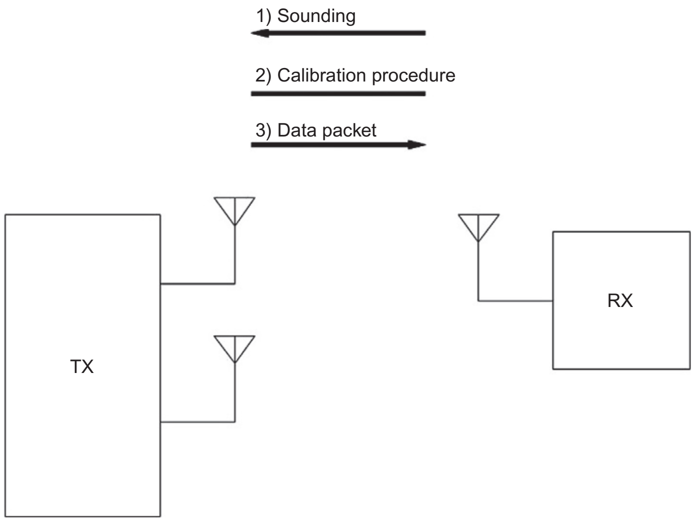


FIG. 11.20

Implicit feedback. *(After [9]).*

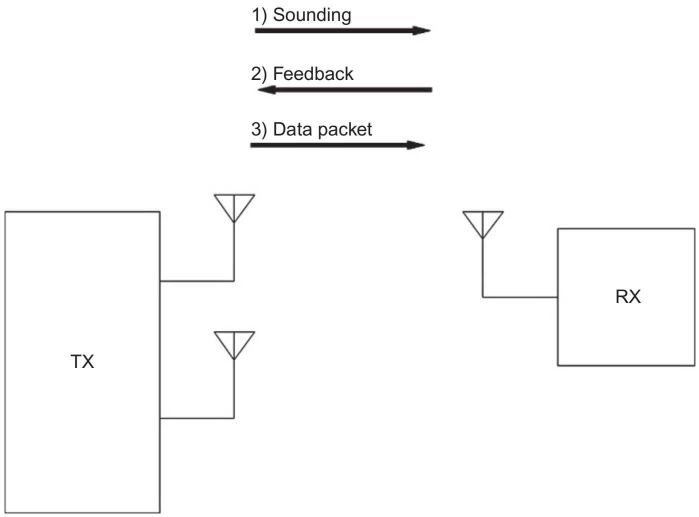


FIG. 11.21

Explicit feedback. *(After [9])*.

receiver. Although the channel between transmitting and receiving antennas is symmetrical, differences in the transmitting and receiving hardware of the terminals distort the amplitude and phases measured. In order to remove this distortion a calibration procedure is needed, which is described in [2] for HT. Since the receiver determines the CSI in explicit feedback, it is just what the transmitter needs for beamforming, but the defining information must be sent back to the transmitter. In order to reduce the amount of data to be transferred, the CSI is compressed into what is specified as the V matrix. This requires more back and forth transmissions, but the CSI is apt to be more accurate than when implicit feedback is used.

11.4.5.3 Multi-user MIMO (MU-MIMO)

While VHT has quantitative advantages over HT in bandwidth, modulation modes, number of spatial streams and consequently throughput, downlink multiuser MIMO (DL-MU-MIMO) is specified only for VHT. Fig. 11.22 shows an illustrative example. Two client receivers at 802.11 stations each receive on the downlink two independent data streams from the transmitting AP, all on the same carrier frequency and during the same time. Note that all receivers receive signals from all transmitting antennas. The data streams are separated using spatial multiplexing as explained in Chapter 2. The challenge here is to receive the required CSI from each of the client receivers. Explicit feedback is used, so the protocol has to coordinate the sending of sounding frames to each of the clients and reception of the CSI. The basis of this protocol is as follows [10]. The AP sends a null data packet announcement frame that notifies the relevant receiving stations that a null data sounding packet follows. The recipient stations will each process the sounding packet to estimate the channel

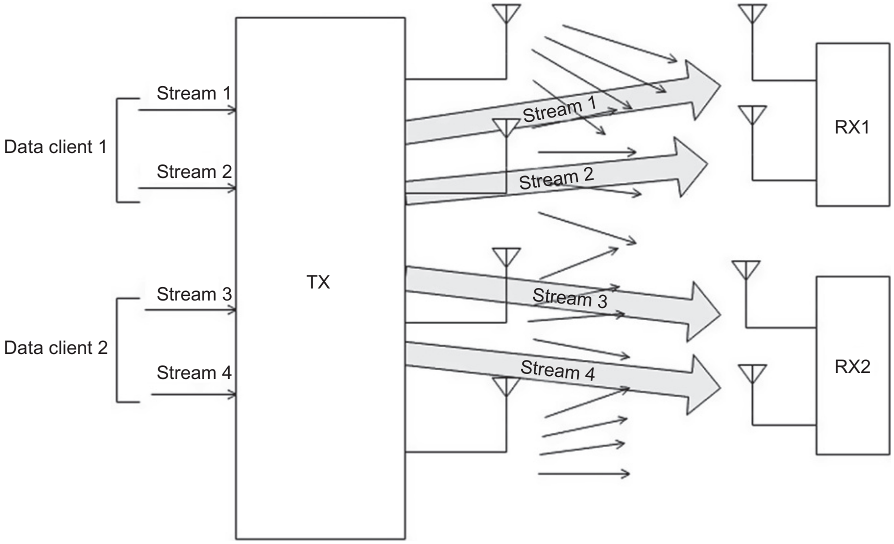


FIG. 11.22

Multi-user MIMO.

