Chapter 2
Fundamentals of ZigBee and WiFi

This chapter focuses on the fundamentals and technical characteristics which will bring up significant effects on the interference and solutions. Since it is much easier for ZigBee to be interfered with by WiFi, this chapter will discuss ZigBee more.

2.1 ZigBee

Based on IEEE 802.15.4, ZigBee is currently the de facto standard for wireless sensor networks (WSNs) [1, 2]. It is designed for ZigBee focuses on the field of low-power, low-cost, and low-bit rate communications, which has been widely used in sensor networks, cyber-physical systems [4], and smart buildings. We will first introduce the basic conceptions in ZigBee networks and then introduce some important mechanisms in ZigBee specification. These mechanisms will be exploited for handling interference from WiFi in the following chapters.

2.1.1 Overview of ZigBee

ZigBee is a specification that is built on top of the IEEE 802.15.4 short-range communications standard [3]. The name ZigBee comes from the fact that bees can dance to pass messages to each other, also in a multihop fashion. ZigBee covers the upper layers of the protocol stack, while 802.15.4 is in charge of MAC and PHY layers.

ZigBee is intended for low-throughput, low-power, low-cost applications. For this reason, it is much simpler than other protocols such as WiFi (IEEE 802.11). It has support for mesh topologies, which means that ZigBee devices relay messages for each other through multiple wireless hops.

G. Shi and K. Li, *Signal Interference in WiFi and ZigBee Networks*,
Wireless Networks, DOI 10.1007/978-3-319-47806-7_2

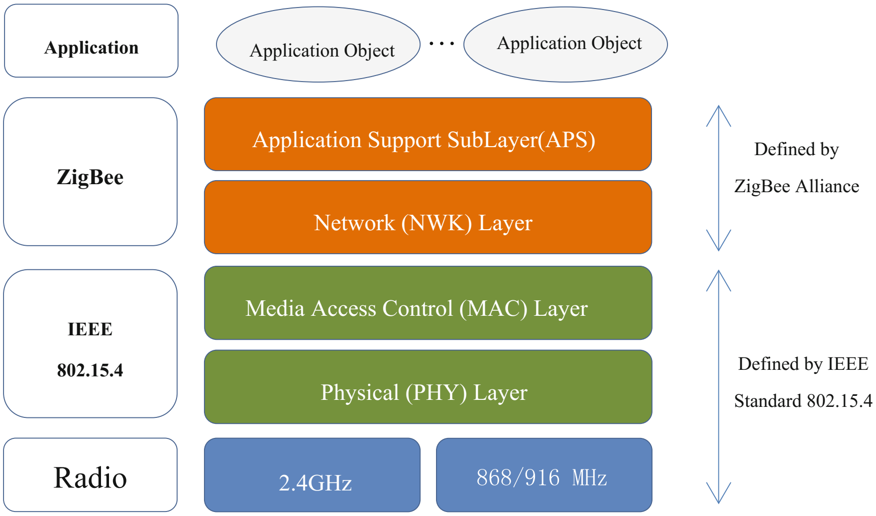


Fig. 2.1 ZigBee protocol stack architecture

Figure 2.1 depicts ZigBee protocol stack, which consists of four layers, viz., PHY, MAC, network and application layer. The first two are covered in IEEE 802.15.4 standard and the latter two are covered in documents published by ZigBee alliance. The first two are the critical factors for handling the interference from WiFi. Therefore, the following content focuses on MAC and PHY layer.

There are three network topologies in ZigBee. Besides the star topology, the ZigBee network layer also supports more complex topologies like the tree and the mesh, shown in the image below. Among the functionalities provided by the network layer are multihop routing, route discovery and maintenance, security and joining/leaving a network, with consequent short (16-bit) address assignment to newly joined devices.

There are three main players in a ZigBee network:

- **Coordinator**: is the most powerful device. There is a single coordinator in each network. It is the node that creates the network and the other nodes simply join in. Quite often, this is the sink of the WSN, which gathers all the data that is transmitted. One of the coordinator tasks is to assign short addresses.
- **Router**: are intermediate devices. They can relay packets for other nodes. They join a network that already exists and then announce it using beacons. Therefore, they can have "children" nodes that join the network by establishing communication with the router.
- **End Devices**: these are the simplest devices. They cannot forward packets nor have children that depend on them and, quite often, they enter a sleep mode in order to save energy. Figure 2.2 illustrates the players in three different network topologies which are Star, Tree and Mesh, respectively.

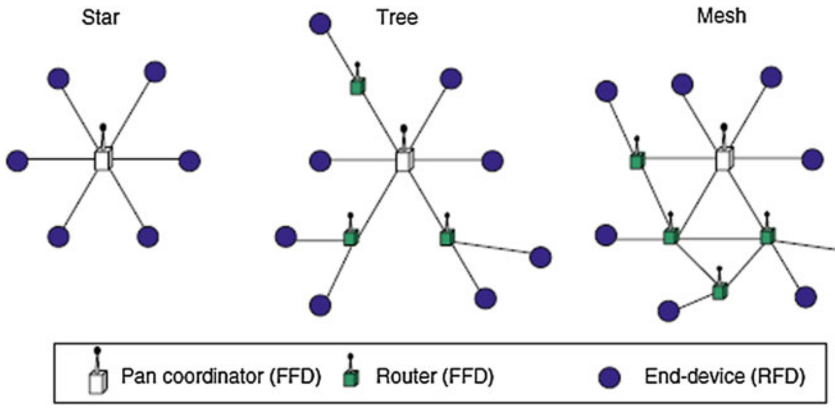


Fig. 2.2 Network topology

There are two types of data transfer transactions in ZigBee networks.

- The first one is the data transfer between a coordinator and a device, in which a device transmits the data to or receives the data from a coordinator. This transaction is used in star topology.
- The second transaction is the data transfer between two peer devices. In a peer-to-peer topology, data is exchanged between any two devices on the network; consequently all three transactions are used in this topology.

