Specification parameters of WLAN performance with MatLab Simulink model of IEEE 802.11.

Dr. Faeza Abas Abid, Fatima Faydhe Al-azzawi, Nooraldeen Raaof Hadi
Middle technical university, institute of technology, electronic technical department, Dr.faeza@mtu.edu.iq

Abstract. Wireless networks have gained popularity that are providing users flexibility and mobility in accessing information. The IEEE 802.11 Wireless Local Area Network (WLAN) standard has become the dominant architecture in practice. In this paper IEEE 802.11 standard implemented in MATLAB Simulink, where allowing to modify beacon frame parameters such as beacon interval, SSID, supported rates, etc. Also include or exclude the CF parameter set element from the generated beacon frame, DBPSK and DQPSK modulation techniques of BER performance included in this paper to illustrate the performance of the model in AWGN and Rayleigh channels.

1. Introduction
Wireless networks are emerging as a significant aspect of networking; wireless local area networks WLANs, Bluetooth, and cellular systems have become increasingly popular in the business and computer industry with consequent security issues. WLANs, especially the Institute of Electrical and Electronics Engineers (IEEE) 802.11 networks, are becoming common access networks in private and public environments. The freedom of movement and simplicity in its implementation have made WLANs popular in the home and businesses sectors, as well as hotspots such as airports and cafes [1]. The increasing availability, off, and therefore increasing reliance on, wireless networks make it extremely important to maintain reliable and secure communications in the wake of network component failures or security breaches. However, recent news reports on a number of attacks against wireless networks, especially WLANs, have alarmed wireless adopters, developers, and intended users [1], [2]. The broadcast nature of wireless communication links makes them unique in their vulnerability to security attacks and their susceptibility to intentional threats. Organizations that want to deploy a secured WLAN infrastructure are challenged by the flaws in the existing wireless mechanism design, such as the wired equivalent privacy (WEP) protocol. WLANs provide greater flexibility and scalability than traditional LANs. Unlike a wired LAN, which requires a wire to access the network, a WLAN facilitates network transmissions of data from computers and other components through an access point (AP). An AP typically provides a range (cell or area coverage) of 100 metres. IEEE 802.11 is an international standard providing transmission speeds ranging from 1 Mbps to 54 Mbps in either the 2.4 GHz or 5 GHz frequency bands. The 802.11b is the dominant WLAN technology at present [WECMA, 2001b], and provides an expected data throughput of 5.5 Mbps. High performance radio LAN is a European Telecommunications Standards Institute (ETSI) standard operating in the 5 GHz frequency band; Hiper LAN/1
has a transmission speed of 19 Mbps, while Hiper LAN/2 operates at 54 Mbps. Hiper LAN/2 supports quality of service (QoS) and is based on an infrastructure topology, whereas Hiper LAN/1 is more suitable for forming ad-hoc networks [3] and [4].

2. IEEE 802.11 Standard

The standard provides three physical (PHY) layers and one medium access control (MAC) layer for deploying wireless communication in local networks as shown in Fig. 1. As for the logical link control (LLC) layer, there is no difference between wireless (802.11) and wired (802) LANs, such as the IEEE 802.3 Ethernet network. The MAC protocol provides two service types: asynchronous using the distributed coordination function (DCF), and synchronous using the point coordination function (PCF) that is contention-free [1].

![The 802.11 Protocol Stack](image.jpg)

The 802.11 standard is a family of specifications originally providing 1 to 2 Mbps data transmission rate using either the frequency-hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). After revisions, the standard includes 802.11a, which is operating in a 5 GHz frequency band at 54 Mbps, and 802.11b and IEEE 802.11g, operating in a 2.4 GHz frequency band at speeds of 11 Mbps and 54 Mbps, respectively [2], [3], [4]. The 802.11 standard takes advantage of radio spectrum technologies, allowing multiple users to share the radio frequencies without end-user licenses. Specifically, it makes uses of the 2.4 GHz Industrial, Scientific, and Medical band (ISM) for 802.11 and 802.11b networks, and the 5 GHz Unlicensed National Information Infrastructure (UNII) band for 802.11a-based networks. The International Telecommunication Union (ITU) defines both bands. However, interference issues remain especially in the 2.4 GHz band; if the technology interferes with an authorized operation such as an airline radio frequency, it will cease to operate. In addition, there is no protection from other technologies, such as Bluetooth, accessing 802.11 frequencies. A portal is a logical point, which is required to integrate the 802.11 architecture with existing wired LANs facilitating the transmission. An AP with software implementation can offer the portal service [5, 6].