matrix and will send back to the AP, using polled access, their CSI report using the prescribed compressed format. The API uses the information it receives for the *Q* block of Fig. 11.19 to create the spatial multiplexing beams for the multiple users. Note that MU-MIMO works only in the downlink direction, from AP to client station, in the VHT specification.

11.4.6 IEEE 802.11ax

The successor to VHT in 802.11, draft amendment IEEE 802.11ax, has not yet been published as this book is being written. It is called high efficiency (HE) wireless. Its major features compared to VHT are shown in Table 11.5.

Table 11.5 802.11ax compared to VHT

	VHT	802.11ax
Bands	5 GHz	2.4 and 5 GHz
Bandwidth	20, 40, 80, 80 + 80, 160 MHz	20, 40, 80, 80 + 80, 160 MHz
FFT size	64, 128, 256, 512	256, 512, 1024, 2048
Highest modulation mode	256-QAM	1024-QAM
MIMO	DL MU-MIMO	DL and UL MU-MIMO
Access method	CSMA/CA	OFDMA
Data rates	433 MB/s, 80 MHz, 1 spatial stream	600.4 Mb/s (80 MHz, 1 spatial stream)

The comparison in the table doesn't give the whole picture. An impetus for 802.11ax is to provide high throughput in a dense Wi-Fi environment where there may be many APs in a relatively small area. To this end, new technologies were introduced to optimize average per-user throughput, instead of increasing the physical layer transmission rate and peak throughput under a single-user scenario [11]. Also, features are included for reduced power consumption. Technologies and features of HE 802.11 include:

- Orthogonal frequency division multiple access (OFDMA) PHY
- Uplink as well as downlink MIMO
- Spatial reuse
- Trigger frame
- Power saving with target wake time (TWT)
- Station-to-station (S2S) operation

OFDMA is the multiple access means used in LTE (long term evolution) cellular communication. In 802.11ax it substitutes frequency division multiplex for the collision avoidance with random stand-off used in earlier versions of 802.11. In addition, OFDMA allocates transmission bandwidth according to the data rate requirements of each station instead of using a common bandwidth for all, to a greater degree than is achieved with the multiple of 20 MHz bandwidths of HT and VHT 802.11 (amendments *n* and *ac*). It does this by allocating blocks of OFDM subchannels, called resource units (RU), to different stations in a BSS according to their needs. In order to provide a larger number of subchannels to allocate among stations, subcarrier spacing is decreased by four, from 312.5 to 78.125 kHz, increasing by four the number of subchannels per overall channel width. Correspondingly, the OFDM symbol length is increased by four to maintain orthogonality, leaving more room for inter-symbol interference compensation that is necessary particularly for longer reflections in outdoor environments.

IEEE 802.11ax supports uplink as well as downlink multi-user MIMO (MU-MIMO). Each of up to eight users can get up to four time-space streams, but the total number of streams is limited to eight. Combining OFDMA and MU-MIMO enables two-dimensional scheduling, frequency and spatial.

For multi-user simultaneous uplink transmissions frequency and time synchronization has to be exact. To this end, a new control frame, called a trigger frame, is introduced. The AP notifies in the trigger frame which stations are to respond and allows those stations to synchronize and to insure orthogonality between them. After receiving equal length PPDUs (PHY protocol data units) from the stations, the AP can send a common acknowledgement frame to all of them, thereby also reducing the acknowledgement overhead.

In dense WLAN deployments, spatial reuse is limited by overlapping independent BSSs. Stations associated with one AP, and the AP itself, can be heard by adjacent APs and their associated stations. This causes frequent transmission deferrals, as in the description above of the CSMA/CA access method, which of course reduces throughput. 802.11ax proposes to adjust the threshold power level for detecting interference on the channel, as well as controlling transmitter power output for minimum interference.

IEEE 802.11ax has new power saving schemes. A TWT (target wake time) mechanism allows stations to stay in power saving mode for a long time without listening for a beacon. Stations are scheduled to wake up at different times to minimize contention between them. Another power saving measure is for a station to identify a received packet as not in the same BSS, and to enter the "doze" state until the end of the frame. Operation mode indication (OMI) is the name of a mechanism for reducing power by changing PHY parameters like bandwidth and number of spatial streams.

S2S operations, including Wi-Fi Aware and Wi-Fi Direct, can increase contention in the vicinity of a BSS due to the lack of coordination between the transmissions. A quiet time period (QTP) is proposed during which only the S2S stations transmit frames and other non-participating stations remain quiet.