2.1.2 IEEE 802.15.4 Physical Layer

Since the interference effect on ZigBee is more prominent than that on WiFi, many works search solutions from physical layer. Thus, in this subsection, we will provide the key designs in ZigBee physical layer.

The PHY provides an interface between the MAC sublayer and the physical radio channel, via the RF firmware and the RF hardware. Besides radio on/off operation, the physical layer includes functionalities of channel selection, link quality estimation, energy detection (ED) measurement, and clear channel assessment (CCA).

2.1.2.1 Channel Assignment and Switching

The IEEE 802.15.4 PHY layer supports three frequency bands: a 2450 MHz band (with 16 channels), a 915 MHz band (with 10 channels), and an 868 MHz band (1 channel), all using the direct sequence spread spectrum (DSSS) access mode. In these three frequency bands, only 2.4 GHz band overlaps with that of WiFi. Thus, we only introduce the protocol defined for operating in the 2.4 GHz ISM band.

The frequency band for IEEE 802.15.4 in 2.4 GHz ranges from 2400 to 2483.5 MHz. Furthermore, these spectrums are subdivided into channels with a center frequency and bandwidth. It is well known that the IEEE 802.15.4 standard defines 16 channels within this band, each 2 MHz wide with 3 MHz interchannel gap-bands (see Fig. 2.3). The center frequency of these channels can be calculated as follows:

$$F_c = 2405 + 5(k - 11) \text{ in megahertz, for } \quad k = 11, 12, \ldots, 26$$

where F_c and k are the center frequency and channel number, respectively. The detailed frequency ranges and the center frequencies of every channel are listed in Table 2.1.

Although these channels are nonoverlapping in frequency band, a channel is not orthogonal to all the other channels. Some results show that concurrent transmissions on adjacent channels will result in interference [4]. This is due to energy spill over and imperfect filtering. In comparison, the two channel away interference will

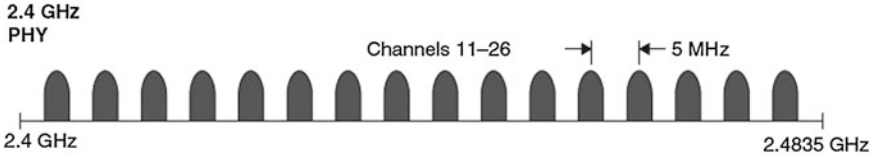


Fig. 2.3 Frequency and channel for ZigBee in 2.4 GHz

Table 2.1 GHz PHY channel frequencies

Channel ID	Lower frequency	Center frequency	Upper frequency
11	2404	2405	2406
12	2409	2410	2411
13	2414	2415	2416
14	2419	2420	2421
15	2424	2425	2426
16	2429	2430	2431
17	2434	2435	2436
18	2439	2440	2441
19	2444	2445	2446
20	2449	2450	2451
21	2454	2455	2456
22	2459	2460	2461
23	2464	2465	2466
24	2469	2470	2471
25	2474	2475	2476
26	2479	2480	2481

be smaller. Therefore, the 16 channels can however be divided into two sets of orthogonal 3 channels, with each containing 8 channels—(11, 13,…, 25) and (12, 14,…, 26). *More interference models and experiments will be discussed in* Chap. 3.

Generally, the working channel of ZigBee network is predefined. But all devices can trigger scanning operations for dynamic channel selection. Channels are scanned in order from the lowest channel number to the highest if the scanning is for channel selection. The scanning process will provide the energy level feedback and the nodes will select the quietest one for their new working channel.

The channel switching operation, via channel register writing, can only happen when the radio is in IDLE state and will induce cost of time. In another word, the channel switching will not come into effect immediately if the request is sent out when the radio is not in IDLE state. The procedures for channel switching roughly include radio status change, channel number register writing, and PLL (phase-locked loop) calibrating. In literature [5], the experiments with Micaz mots show that the time to switch between channels and wait until the frequency synthesizer stabilizes is roughly equal to the time to transmit one packet with 32 bytes. The widely used CC2420 transceiver has channel switching times of only 300 microseconds. More recent radios have dramatically reduced the time it takes to switch channels. For example, the newer Chipcon CC2500 2.4 GHz radio takes only 90 μs to switch channel. But this time is measured when the radio has been calibrated at startup [6]. Therefore changing to another frequency channel dynamically and frequently has the potential to become a damper on system performance.

2.1.2.2 Energy Detection and CCA

The receiver ED measurement in IEEE 802.15.4 is intended for use by a network layer as part of channel selection algorithm. It is an estimate of the received signal power within the bandwidth of an IEEE 802.15.4 channel. No attempt is made to identify or decode signals on the channel. The ED time should be equal to 8 symbol periods. Generally, the ED value is calculated by averaging RSSI values over eight symbols (128 μs).

The ED result shows the power level of received signal including interference and noise. The ZigBee network node could use this information to infer the interference condition so that a better channel could be selected.

The ED report defined in the standard is an 8-bit integer ranging from 0x00 to 0xff. The minimum ED value (0) shall indicate received power less than 10 dB above the specified receiver sensitivity. The range of received power spanned by the ED values shall be at least 40 dB. Within this range, the mapping from the received power in decibels to ED values shall be linear with an accuracy of ±6 dB.

CCA, partially based on ED, is an essential ingredient in wireless networks employing channel sensing as part of their medium access mechanism. CCA is implemented at the PHY layer from the view of protocol stack, but it is often used by MAC layer. When the MAC layer receives a packet to transmit, it instructs the PHY to do CCA as described in the following MAC section.

The standard specifies that the CCA duration shall be 8 symbol periods or 128 μs. The CCA is performed according to at least one of the following three methods:

- Energy above threshold. CCA shall report a busy medium upon detecting any energy above the ED threshold.
- CS only. CCA shall report a busy medium only upon the detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4. This signal may be above or below the ED threshold.
- Carrier sense with energy above threshold. CCA shall report a busy medium only upon the detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4 with energy above the ED threshold.

