IEEE 802.11b WLAN Standards Simulations

Jongoh (Andy) Jeong
jeong2@cooper.edu
The Cooper Union, New York, NY
February 19, 2020

***Abstract*—IEEE 802.11b standard is a Wireless Local Area Network (WLAN) standard that has been in use since 1999. It specifies a 2.4 GHz operating frequency for data rates of 1 and 2 Mbps using Direct Sequence Spread Spectrum (DSSS) and rates of 5.5 and 11 Mbps using Complementary Code Keying (CCK) chipping sequences to achieve 11 Mbps, as well as some common modulation techniques, such as BPSK and QPSK. In this project, the physical layer (PHY) of 802.11b ("WiFi-1") is to be implemented in MATLAB. This transmission standard implementation is strictly within the physical, focused on modulation, pulse shaping, coding and equalization, for example, and not particularly on the security, authentication, encryption aspects.**

***Index Terms*—802.11b WLAN, DSSS, CCK, BPSK, QPSK**

I. Introduction

WLAN standards are widely taken into account for data communication and incorporated in most wireless devices, such as laptops and mobile phones, to provide data communication protocols with increased range of operation. IEEE 802.11 WLAN is a network architecture in which cells, or basic service set (BSS), are controlled by a base station, or access point (AP), which are connected through some distributed system (DS), or the Ethernet – in this case wirelessly. IEEE 802.11 is currently taken as the de facto standard for WLANS, and it specifies both the medium access control and the physical layers for WLANs. Following down the OSI network model, MAC lies in the data link layer, and below sits the physical layer. While the MAC layer establishes connection between AP and STA (stations) framing data differently by its type and sub-type fields, such as authentication, association, distribution, integration and privacy, the PHY layer allows the MAC frame to be compatible for transmission over a channel medium to help recover the data from the other end. Two primary modulation and coding schemes (MCS) 802.11 employs in the physical layer are OFDM and DSSS/CCK. 802.11b specifically uses the latter mode, supporting a range of data rates up to 11 Mbps in the 2.4 GHz ISM (Industrial, Scientific and Medical) band. *Table I* describes the chipping code length, modulation type and symbol rates for each data rate for 802.11b.

II. Specifications

The PHY layer specification for the 802.11b consists of transmitter and receiver components, each broken down into smaller blocks, such as scrambler, modulator and pulse shaping filter as per IEEE 802.11b-1999 standards (see Figures 4, 5).

TABLE I
802.11b Modulation Schemes by Data Rates

Data Rate	Chipping Code Length	Modulation	Remark
1	11 (Barker seq.)	DBPSK	-
2	11 (Barker seq.)	DQPSK	-
5.5	8 (CCK)	DBPSK	first 2 bits DQPSK, next 2 bits CCK
11	8 (CCK)	DQPSK	first 2 bits DQPSK, next 6 bits QPSK

The parameters for the preamble, modulation technique and symbol rates are all different for the supported four data rates (1, 2, 5.5, 11 Mbps), they would need to be adjusted accordingly, as follows:

- **1 Mbps**: DBPSK modulation, DSSS scheme, long preamble, 1 bit/symbol
- **2 Mbps**: DQPSK modulation, DSSS scheme, long/short preamble, 2 bits/symbol
- **5.5 Mbps**: CCK modulation, CCK scheme, long/short preamble, 4 bits/symbol, first 2bits DQPSK modulated and next 2bits CCK modulated)
- **11 Mbps**: CCK modulation, long/short preamble supported, 8 bits/symbol, first 2bits DQPSK and next 6 bits QPSK