IEEE 802.11ax proposal includes operation on the 2.4 and 5 GHz band, as well as newly assigned channels at 6 GHz, and so can have complete backward compatibility when necessary.

11.4.7 IEEE 802.11ah

IEEE 802.11ah amendment specifies a new physical layer for sub 1 GHZ license-exempt bands. Designated Wi-Fi HaLow by the Wi-Fi Alliance and S1G by IEEE, it offers the possibility of extended range for WLAN although throughput is limited compared to the 2.4 and 5 GHz bands due to reduced bandwidth. Among the potential use cases are wireless sensor networks and utility meter monitoring. Modulation is based on OFDM, but the PHY is not compatible with 2.4 and 5 GHz systems [12].

The physical layer (PHY) of 802.11ah is based on VHT of IEEE 802.11-2016 but with a sampling frequency reduced by 1/10 to give bandwidths of 2, 4, 8, and 16 MHz on ISM frequencies below 1 GHz [13]. In addition, 1 MHz bandwidth operation is defined for increased sensitivity and consequently range, but at reduced data rates. Sub-carrier separation is 31.25 kHz, 1/10 that of VHT, HT and 802.11a. Cyclic prefix length may be 4 or 8 μs. Modulation schemes are BPSK, QPSK, 16-QAM, 64-QAM, and 256-QAM, with coding rates of ½ to 5/6, as for VHT. Up to four data streams for SU-MIMO (single-user MIMO) and MU-MIMO (multi-user MIMO) are specified with a maximum of three streams per user for MU-MIMO. Maximum data rates are between 150 kbps and 234 Mbps, according to bandwidth, modulation level, coding rate, cyclic prefix length and number of spatial streams. At 2 MHz bandwidth, one spatial stream, 256-QAM modulation and coding rate of 3/4, raw data rate is 7.8 Mbps [14]. Operating frequency bands are 902 to 928 MHz in the United States and 863 to 868 MHz in Europe.

The MAC layer of 802.11ah has special features to meet the particular requirements of sub 1 GHz applications. With its increased range and use in large multinode networks, a larger address space is accommodated. A 2.4 and 5 GHz 802.11 network supports up to 2007 network addresses (association identifiers—AID) whereas 802.11ah can assign up to 8191 addresses. With a larger number of nodes, medium access collisions become more likely. A restricted access window (RAW) mechanism divides the network devices into groups and assigns specific access periods (RAW) for each group such that contention in a group is significantly less than if all devices had access to the medium at all times. The RAW mechanism is also used to reduce energy consumption. Since a node knows when it can access the medium, it can plan its sleep intervals accordingly. The node will wake up at a scheduled time when the AP sends a beacon indicating which nodes have messages waiting for them. A node expecting a message, or having data to send, will then wake up during its RAW to access the channel. Variations of the access and sleep mechanism are explained in [14] and in the 802.11ah amendment [15].

11.5 IEEE 802.11 Wi-Fi certified location

The Wi-Fi Alliance has announced that Wi-Fi includes advanced capabilities to bring location determination indoors [16]. The location service is based on the fine timing measurement (FTM) protocol in IEEE 802.11-2016, which can deliver meter-level accuracy for indoor device location data. FTM calculates an accurate distance from a mobile device to an AP, which is configured with its exact location, including geospatial coordinates (latitude, longitude, and altitude) and a civic address. This can give precise location determination, even in multilevel structures. More information on location is given in Chapter 14.

11.6 Wi-Fi security

Security in Wi-Fi networks, as specified in IEEE 802.11, has gone through major enhancements since the originally defined wireless equivalent privacy (WEP). Since 2006, all Wi-Fi devices certified by the Wi-Fi Alliance implement WPA2 [17]. In 2017 the Wi-Fi Alliance introduced Wi-Fi Certified WPA3 as a new generation of Wi-Fi security with new capabilities to enhance Wi-Fi protection in personal and enterprise networks. We discuss here the evolution of 802.11 security from WEP since understanding the basic architecture will help learning the more complicated and much more secure arrangement that has been in force for over 20 years.

First, let’s examine some basic security concepts, shown in Fig. 11.23.

Confidentiality is keeping the data secret from the unintended listeners on the network. It is maintained by *encryption*, where a secret key known only to the two sides maps the message (plaintext) to a form unintelligible to a third party (encrypted text). In Fig. 11.23, Eve (the eavesdropper) is monitoring the communication medium between Alice (side A) and Bob (side B), but is unable to decipher the messages between them.