Take CC2420, a popular ZigBee-compliant RF transceiver, as an example, it has a built-in RSSI (received signal strength indicator) which has the likewise effect of ED and provides a digital value that can be read from the 8 bit, signed 2's complement RSSI.RSSI_VAL register. As defined in IEEE 802.15.4 standard, the RSSI value is always averaged over 8 symbol periods (128 μs). The RSSI register value RSSI.RSSI_VAL can be referred to the power P at the RF pins by using the following equations:

$$\mathrm{P = RSSI\_VAL\ +\ RSSI\_OFFSET\ [dBm]}$$

where the RSSI_OFFSET is found empirically during system development from the front-end gain. RSSI_OFFSET is approximately −45. For example, while reading a value of −20 from the RSSI register, the RF input power is approximately −65 dBm.

2.1.2.3 PHY Protocol Data Units

The PHY protocol data unit is called PPDU, which encloses the MAC frames passed to the PHY as the PHY service data unit (PSDU).

The schematic view of PPDU is illustrated in Fig. 2.4. Each PPDU packet consists of the following basic components:

- SHR, which allows a receiving device to synchronize and lock into the bit stream.
- PHR, which contains frame length information.
- PSDU, a variable length payload, which carries the MAC sublayer frame.

The PPDU packet structure is illustrated in Fig. 2.5. PPDU begins with a preamble sequence which is composed of 32 zeros (all bytes set to 0x00) and is used for chip and symbol synchronization at receiver part of transceiver. Start of frame delimiter (SFD) follows the preamble and is 8 bit field segregate between

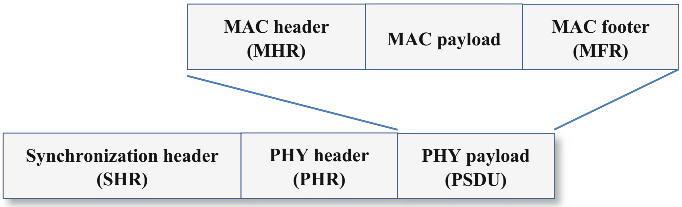


Fig. 2.4 Schematic view of the PPDU

preamble and actual physical layer data. The SFD indicates the end of the SHR and the start of the packet data and is set to 0x7A. At the receiver side, an 802.15.4 radio synchronizes to incoming zero-symbols and searches for the SFD sequence to receive incoming packets. The PHR includes a 1-byte length field that describes the number of bytes in the packet's payload, including the 2-byte CRC. PSDU field carries PHY packet but the payload is transferred from MAC sublayer. Its length is variable.

From Fig. 2.5 we can see that ZigBee PPDU Frame consists of SHR (Preamble 4 bytes, SFD 1 byte) + PHR (Frame length 1 bit, Reserved 1 bit) + PHY Payload (PSDU variable length). Therefore, *the maximum packet size in IEEE 802.15.4 is 133 bytes*, including all the headers. Note that while the IEEE 802.15.4 specification mandates a 4-byte preamble, some radios such as the CC2420 allow the user to set the length of the transmitted preamble up to 17 bytes.

2.1.2.4 Modulation and Spreading

Any information to be transmitted via ZigBee must be modulated firstly. To improve signal-to-noise Ratio (SNR) of received signals at the receiver, ZigBee employs direct sequence spread spectrum (DSSS) that uses a digital spreading function representing pseudorandom noise (PN) chip sequences [1]. A bit in a PN-code is called a *chip* and thus a PN-code can be also called a *chip sequence*. In reality, each symbol is presented by using predefined chip sequences.

At the sender side before the bit sequences are being modulated and transmitted through the antenna, there is an additional process to chop the sequences into symbols and replace each symbol with the corresponding chip sequence, which is modulated to baseband transmission waveform and is ultimately transmitted over the air.

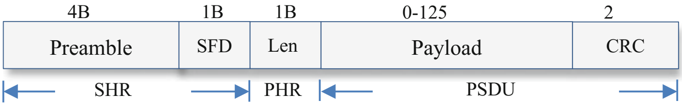


Fig. 2.5 802.15.4 PHY protocol data units format

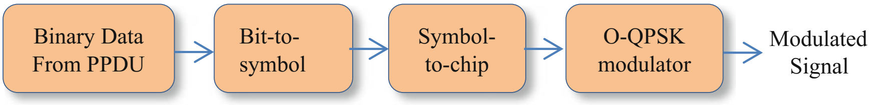


Fig. 2.6 Modulation and spreading functions for the O-QPSK PHYs

To do this, outgoing bytes are divided into two 4-bit symbols, the 4 least significant bits (LSB) and the 4 most significant bits (MSB). Each 4-bit symbol will be spread to a specified 32-bit long PN sequence. IEEE 802.15.4 predefines the map table from 4-bits symbol to 32-bits chip sequences, as illustrated in Table 2.2. The radio encodes these chip sequences using orthogonal quadrature phase shift keying (O-QPSK) and transmits them at 2 Mchips/s (i.e., 250 kbps). O-QPSK PHY is mandatory when IEEE 802.15.4 is operating in the 2450 MHz band. The modulating and spreading process in IEEE 802.15.4 PHY is illustrated in Fig. 2.6.

For example, one byte binary data from PPDU, denoted as $(b_0b_1b_2b_3b_4b_5b_6b_7)$, is first grouped into two nibbles of 4-bit symbols $(b_0b_1b_2b_3)$ and $(b_4b_5b_6b_7)$. And then each 4-bit symbol will be spread to a specified 32-bit long PN sequence $\leftarrow C_0C_1C_2 \ldots C_{31}$ which is also called chips sequence. Each bit or chip (C_i) in a PN sequence is then modulated using O-QPSK. The modulated O-QPSK signal goes to the half-sine pulse shaping stage and then the digital–analog conversion converts the digital baseband waveform into the analog baseband waveform. The radio front-end up-converts the baseband waveform to 2.4 GHz carrier and transmits it by the radio frequency (RF) transmitter finally [7].