2.1 MAC Layer

The 802.11 specifications provide asynchronous of DCF and contention-free of PCF services. The asynchronous service is always available whereas the contention-free service is optional. DCF implements the basic access method of the 802.11 MAC protocol, or path sharing. The PCF provides contention-free service, which implements a polling access method. It uses a point coordinator (PC), usually the AP, which cyclically polls stations, giving them the opportunity to transmit. Thus the access priority is provided by a PCF may be utilized to
create a contention-free access method. The PC controls the frame transmissions of the stations in order to eliminate contention for a limited period of time. Unlike the DCF, the implementation of the PCF is not mandatory. Furthermore, the PCF itself relies on the asynchronous service provided by the DCF as illustrated in Fig.1. All physical layers support one common MAC layer. Task Group 802.11e focuses on enhancing the MAC layer for QoS. [7, 8]

2.2 Physical Layers
The physical layer processes data to and from radio signals over the airwave. In other words, it handles the transmission of the frame via the air interface. The standards define three alternative physical layers (Figure 1):
1. Frequency-Hopping Spread Spectrum (FHSS)
2. Direct Sequence Spread Spectrum (DSSS)
3. Infrared (IR)

The first three physical layers belong to radio spread spectrum technology that operates in the 2.4 GHz band, while OFDM operates in the 5 GHz band. IR operates in the 300-428 GHz band and operates at a slow speed with line-of-sight connection. IR has become a legacy protocol thus will not be addressed in this discussion. [8]

2.2.1 FHSS
FHSS modulates data signals with a carrier signal that hops from one frequency to another, using time as its measurement, over a wide range of frequencies. The carrier frequency between 2.4 and 2.483 GHz is changed periodically to avoid collisions. A collision occurs only when both a narrowband system and the spread spectrum signals are transmitting at the same frequency simultaneously. A hopping code is used to decide the order of data transmission and which frequency to hop to. FHSS provides a maximum data transmission speed of 2 Mbps [9,10,11].

2.2.2 DSSS
DSSS combines a data signal at the sending station with a higher data rate bit sequence, known as the chipping code or processing gain. This chipping code reduces interferences by dividing the user data according to a spreading ratio, enabling a faster data transmission rate of 11 Mbps. It sets a specific string of bits to be sent for each data bit. A redundant bit pattern is included in the chipping code to increase resistance to interference [10, 11,12].

3. WLAN IEEE 802.11 Simulink Model
IEEE 802.11 have been implemented with MATLAB Simulink as shown in Fig.2, where the model has three main parts: Model Parameters, where the information can be selected and sent within the beacon frame and the channel parameters, 802.11 system, which is formed of the transmitter, channel, and the receiver, results, where there is a viewing to the most important received information, such as CRC flags, packet type, and received SSID.

![IEEE 802.11 WLAN](image)

**Figure 2.** IEEE 802.11 Simulink model
The transmitter is implemented with lightweight MAC sublayer and physical layer that constructs the PHY layer frame as shown in Fig. 3. It transmits each PHY frame using several consecutive channel frames.

**Figure 3.** The transmitter block in the IEEE 802.11 Simulink Model.

The MAC sublayer constructs the beacon frame, which is a type of a management frame. Fig. 4 shows the management frame format. This frame is also called a MAC protocol data unit (MPDU).

**Figure 4.** MAC sublayer beacon frame

To implement a beacon frame with a frame body that contains the following fields: Timestamp, Beacon interval, Capability, SSID elements, Supported rates element, Direct sequence (DS) parameter set element, Contention Free (CF) parameter set element (optional). The transmitter turns on periodically to transmit a beacon frame. The beacon interval parameter determines the transmission period.