Integrity is insuring that the received data is the data that was actually sent, and was not modified or replaced in transit. It is implemented using a *one-way hash*

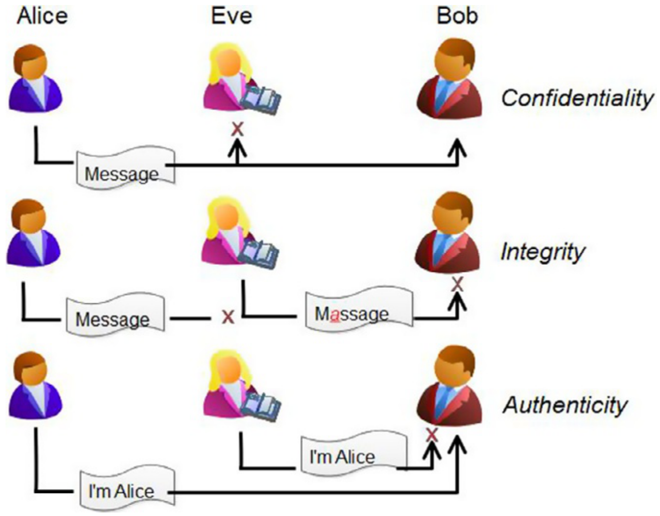


FIG. 11.23

Security concepts.

function (similar purpose to a CRC -cyclic redundancy check). A cryptographic hash function is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (**cryptographic**) **hash value**, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded is often called the *message*. Eve has intercepted the message in the (second row in Fig. 11.23) and changed the first "e" to "a". Although "Massage" has a valid meaning, Bob knows that the message he received was modified, due to integrity protection.

Authenticity is ascertaining the identity of the end point to ensure that the end point is the intended entity to communicate with. Use of a digital signature with challenge-response schemes prove authenticity. These schemes involve public key cryptography (PKC) (asymmetric keys). Referring to row 3 of Fig. 11.23, when setting up a communication link or associating with a network Bob needs to be sure the intended opposite terminal, Alice, is who he thinks it is, and not an imposter (Eve). Often authentication is performed for one side of the link only, but for higher security each side will authenticate the other.

Two more security concepts are *non-repudiation* and *service reliability* [18]. *Non-repudiation* is the receiver's ability to prove that the sender did in fact send a given message (bank client cannot deny that she did not withdraw money from her account). PKC, digital signature, or time stamping, can prevent such fraud. *Service reliability* is the ability to protect the communication session against denial of service attacks. These are difficult to combat. Countermeasures include reservation of redundant resources, identification of the attack source and selective blocking.

Table 11.6 Security threats and countermeasures

Threat	Category	Countermeasure
Denial of service	Service reliability	Multiple resources, source tracing
Eavesdropping	Confidentiality	Encryption
Man-in-the-middle	Authentication, confidentiality	Authentication, encryption
Masquerading	Authentication	Authentication
Message modification	Integrity	Hash function
Message replay	Authentication	Time stamp, session numbering
Traffic analysis	Confidentiality	Steganography

Table 11.6 lists some threats and their categories, and countermeasures.

The word steganography, in the last row under **Countermeasure**, means *the science of hiding information*. It involves hiding the fact that a message is sent—for example hiding a message in insignificant pixels of a JPEG image, or hiding one message inside another (i.e., in a WEB page) [18].

The principles of symmetric and asymmetric (public) key cryptography are shown in Fig. 11.24. For symmetric key cryptography (SKC), both terminals, Alice and Bob, share a common password, or secret key. In the simplified example in Fig. 11.24, that secret key is XOR'ed with the plaintext at Alice's terminal, creating the ciphertext. Bob performs exactly the same process, XOR'ing the secret key with ciphertext, which produces the original plaintext. There are other algorithms for using a common key to encrypt and decrypt a message. For all of them and for the asymmetric key cryptography as well, it is preferable that the security of the cryptosystem resides in the secrecy of the keys rather than with the supposed secrecy of the crypto algorithm. This means that it should be virtually impossible to decrypt a ciphertext to plaintext if the decryption key is unknown, even if the full details of the encryption and decryption algorithms are known.

The major problem with SKC is dissemination of the keys. Both sides use the same key, so how is the key sent from the key originating side to others that need it? If it is sent over a communications medium it is susceptible to interception. In a small place like an office or a home, it can be transferred personally but for large area distribution this is not an option. PKC gets around this problem.

PKC (Fig. 11.24B) is an asymmetric mechanism. Two keys are created by an appropriate key generation algorithm, for example RSA, (Rivest-Shamir-Adleman protocol) [18]. Either key can decrypt a ciphertext created with the other. The public encryption key can be openly distributed. The private decryption key is secret, and is not disseminated. The public/private keys are a pair. Asymmetric algorithms are slow—not practical for lots of data. They are used to distribute secret symmetrical keys, which are then used in a symmetric algorithm for encrypting/decrypting