Specifically, the even chips $C_0C_2C_4\ldots$ are modulated as In-phase (I) component of the carrier and the odd indexed chips $C_1C_3C_5\ldots$ are modulated as Quadrature

Table 2.2 Symbol-to-chip mapping table

Data symbol $(b_0\ b_1\ b_2\ b_3)$	Chip values $(c_0\ c_1\ \ldots\ c_{30}\ c_{31})$
0000	(PN_1) = 11011001110000110101001000101110
1000	(PN_2) = 11101101100111000011010100100010
0100	(PN_3) = 00101110110110011100001101010010
1100	(PN_4) = 00100010111011011001110000110101
0010	(PN_5) = 01010010001011101101100111000011
1010	(PN_6) = 00110101001000101110110110011100
0110	(PN_7) = 11000011010100100010111011011001
1110	(PN_8) = 10011100001101010010001011101101
0001	(PN_9) = 10001100100101100000011101111011
1001	(PN_{10}) = 10111000110010010110000001110111
0101	(PN_{11}) = 01111011100011001001011000000111
1101	(PN_{12}) = 01110111101110001100100101100000
0011	(PN_{13}) = 00000111011110111000110010010110
1011	(PN_{14}) = 01100000011101111011100011001001
0111	(PN_{15}) = 10010110000001110111101110001100
1111	(PN_{16}) = 11001001011000000111011110111000

(Q) component of the carrier. A chip ‘1’ is shaped to a positive half-sine and a chip ‘0’ is shaped to a negative half-sine as shown in Fig. 2.7. Here ‘O’ in O-QPSK expresses a half chip time offset. Since the time duration of each chip is 1 μs, the time offset between the Q-phase chips and I-phase chips is a half chip time, i.e., 1 μs/2 = 0.5 μs which is illustrated in Fig. 2.7. This offset results in a continuous phase change and constant envelope. For more implementation information about O-QPSK, please refer to literature [8].

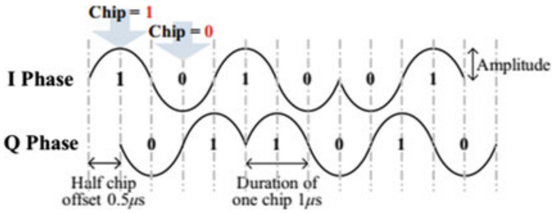
Based above introduction, Fig. 2.8 summarizes the whole process of spectrum spreading in IEEE 802.15.4. For demodulation, the receiver’s radio converts each half-sine pulse signal into a chip. Then these chips are grouped to provide PN sequences. The de-spreading is performed by mapping the PN sequence to the symbol with the highest correlation. A correlator is responsible for separating PN-Codes out of all chips that were received. The correlator captures chip sequences that are the same or similar to PN-Codes defined in Table 2.2. It then tries to find a best-match PN-Code for a chip sequence.

In the ideal case, the “best-match” PN-Code should be exactly equal to the captured chip sequence; whereas, in real situations, it is a different story. Although a sender should never transmit a wrong PN-Code (a chip sequence not included in the predefined Table), some chips could be corrupted during transmission in the presence of interference and multipath. Interference and noise can corrupt the incoming chip stream, leading to 32-chip sequences that do not match one of the 16 valid sequences. In case of corrupted chips, however, the “best-match” PN-Code need not fully agree with the erroneous chip sequence.

There are various methods to find out a “best-match” PN-Code. One such method is maximum likelihood decoder (MLD) where each received 32-bit chip sequence P is compared with the predefined PN-Codes PN_1; PN_2; … ; PN_{16} in Table 2.2 in turn to find out the corresponding symbol such that the *hamming distance* of P and the PN-code of the symbol are minimized. Here *hamming distance* is the number of different positions of two bit strings. In case of corrupted packet, the receiver maps the input sequence to the valid sequence with the smallest Hamming distance.

Besides, the literature [9] mentions that some 802.15.4 radios (e.g., CC2420) enable users to control the correlation threshold to control the maximum Hamming distance between the received 32-chip sequence and the valid SFD sequence that the receiver is willing to tolerate. If this threshold is high, the received signal must closely match the ideal signal. If this threshold is low, the receiver allows a low signal-to-noise ratio at the expense of potentially interpreting corrupted packets or channel noise as valid packets.

Fig. 2.7 Half-sine pulse shaping in O-QPSK



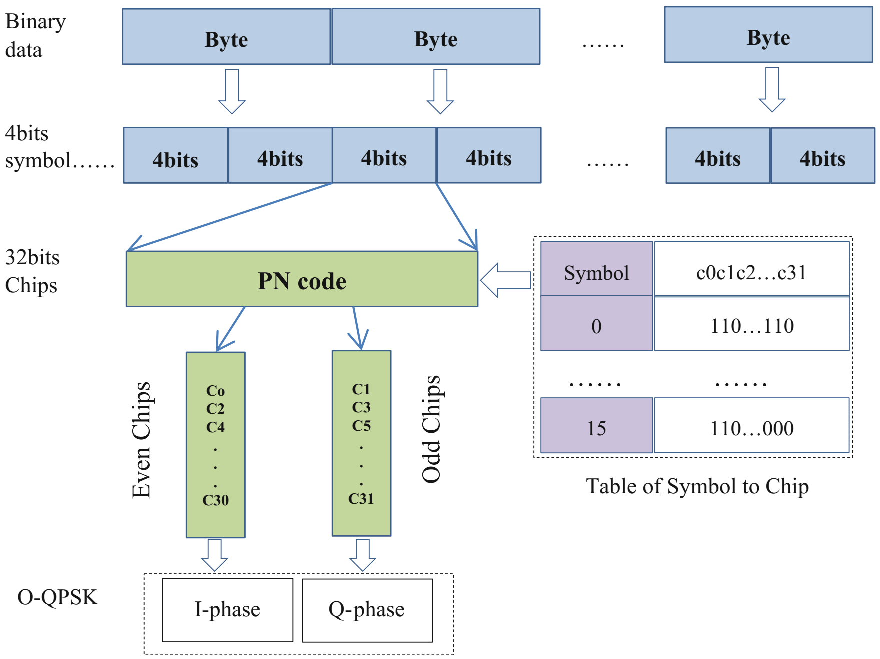


Fig. 2.8 The flowchart of spectrum spreading

2.1.3 *IEEE 802.15.4 MAC Layer*

The MAC layer in IEEE 802.15.4 handles all access to the physical radio channel and is responsible for the tasks such as generating network beacons if the device is a coordinator, supporting PAN association, employing the CSMA-CA mechanism for channel access, and so on. We have no plan to introduce every detail of IEEE 802.15.4 MAC Layer. We only focus on the related protocol procedures and characteristics with the methods of interference handling.