The PHY Framer and Modulator are created as shown in Figs. 5 and 6, the PLCP protocol data unit (PPDU) by adding the physical layer convergence procedure (PLCP) preamble and header to the MPDU. The PLCP preamble contains 128 bits of ones (SYNC), which are later scrambled. The receiver determines the presence of a PPDU frame using this SYNC signal. The LENGTH field of the PLCP header determines the MPDU frame length. PLCP header also contains a 16-bit CRC.

**Figure 5.** PHY Framer and Modulator block
The transmitter scrambles the PPDU frame, modulates using differential binary phase shift keying (DBPSK or DQPSK) at a rate of 1 Mbps, and applies spreading using a length of 11 Barker code. This subsystem also pads extra chips to the spread symbols to reach a 1024-bit maximum PPDU length. This way, the system forces the MAC layer to work at a period of 1024 microseconds, which is a time unit (TU).

The transmitter emits 128 modulated symbols (1408 chips), which is a channel frame, at a time. Modulated symbols pass through a square root raised cosine pulse shaping filter. Pulse shaped symbols are sent through an AWGN channel that also applies a frequency offset and delay [13], [14],[15].

A Barker code or Barker sequence is a finite sequence of $N$ values of +1 and −1, with the ideal autocorrelation property, such that the off-peak (noncyclic) autocorrelation coefficients.

A Barker code has a maximum autocorrelation sequence which has side lobes no larger than 1. It is generally accepted that no other perfect binary phase codes exist [3]. It has been proven that there are no further odd-length codes, nor even-length codes of $N < 10^{22}$ [3, 4]. Barker codes of length $N$ equal to 11 and 13 are used in direct-sequence spread spectrum and pulse compression radar systems because of their low autocorrelation properties.
The side lobe level of amplitude of the Barker codes is $1/N$ that of the peak signal [3, 4]. A Barker code resembles a discrete version of a continuous chirp, another low-autocorrelation signal used in other pulse compression radars. The positive and negative amplitudes of the pulses forming the Barker codes imply the use of bi-phase modulation or binary phase-shift keying; that is, the change of phase in the carrier wave is 180 degrees.

Figure 9. Barker code used in BPSK modulation

Similar to the Barker codes are the complementary sequences, which cancel side lobes exactly when summed; the even-length Barker code pairs are also complementary pairs. There is a simple constructive method to create arbitrarily long complementary sequences. For the case of cyclic autocorrelation, other sequences have the same property of having perfect (and uniform) side lobes, such as prime length Legendre sequences and maximum length sequences (MLS). Arbitrarily long cyclic sequences can be constructed.

In wireless communications, sequences are usually chosen for their spectral properties and for low cross correlation with other sequences likely to interfere. In the 802.11b standard, an 11-chip Barker sequence is used for the 1 and 2 Mbit/sec rates. The value of the autocorrelation function for the Barker sequence is 0 or $-1$ at all offsets except zero, where it is +11. This makes for a more uniform spectrum, and better performance in the receivers [3, 4].

4. Results

Simulink model that was implemented in this paper allowing “to modify beacon frame parameters such as beacon interval, SSID, supported rates, etc. also include or exclude the CF parameter set element from the generated beacon frame as shown in Table 1 setting the noise level (Es/No), delay, and frequency offset introduced by the channel.

Table 1: Received MPDU

| Received MPDU |
|---------------|
| Time stamp (usec): | 1052672 |
| Beacon interval (TU): | 2 |
| SSID: | MathWorks SDR team |
| Supported Rates (Mbps): | [1 2] |
| DS Parameters: | Received |
| Channel number: | 11 |
| CF Parameters: | Received |
| CFP Count: | 2 |
| CFP Period: | 20 |
| CFP MaxDuration (TU): | 10 |
| CFP DurRemaining (TU): | 5 |
The simulation also displays the scatter plots of transmitted and received chips, and the despread symbols as shown in Figures 10-12 respectively. You can see the rotating scatter plot due to the frequency offset. The differential demodulator is able to track the phase change and correctly demodulate the symbols.