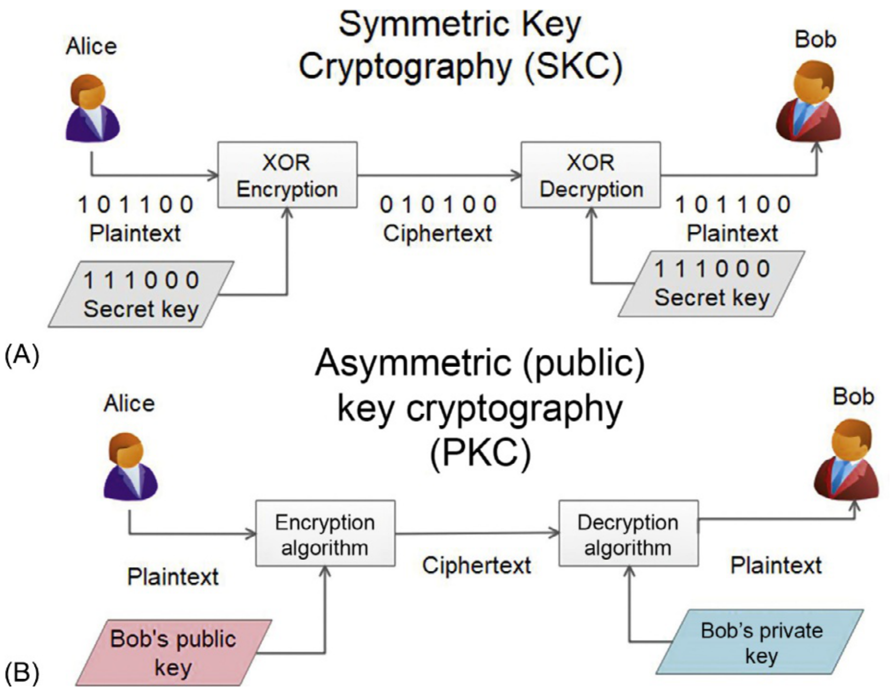


FIG. 11.24

Symmetric and asymmetric key cryptography. (A) Symmetric key cryptography (SKC).
(B) Asymmetric (Public) key cryptography (PKC).

messages or streams of data. In Fig. 11.24B, Alice encodes a plaintext using Bob's public key. Only Bob can decode it, because only he has the private key. Eve, from Fig. 11.23 *Confidentiality*, can eavesdrop on the message, but she can't decode it, even if she has Bob's public key. As mentioned, Alice can send a symmetric key to Bob through PKC which can be then be used to efficiently communicate messages between them.

A random number sent back and forth is used in an authentication process. The authenticator (Bob) sends a random number in the clear to Alice. Alice encrypts the number with her private key which serves as a *digital signature*. Bob decodes the message with Alice's public key. If the message (random number) is correct, Bob knows it can only be from Alice. This message itself is not secure, as Eve can decode it also if she has Alice's public key. But it serves its purpose of authenticating that Alice is the origin of the message.

PKC is also used for non-repudiation, Bob sends a message encrypted with Alice's public key (which can contain for example access to a large sum of money) to Alice. When the message is acknowledged, by withdrawing money from a bank account for example, Alice can't say she didn't receive it (the message or the money) since only she could have decrypted the message using her private key.

Of course it is very important that the owner of a public key be verifiable. The secure distribution of public keys is done utilizing specific certificates. Secure public key management is accomplished with a public key infrastructure (PKI), which contains catalogs with public keys and their owners, as well as such information as the validity period of the keys. A certificate for public keys is a document that confirms the connection between the public key and the key-owner. Each certificate includes the name of the authority that issued it, the name of the entity to which the certificate was issued, the entity's public key, and time stamps that indicate the certificate's expiration date.

11.6.1 WEP

Now that the basics are understood, we move on to discuss confidentiality in 802.11. The original 802.11 security architecture and protocol is called WEP. It aimed to give 802.11 the same security as traditional wired (Ethernet) networks. Here's how it works, following the circled numbers in Fig. 11.25.

(1) Calculate ICV (Integrity Check Value) using CRC-32 algorithm.
(2) Select one of 4 pre-established secret keys.
(3) Create 24 bit IV (Initialization Vector) and concatenate it with the key—used to insure a different key sequence for each message.
(4) Use the *seed* (2+3) in an encryption algorithm (Pseudo Random Noise Generator—type RC4) to get keystream which is XOR'd with ICV plus plaintext, giving ciphertext.
(5) Concatenate the ciphertext to a plaintext header containing the three byte IV plus a one byte key ID indicating which of 4 keys used and the 802.11 header.

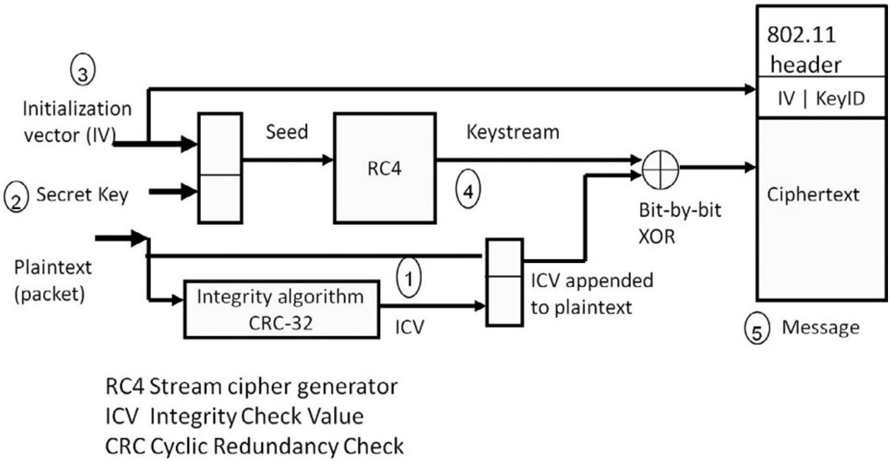

3
Initialization vector (IV)
2 Secret Key
Plaintext (packet)
Seed
RC4
Keystream
4
Bit-by-bit XOR
Integrity algorithm CRC-32
1
ICV
ICV appended to plaintext
802.11 header
IV | KeyID
Ciphertext
5 Message
RC4 Stream cipher generator
ICV Integrity Check Value
CRC Cyclic Redundancy Check

FIG. 11.25

Wireless equivalent privacy (WEP).