2.1.3.1 MAC Frame Format

In the PHY protocol data unit (PPDU), the PSDU is enclosed following PHY header PHR and contains the MAC Header (MHR), which has two frame control octets, a single octet data sequence number, good for reassembling packets received out of sequence, and 4–20 octets of address data. The MAC service data unit (MSDU) carries the frame’s payload and has a maximum capacity of 104 octets of data. Finally, the MPDU ends with the MAC footer (MFR), which contains a 16-bit frame check sequence (FCS). The frame format is illustrated in Fig. 2.9.

Table 2.3 summarizes the bit length of each field in PPDU.

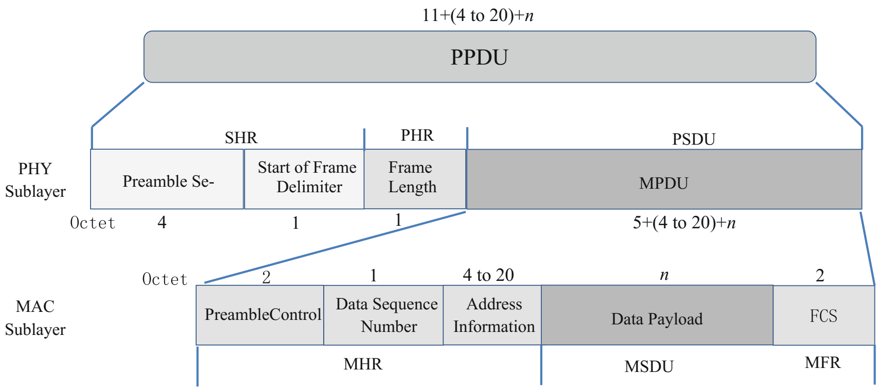


Fig. 2.9 MAC frame format and the layout in PPDU

Table 2.3 Bit length of PPDU

Field	Bit length
Preamble sequence	32
SFD	8
PHR	8
Frame control	16
Sequence number	8
FCS	16

2.1.3.2 Channel Access

An IEEE 802.15.4 network can work either in beacon-enabled or in non-Beacon mode. In the beacon-enabled mode, a network coordinator transmits regular beacons for synchronization and association procedures to control communication. Data transfer between a device and a coordinator is synchronized in a superframe. The superframe can have an active and an inactive portion. All communications take place in the active period while nodes are allowed to enter a low-power mode during the inactive period.

Furthermore, the active period in turn may consist of a contention access period (CAP) and a contention-free period (CFP). Channel access in the CAP is in the form of slotted CSMA/CA for contention access. Meanwhile, the guaranteed time slot (GTS) forms the CFP which is dedicated to low-latency applications or applications requiring specific data bandwidth. CFP always appears at the end of the active superframe starting at a slot boundary immediately following the CAP. The detailed superframe structure can be found in the IEEE 802.15.4 specification.

In the beaconless mode, there are no regular beacons, and devices communicate with each other using unslotted CSMA/CA protocol for channel access. According to the IEEE 802.15.4 protocol, the unslotted CSMA/CA algorithm is similar to the slotted CSMA/CA algorithm, besides that it is used in the non-Beacon-enabled mode. In the ***unslotted CSMA/CA***, each time a device wishes to transmit data frames or MAC commands, it waits for a random period. If the channel is found to be idle (done by CCA mechanism), following the random back-off, the device transmits its data. If the channel is found to be busy following the random back-off, the device waits for another random period before trying to access the channel again. Acknowledgment frames are sent without using a CSMA-CA mechanism.

When ***slotted CSMA/CA*** is employed, the back-off periods of one device are aligned with the start of the beacon transmission. Each time a device wishes to transmit data frames during the CAP, it locates the boundary of the next back-off period and then waits for a random number of back-off periods. If the channel is idle, the device begins transmitting on the next available back-off period boundary. In conclusion, the status switching in slotted CSMA/CA should be related with the slots arrangement.

While the *classical CSMA/CA* protocol uses binary exponential back-off, in practice some CSMA/CA protocol implemented in TinyOS uses a fixed length back-off interval [10]. At the same time, IEEE 802.15.4 does not employ RTS/CTS since the normal packet has a short packet length, compared with IEEE 802.11. This RTS/CTS overhead proves to be useful when traffic load is high, but obviously too expensive for low-data rate applications as of the case of WPANs for which IEEE 802.15.4 is designed.

2.2 WiFi

2.2.1 Overview of WiFi

Wireless fidelity (WiFi) includes IEEE 802.1l a/b/g standards for wireless local area networks (WLAN) [11, 12]. It is designed to enable users to surf the Internet at broadband speeds with mobile wireless devices via an access point (AP) or in ad hoc mode. The IEEE 802.11 architecture consists of several components that interact to provide a wireless LAN that supports station mobility transparently to upper layers. Since we are focusing on the signal interference from WiFi, we do not introduce all functions such as the mobility mechanism supported by WiFi.

The IEEE 802.11 standard covers both the medium access control (MAC) and physical (PHY) layers. These two layers have direct effect on the interference characteristics. Like in Sect. 2.1, the following content manifests the key protocol components in these two layers.

2.2.2 IEEE 802.11 Physical Layer

The original 802.11 standard defines a DSSS system operating in the 2.4 GHz frequency band. A number of amendments have greatly expanded WLAN capability by specifying more modulation and coding schemes and more frequency bands.