**Figure 10.** Scatter plot of transmitted chip

**Figure 11.** Scatter plot of received chip

**Figure 12.** The despread symbols

Modulation techniques that used in the Simulink model were DBPSK and DQPSK that tested under AWGN channel. Figure 13 is shown BER parameter of both modulation techniques where DBPSK shows butter BER with 2dB gain in $E_b/N_0$, while in Rayleigh channel both techniques show same BER as shown in Figure 14.
5. Conclusion

In this paper, IEEE 802.11 standard was implemented in MATLAB Simulink where transmitter, channel and receiver designed. Allowing to modify beacon frame parameters such as beacon interval, SSID, supported rates, etc. also include or exclude the CF parameter set element from the generated beacon frame and displaying the scatter plots of transmitted and received chips, and the despread symbols. Modulation techniques that used in the Simulink model are DBPSK and DQPSK which are tested under AWGN channel and Rayleigh channel. DBPSK shows butter BER with 2dB gain in $E_b/N_0$. While in Rayleigh channel both techniques, Wireless networks have gained popularity, providing users flexibility and mobility in accessing information. IEEE 802.11 networks, are becoming common access networks in private and public environments.

6. Reference

[1] Fitchard Kevin 2016 Wi-Fi Alliance gobbles up WiGig; plans to certify devices this year. Archived from the original on 5 March 2016. Retrieved 8 January.

[2] Fleishman Glenn December 7, 2009 The future of WiFi: gigabit speeds and beyond”. Ars Technica. Archived from the original on December 13, 2009.

[3] Retrieved Borwein, Peter; Mossinghoff, Michael J, 2009 Barker sequences and flat polynomials In James McKee; Chris Smyth. Number Theory and Polynomials. LMS Lecture Notes. 352. Cambridge University Press.

[4] Merrill I. Skolnik, 2001, Introduction to Radar Systems, 3rd Edition McGraw–Hill.

[5] Sun Weiping Choi, Munhwan Choi Sunghyun 2013 IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz (PDF). Journal of ICT Standardization.
[6] Chen, J. C, 2001 Measured Performance of 5-GHz 802.11a Wireless LAN Systems. *Atheros Communications, Inc.* 27 Augus.

[7] Enterasys Network. Wireless Demilitarised Zone (WDMZ)-Enterasys Network's Best Practices Approach to an Interoperable WLAN Security Solution. Enterasys Network 2002.

[8] Goth, G. 2002 Wireless Security Still Ad Hoc and Add-On. DS Online Exclusive. IEEE Distributed Systems Online, 3(7). 7

[9] Tittelbach-Helmrich, K., Miletić, E., Wcisleková M. and Stamenković Z, 2010 MAC Hardware Platform for RF-MIMO WLAN. Proceedings of 53rd IEEE International Midwest Symposium on Circuits and Systems, Seattle, 339-342.

[10] Dr. Emad Shehab Ahmed, Fatima, Faydhe AL-Azzawi 2008 Frequency Hopped-Orthogonal Frequency Division Multiple Access (FH-OFDMA) System Performance with Extending Quadratic Congruence (EQC) Hoping Code patterns *Journal of Engineering and Development*, Vol. 12, No. 1, March.

[11] Fatima, Faydhe AL-Azzawi Dr. Emad Shehab Ahmed 2006 Effect of multi-tone jamming on FH-OFDMA system with orthogonal hopping patterns Effect of multi-tone jamming on FH-OFDMA system with orthogonal hopping patterns, *IEEE GCC Conference (GCC)*.

[12] Fatime faydhe al-azzawi 2019 LTE RF receiver modeling and each part testing with MATLAB simulink *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 14, No. 3, pp. 1251–1257

[13] Zainab faydhe , Fatima faydhe, sada faydhe 2019 M-PSK system performance in multi-channel environments with Matlab Simulink models *Journal of Engineering and Applied Sciences*, 14(20): 7509-7516.

[14] Fatima faydhe, faeza abas, Zainab faydhe 2019 Performance Comparison between DPSK and OQPSK modulation approaches in multi environments channels with Matlab Simulink models *Wasit Journal of Engineering Sciences*, V(7), No.1).

[15] Fatima faydhe al-azzawi, Dr. Faeza Abas Abid, Zainab faydhe al-azzawi 2020 Duplexing mode, ARB and modulation approaches parameters affection on LTE uplink waveform, *International Journal of Electrical and Computer Engineering (IJEECE)*Vol. 10, No. 2, pp. 1483–1491.