WEP was found to have multiple weaknesses that made it imperative to revamp the security architecture of 802.11.

(1) IV is transmitted in the clear so attacker knows 3 bytes (24 bits) of the 64 or 128 bit seed—40 (or 104) bits of the key usually don't change. This makes the seed a weak key. By accumulating enough packets, the secret key can be found.
(2) Additionally, a short IV and no rules on how it is created means that the seed, thus the keystream, will be repeated after a relatively short time (hours). Two encrypted packets with common keys can be unraveled if one plaintext is known or can be guessed. Reuse of the seed allows logical cancelling out of the keystream to expose the message.
(3) The integrity algorithm is not secure (CRC-32 uses no key) and allows substitution or modification of a data packet without being detected.
(4) The 802.11 header is not encrypted—packets can be maliciously diverted without detection by changing the destination address.
(5) There is no protection against replay attacks.

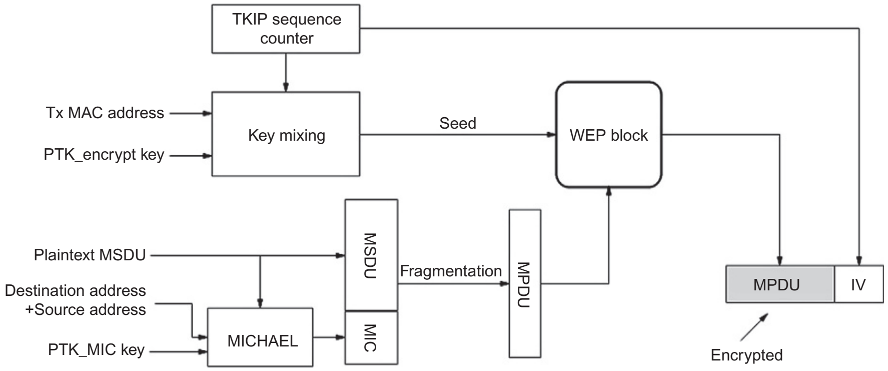
In order to distinguish between levels of security in Wi-Fi implementations, IEEE 802.11 defined two classes of security algorithms: algorithms for creating and using a *robust security network association* (RSNA) which includes TKIP and CCMP (within WPA2), and pre-RSNA of which WEP is a part. These terms are explained below.

11.6.2 WPA

The second phase of Wi-Fi security was based on existing WEP hardware with numerous changes incorporated in firmware. Called Wi-Fi protected access (WPA), it was an interim solution introduced by the Wi-Fi Alliance in anticipation of completion of amendment IEEE 802.11i and implementation of WPA2. WPA, shown in Fig. 11.26, allowed upgrading the security of existing Wi-Fi devices through firmware changes while retaining the equipment's WEP hardware. The temporal key integrity protocol (TKIP) was adopted by the Wi-Fi alliance as a Wi-Fi security standard for confidentiality and improved integrity. MICHAEL was new protocol for MIC (Message Integrity Check) with higher reliability and relatively simple computations.

Here are some WPA/TKIP features and benefits:

(1) May use 802.1X authentication and key-establishment (enterprise deployments).
(2) Creates PTK (pair-wise transient keys) per session (station connection to AP) based on a secret key plus access point (AP) and client station (STA) MAC addresses and nonces (one time random numbers) to insure one-time key sequences, and key mixing functions to reduce exposure of the master key (instead of the simple concatenation used in WEP). In Fig. 11.27, a shared secret, which may be a password or an authentication key obtained through an



MSDU: MAC Service Data Unit
MPDU: MAC Protocol Data Unit
MIC: Message Integrity Check
IV: Initialization Vector
PTK: Pairwise Transient Keys

FIG. 11.26

WPA with temporal key integrity protocol (TKIP).

authentication server over the network, is transformed to a pair-wise master key (PMK) of 256 bits. The PTK is formed using a pseudo-random function acting on the PMK, session terminal addresses and nonces. It contains up to four keys: encryption and integrity keys for the STA/AP data flow and two keys for communication with an out-of-local-network server based on the EAPoL (Extensible Authentication Protocol over LAN) used by enterprise networks.

(3) Initialization vector (IV) increased to 56 bits (of which 48 used) to insure stronger keys.

(4) Specifies incrementation of IV for each packet—no repetition. Protects against replay.

(5) MICHAEL integrity check much safer than CRC-32 (which is still used within WEP hardware). MIC (message integrity check) computation includes packet destination and source addresses to protect against redirection attacks.

While, as described above, TKIP is an RSNA algorithm, its use, as is the use of WEP, is deprecated [2].