However, IEEE 802.11a works in 5 GHz ISM band, it does not have interference effect on ZigBee in 2.4 GHz. Thus, we only consider the standard that works in 2.4 GHz, including IEEE 802.11b/g/n. IEEE 802.11b is the first to reach mass production, which runs DSSS in the 2.4 GHz ISM band and 802.11g are orthogonal frequency division multiplexing (OFDM) systems. IEEE 802.11n mainly enhances the previous three by adding multiple-input multiple-output (MIMO) antenna support.

- Frequency Occupation and Channel

Every WiFi subtype standard predefines a fixed set of RF channels. Though a single WiFi network can only use one of these predefined RF channels, when several WiFi networks coexist in an area, they will try or will be configured to use nonoverlapping RF channels. This can easily exhaust the whole 2.4 GHz ISM band. For example, two coexisting IEEE 802.11n networks, each with 20 MHz frequency width, are enough to occupy the whole 2.4 GHz ISM band as illustrated in Fig. 2.10. Such scenario is not uncommon nowadays given the ubiquitous presence of WiFi networks. When all such WiFi networks are active, jamming the whole 2.4 GHz ISM band, it is hard to carry out WBAN communications, no matter the WBAN uses ZigBee, Bluetooth, or the draft IEEE 802.15.6 2.4 GHz standard (Fig. 2.10).

- DSSS and OFDM

DSSS and OFDM is the two most used RF transmission techniques in IEEE 802.11 standard. DSSS is also used in ZigBee. The fundamentals are the same with that in ZigBee but the spreading processes have serval differences. In IEEE 802.11, a single PN-code is used by every user in the network. This PN-code is the 11 bit barker sequence: +1 −1 +1 +1 −1 +1 +1 +1 −1 −1 −1. Spectrum spreading of each bit can be thought of as XORing operation on a stream of data bits with this specific PN sequence. As result, a "one" or a "zero" is transmitted as 11 bits of data represented by the original Barker sequence or the inverse of the Barker sequence. However, in ZigBee, there are 16 32-bit long PN-codes corresponding to 4-bit symbol. The spectrum spreading is done through predefined mapping.

Different with DSSS, OFDM is a multi-carrier modulation scheme that extends the concept of single subcarrier modulation by using multiple subcarriers within the same single channel. OFDM divides the used RF bandwidth into many narrow sub-channels called OFDM bins or subcarrier. Each OFDM bin can be treated

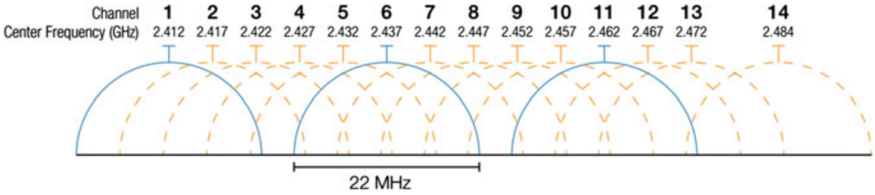


Fig. 2.10 Frequency and channel for IEEE 802.11 in 2.4 GHz

independently from other bins, and may use a different modulation (e.g., BPSK, 4-QAM) or transmission power. For 802.11 in 2.4 GHz, there are 52 OFDM subcarriers, 48 are for data.

In OFDM, a data stream is striped into bits, with different numbers of bits assigned to each bin based on its modulation scheme. An assignment of modulated bits to each of the OFDM bins is called an OFDM symbol, see Fig. 2.11. The frequency domain OFDM symbol is converted to a time domain OFDM symbol by using an inverse fast Fourier transform (IFFT) and sent on the medium by the transmitter. The receiver passes the received signal to a fast Fourier transform (FFT) module to produce the frequency representation. The data symbols are then converted to their frequency representation, corrected for the channel, and demodulated to retrieve the transmitted data bits.

- PHY Packet Format

Due to backward compatibility considerations, all subtypes of WiFi running in 2.4 GHz ISM band recognize the IEEE 802.11b packet format.

Viewing from PHY layer, a WiFi packet transmission begins with a PHY preamble, followed by a PHY header, and then the DATA. The PHY encapsulation for IEEE 802.11 is illustrated in Fig. 2.12. The PHY preamble is for receiver carrier acquisition which is a DSSS modulated signal. The PHY header contains several fields that carry control/management information. *LENGTH* field is a 16-bit unsigned integer specifying the number of microseconds that WiFi packet lasts. This implies that a maximum of 65,535 µs can be reserved for DATA segment.

Other fields in PHY frame includes:

- SYNC. This field consists of alternating 0 s and 1 s, alerting the receiver that a receivable signal is present. The receiver begins synchronizing with the incoming signal after detecting the YNC.
- Start Frame Delimiter. This field is always 1111001110100000 and defines the beginning of a frame.
- SIGNAL. This field identifies the data rate of the 802.11 frame, with its binary value equal to the data rate divided by 100 Kbps. For example, the field contains the value of 00001010 for 1 Mbps, 00010100 for 2 Mbps, and so on. The PLCP

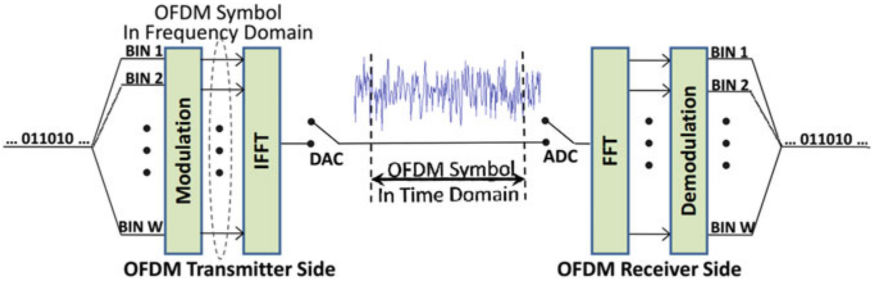


Fig. 2.11 Schematic of an OFDM system [13]