11.6.3 WPA2

The outstanding feature of WPA2 is the use of the Advanced Encryption Standard AES. Counter mode cipher block chaining message authentication code protocol (CCMP) provides the highest level of confidentiality, integrity and replay protection available in the 802.11 standard [19]. WPA2 is shown in Fig. 11.28. It uses essentially the same key-establishment process and key hierarchy architecture as WPA (Fig. 11.26). An exception is that the same key is used for confidentiality and

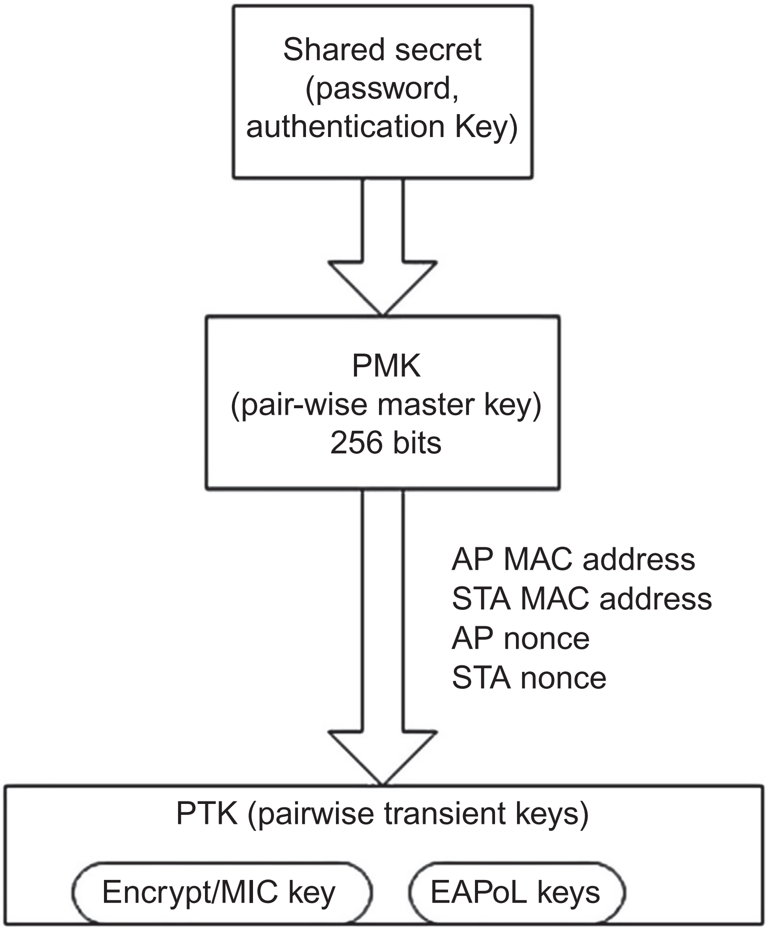
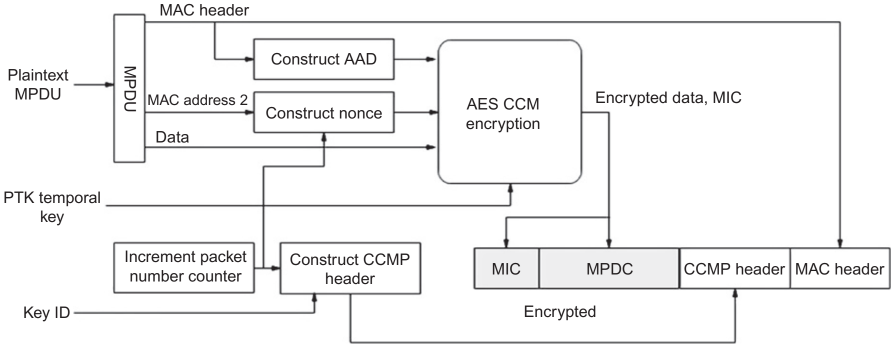


FIG. 11.27

Transient key formation.

integrity; there are no separate encryption and MIC keys. In contrast to RC4 of WEP which is a stream cipher, AES is a block cipher, although it does use a key stream to encrypt each block. CCMP achieves confidentiality in counter mode by taking each of consecutive 128 bit blocks of packet plaintext and XORing it with a keystream formed from encryption of a counter, incremented for each block, using the temporal key. To create the MIC used to insure integrity, cipher block chaining message mode is used. Each block is XOR'ed with the ciphertext of the previous block and encrypted with the temporal key. The process is started with an initializing vector (IV) created with a counter that is incremented for each packet. MIC is 64 bits of the last ciphertext block. Because of the chaining of blocks, a change in one or more bits of the message will cause a large difference between the MIC sent with the packet and the MIC constructed at the receiver.



AAD: additional authentication data - non-changing header fields
MAC address 2: Source MAC address
AES CCM: AES counter mode
CCMP: CCM protocol
PTK pairwise transient keys

FIG. 11.28

WPA2.