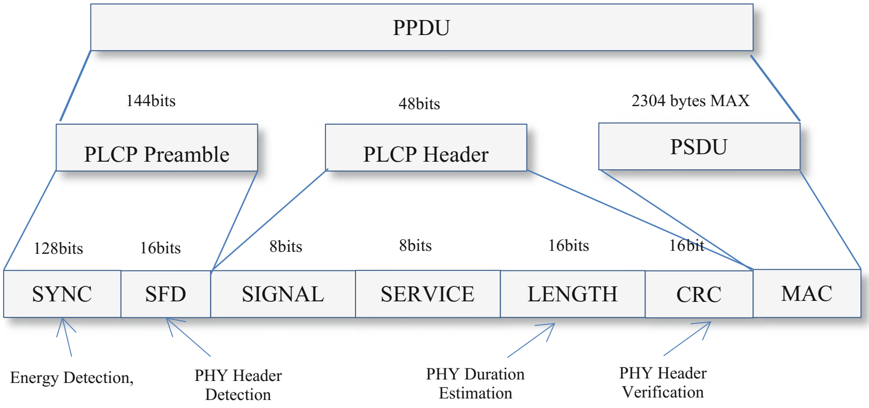


Fig. 2.12 PHY encapsulation for IEEE 802.11

fields, however, are always sent at the lowest rate, which is 1 Mbps. This ensures that the receiver initially uses the correct demodulation mechanism, which changes with different data rates.

- Service. This field is always set to 00000000, and the 802.11 standard reserves it for future use.
- Frame Check Sequence. In order to detect possible errors in the Physical Layer header, the standard defines this field for containing 16-bit cyclic redundancy check (CRC) result. The MAC Layer also performs error detection functions on the PPDU contents as well.
- PSDU. The PSDU, which stands for Physical Layer Service Data Unit, is a fancy name that represents the contents of the PPDU (i.e., the actual 802.11 frame being sent).

- Clear Channel Assessment

IEEE 802.11 standard also have the necessity function of CCA. Like ZigBee, all subtypes of WiFi carry out carrier sense multiple access (CSMA) MAC protocol. An IEEE 802.11 node shall always listen to the wireless medium before transmission. Only when the wireless medium is idle the node start transmitting. This procedure is called CCA.

The CCA mechanism used in IEEE 802.11 has the same working way with 802.15.4. There are also three types of CCA: ED only CCA measures the wireless medium spectral power level; if it is greater than a threshold, the wireless medium is considered busy. Carrier sense (CS) only CCA tries to capture WiFi PHY preambles; if a PHY preamble is successfully captured, the wireless medium is considered busy. Usually, CS-only CCA also looks into the content of the PHY header immediately following the captured PHY preamble (if there is one) to provide more accurate CCA evaluations. ED + CS CCA does both. In practice, CS-only CCA and ED + CS CCA are most widely implemented.

Under the constraint of CCA, a node having packet to be sent enters the transmit mode and waits for a certain time period to make sure the medium is free (CSMA). The determination process is done by using the CCA module that may be configured in above three modes to make this determination. Only when the result is true, the node will have the probability to transmit the packets.

- Reception Handling in PHY Layer

Reception at a node can be explained in terms of the PLCP (physical layer convergence protocol) headers that encapsulate packets (shown in Fig. 2.11).

At the receiver side, the SYNC binary data will be first detected when it is alerting with 0, 1 sequence mode. A preamble of a *SYNC* bit pattern will trigger the ED circuitry that alerts the receiver to an incoming transmission. This 0, 1 altering bit pattern is also used to extract symbol timing. It is always transmitted at 1 Mbps. 802.11b/g uses either a long preamble that transmits the PLCP header (Fig. 2.11) at 1 Mbps or a short preamble that transmits the PLCP header at 2 Mbps, regardless of the transmit speed of the MAC frame itself.

The receive procedure is invoked by the CCA procedure upon detecting a portion of the preamble sync pattern followed by a valid SFD and PLCP Header. The SFD is a specific 16-bit pattern (0x07cf with long preambles) that signifies the start of PLCP data.

After a WiFi device detects a PHY preamble and decodes the following PHY header, it will mute (i.e., refrain from transmitting) for a number of microseconds depending on the received *LENGTH* field and the device's specific implementation. The *LENGTH* field defines the packet length, which is used with bit rate information in the *SERVICE* field to determine the overall duration of the packet. To complete the PLCP processing, the receiver computes a CRC over the header. It generates a physical layer error if the header is corrupted. The MAC frame follows and it includes a separate CRC over the MAC contents. The receiver generates a separate MAC layer error if the MAC is corrupted. Otherwise, it will deliver the received packets to MAC layer.

2.2.3 IEEE 802.11 MAC Layer

Like IEEE 802.15.4, IEEE 802.11 also has two fundamental modes: distributed coordination function (DCF) and point coordination function (PCF). In DCF mode, each station must sense the status of the wireless medium before transmitting. However, in PCF, a point coordinator also known as AP, coordinates the communication. Both modes are based on CSMA/CA mechanism. The 802.11 standard specifies using CSMA/CA with ACKs as the MAC protocol, optionally with the

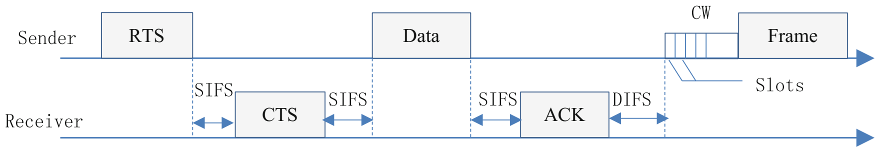


Fig. 2.13 Timing diagram for CSMA/CA with RTS/CTS

addition of RTS/CTS packets. The protocol also specifies the SIFS (short interframe space)[1] and DIFS (DCF interframe space)[2] intervals when nodes should defer using the medium.

Figure 2.13 presents the key features of the 802.11 MAC protocol through a timing diagram. In IEEE 802.11, the CCA module introduced in Sect. 2.2.2 is used to detect whether the medium is free and if it declares the medium to be free, the packet is sent. If it is busy, the transmitter defers the transmission for a random number of 20 µs slots selected between 1 and the contention window (CW), and repeats the CCA procedure.

The CW following the DIFS is shown in the figure. This window is divided into slots and is doubled every time they fail to access the medium, until CW reaches a maximum size of 1023 slots; the packet is sent if this maximum is reached regardless of whether the medium is busy. Nodes use a uniform random distribution to select a slot and wait for that slot before attempting to access the medium. The node that selects the earliest slot wins while others defer. The CW is reset to a minimum value 31 slots after a transmission.

When receivers receive a nonbroadcast data packet that passes the CRC check for data integrity, they send an ACK packet within a fixed time limit to acknowledge the receipt. If the transmitter does not receive an ACK, it considers the packet (or its ACK) lost. It then retransmits the packet by reinserting it at the front of the transmission queue and treating it as a new packet. Retransmission can be repeated up to seven times, after which the packet is dropped. Optionally, nodes can precede data packets with a RTS/CTS exchange to reduce the likelihood of interference by hidden terminals, but most implementations choose not to do so in practice because the costs outweigh the benefits.

Table 2.4 summarizes the duration of the DIFS, SIFS, and backoff slots for 802.11b and 802.11g. Also shown are the maximum and minimum packet sizes for 802.11b, 802.11g, and 802.15.4. It is worth noting that for many 802.11b and 802.11g packets, the entire air time is smaller than an 802.15.4 slot time. Based on the relatively small time intervals between 802.11 transmissions, one can easily see that a backlogged 802.11 sender can potentially corrupt the vast majority of 802.15.4 packets.

[1] SIFS is the amount of time in micro seconds required for a wireless interface to process a received frame and to respond with a response frame.

[2] If a node finds that the medium is continuously idle for DCF interframe space (DIFS) duration, it is then permitted to transmit a frame.

Table 2.4 Packet and interval durations for 802.11 and 802.15.4 [9]

Parameter	802.15.4	802.11b	802.11g
SIFS	N/A	30 μs	10 μs
DIFS	N/A	50 μs	28 μs
Slot time	320 μs	20 μs	9 μs
Initial CW	1–32	0–31	0–31
Successive CWs	1–8	BEB	BEB
Min length packet	352 μs	202 μs	194 μs
Max length packet	4256 μs	1906 μs	542 μs

Table 2.5 Features comparison between WiFi and ZigBee

Standard	ZigBee	WiFi
IEEE Spec	802.15.4	802.11b/g/n
Frequency band	2.4 GHz	2.4 GHz
Max signal rate	250 kbps	54 Mbps
Nominal range	10–100 m	100 m
Nominal TX power	(−25)–0 dBm	15–20 dBm
Number of channels	16	14
Channel bandwidth	2 MHz	22 MHz
Spreading	DSSS	DSSS, OFDM
Data protection	16-bit CRC	32-bit CRC

Besides above characteristics, the 802.11 MAC also defines management packets, the most relevant here being beacons and probes. An AP periodically (~100 ms) broadcasts beacons to assist clients with association, roaming, synchronization, power saving and other tasks. Beacons carry an 8-octet timestamp field so that the client's NIC can synchronize its clock with the AP to meet the timing constraints of the 802.11 MAC. Probe packets are sent by a client to discover APs.

2.3 Summary

In this chapter, we introduce the key design features in IEEE 802.11 and IEEE 802.15.4. These issues are directly related with the forthcoming solutions discussed in the following content. Here we provide the comparisons in protocol features between WiFi and ZigBee as the summaries in Table 2.5.

References

1. IEEE Computer Society, 802.15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs). Available at: http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf
2. J. Eidson, E.A. Lee, S. Matic, S.A. Seshia, J. Zou, Distributed real-time software for cyber-physical systems. Proc. IEEE (special issue on CPS) **100**(1), 45–59 (2012)

3. ZigBee Alliance, ZigBee specification. ZigBee document 053474r17, (2008)
4. Y. Wu, J.A. Stankovic, T. He, S. Lin, Realistic and efficient multi-channel communications in wireless sensor networks, in *INFOCOM* (2008)
5. K.L. Hieu, H. Dan, A. Tarek, A practical multi-channel media access control protocol for wireless sensor networks, in *ACM/IEEE International Conference on Information Processing in Sensor Networks* (2008)
6. H.W. So, G. Nguyen, J. Walrand, Practical synchronization techniques for multi-channel MAC, in *MobiCom* (2006)
7. L. Kong, X. Liu, mZig: enabling multi-packet reception in ZigBee, in *ACM MobiCom* (2015)
8. R. Ahmad, O. Sidek, S.K.K. Mohd, Development of the OQPSK modulator for ZigBee standard on FPGA, in *Proceeding of International Conference on Robotics, Vision, Signal Processing & Power Applications (RoViSP'09)* (2009)
9. C.M. Liang, N.B. Priyantha, J. Liu, A. Terzis, Surviving Wi-Fi interference in low power ZigBee networks, in *ACM SenSys* (2010)
10. A. Woo, D. Culler, A transmission control scheme for media access in sensor networks, in *MobiCom* (2001)
11. IEEE Computer Society, Local and metropolitan area networks—specific requirements Part 11: wireless LAN Medium access control (MAC) and physical layer (PHY) specifications. Available at: http://standards.ieee.org/getieee802/download/802.11-2007.pdf
12. IEEE Computer Society, Local and metropolitan area networks—specific requirements Part 15.1: wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). Available at: http://standards.ieee.org/getieee802/download/802.15.1-2005_part1.pdf
13. H. Rahul, N. Kushman, D. Katabi, C. Sodini, F. Edalat, Learning to share: narrowband-friendly wideband networks, in *ACM Sigcomm* (2008)

Springer

http://www.springer.com/978-3-319-47805-0

Signal Interference in WiFi and ZigBee Networks
Shi, G.; Li, K.
2017, VII, 90 p. 54 illus., Hardcover
ISBN: 978-3-319-47805-0