Fig. 11.28 shows the main blocks of WPA2. Note that in addition to the message data, fields of the MPDU header, notably the address fields and QoS field, formed in AAD (additional authentication data), are encrypted. The packet number counter, which is incremented on each packet is used in composing a nonce, which never repeats itself in a session. The AES CCM (Counter mode with CBC-MAC) block includes both the counter and cipher block chaining message modes for confidentiality and integrity. The CCMP header and the MAC header which are transmitted in the clear, let the receiver compose the IV which it needs to check integrity and to make the counter used for decryption. The fact that addresses are encrypted from AAD assures that diversion of packets caused by hostile change of packet header addresses can be detected in the receiver.

WPA2 gives similar protection as WPA with TKIP. It gives superior security, however, by using the AES security standard, which is stronger than RC4 for encryption and gives better integrity protection than MICHAEL used in WPA.

The Wi-Fi Alliance announced that new capabilities under WPA3 are available from 2018. Among them are protection of users who choose weak passwords, simplification of the configuration process for devices with limited display interfaces such as sensors and IoT modules, improved privacy on open networks, and stronger security for government, defense and industrial networks through new protocols using a 192 bit security suite [20].

11.7 Summary

The technical capabilities of WLANs have been updated continuously since the emergence of IEEE standard 802.11 in the last decade of the 20th century. In this chapter we reviewed 802.11 from the point of view of network architecture, MAC and the physical layer (PHY). Evolution of the physical layer was described from the early infra-red, frequency hopping and DSSS links with throughputs of several megabits per second up to the techniques that support hundredfold increases in data rates through advanced modulation based on OFDM, multiple element antenna arrays (MIMO) and multiplication of bandwidth on 5 GHz and millimeter wave bands. Expansion of the 802.11 capabilities to the below 1 GHz ISM bands was described. IEEE 802.11 security methods were explained, from the early WEP through Wi-Fi protected access (WPA and WPA2).

References

[1] Wi-Fi Alliance, https:/www.wi-fi.org/who-we-are, 2018. Accessed 24 October 2018.
[2] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11™-2016, IEEE Computer Society, 2016.
[3] 802.11ac: The Fifth Generation of Wi-Fi, Technical White Paper. Cisco, 2017.
[4] 802.11ac In-Depth, White Paper. Aruba Networks, 2014.
[5] T. Paul, T. Ogunfunmi, Wireless LAN comes of age: understanding the IEEE 802.11n amendment, IEEE Circ. Syst. Mag. 8 (1) (First Quarter) (2008).
[6] R.P.F. Hoefel, IEEE 802.11n: on performance of channel estimation schemes over OFDM MIMO spatially-correlated frequency selective fading TGn channels, in: XXX SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES—SBrT'12, 13-16 DE SETEMBRO DE 2012, BRASÍLIA, DF, 2012.
[7] A. Sibille, C. Oestges, A. Zanella, MIMO From Theory to Implementation, Elsevier, 2011.
[8] 802.11ac In Depth, Aruba Networks, www.arubanetworks.com, White Paper2014. Accessed 24 October 2018.
[9] R.U. Nabar, MIMO in WiFi systems, in: Smart Antenna Workshop, August 1, 2014. https://web.stanford.edu/∼apaulraj/workshop70/pdf/MIMO_WiFi_Nabar.pdf. Accessed 24 October 2018.
[10] O. Bejarano, E.W. Knightly, IEEE 802.11ac: from channelization to multi-user MIMO, IEEE Commun. Mag. (2013).
[11] D.-j. Deng, Y.-p. Lin, X. Yang, J. Zhu, Y.-b. Li, J. Luo, K.-c. Chen, IEEE 802. 11ax: Highly Efficient WLANs for Intelligent Information Infrastructure, IEEE Commun. Mag. 55 (12) (2017) 52–59, https://doi.org/10.1109/MCOM.2017.1700285.
[12] W. Sun, M. Choi, S. Choi, IEEE 802.11ah: a long range 802.11 WLAN at sub 1 GHz, J. ICT Stand. 1 (2013) 83–108, https://doi.org/10.13052/jicts2245-800X.125_c. River Publishers.
[13] P.C. Jain, S. Taneeru, Performance evaluation of IEEE 802.11ah protocol in wireless area network, in: 2016 Int. Conf. Micro-Electronics Telecommun. Eng, 2016, pp. 578–583.
[14] H. Wang, A.O. Fapojuwo, A survey of enabling technologies of low power and long range machine-to-machine communications, IEEE Commun. Surv. Tutor. 19 (4) Fourth Quarter. (2017) 2621–2639.
[15] IEEE Std 802.11ah-2016, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation, IEEE Computer Society, 2016.

[16] Wi-Fi Certified Location. Indoor location over Wi-Fi, Wi-Fi Alliance, 2017.

[17] Wi-Fi Security, Wi-Fi-Alliance, https://www.wi-fi.org/discover-wi-fi/security, 2018. Accessed 24 October 2018.

[18] P. Chandra, Bulletproof Wireless Security, Elsevier, 2005.

[19] K. Benton, The Evolution of 802.11 Wireless Security, INF 795, UNLV Informatics-Spring, 2010.

[20] Wi-Fi Alliance® Introduces Security Enhancements, https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements (retrieved 17 July 2018), 2018.

This page intentionally left blank