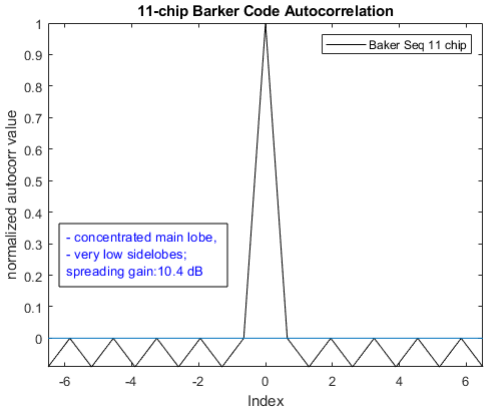
A. Modulation Techniques

DSSS. IEEE 802.11b DSSS modulation works by taking a data stream of binary bits and modulating it with a second pattern (chipping sequence). This chipping sequence used for 802.11b 1 and 2 Mbps data rates is the Barker code, which uses an 11-bit binary sequence (10110111000). This static spreading sequence is used to generate a redundant bit pattern and spread the data over a wider bandwidth. An advantage is that even if 1+ chips in the bit are lost during the transmission stage, they can be recovered with the statistical techniques embedded in the radio without re-transmission. The processing (spreading) gain for Barker coding for 1 Mbps is 10.4 dB by the Equation 1 and as shown in Figure 1. Barker code is used for data rates of 1 and 2 Mbps in 802.11b.

$$G = 10log(chip\_rate/data\_rate) = 10.4\ dBfor1Mbps \tag{1}$$

CCK. Complementary Code Keying (CCK), is also employed in 802.11b to increase the data rate. CCK uses a set of 64 $(= 2^6)$ 8-bit unique complex code words generated from mathematically derived phases ψ_0 to ψ_4, thus allowing up to

Fig. 1. Barker Sequence Autocorrelation



6 bits that can be represented by a code word. For each dibit (2-bit long) is mapped to a phase by Table II, which follows a binary (not Gray) format and assumes dibit is labeled from 0 (even). CCK is used for data rates of 5.5 and 11 Mbps in 802.11b.

TABLE II
CCK PHASE OFFSET FOR A DIBIT

dibit	phase/offset (even)	phase/offset (odd)
00	0	π
01	$\pi/2$	$3\pi/2$
10	π	0
11	$3\pi/2$	$\pi/2$

For the first dibit for both data rates 5.5 and 11 Mbps, DQPSK modulation technique is employed, thus ψ_1 follows the Equation 2, where the offset is from Table II and the last term is 0 if even, π if odd. The rest of dibits for 11 Mbps follow Table II, while for 5.5 Mbps Equation 3 applies. The codeword (c0-c7) for these four phases are shown in Equation 4.

$$\psi_1(i) = \psi_1(i-1) + \text{offset(i)} + \pi * (mod(i,2)) \quad (2)$$

$$\psi_2 = bit_3 * \pi + \pi/2 \quad (3)$$

$$\psi_3 = 0$$

$$\psi_4 = bit_4 * \pi$$

$$C_{0-7} = [e^{j\psi_1+j\psi_2+j\psi_3+j\psi_4}, e^{j\psi_1+j\psi_3+j\psi_4}, e^{j\psi_1+j\psi_2+j\psi_4}, -e^{j\psi_1+j\psi_4}, e^{j\psi_1+j\psi_2+j\psi_3}, e^{j\psi_1+j\psi_3}, -e^{j\psi_1+j\psi_2}, e^{j\psi_1}] \quad (4)$$

B. Frame Structure

For 802.11a and b standards, the packet transmission is performed using BPSK or DBPSK modulations, which allow for minimum probability of bit error rate for a given SNR compared to other modulation schemes. Each packet consists of two general parts – PLCP header and Data packet, – each sent with two different rates. The preamble and header embedded in the PLCP header are sent at the basic rate of 1 Mbps (DBPSK modulation and 16-bit CRC) and the payload is transmitted at a specified higher rate from the PLCP header. The receiver is to verify the received PLCP header is correct using CRC or Viterbi decoding with parity, for example, and to decode the MAC header and payload, as depicted in Figure 2.

Fig. 2. Packet Transmission Data Rates

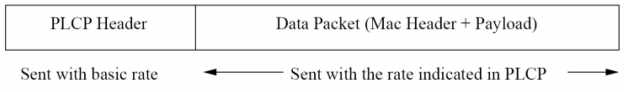
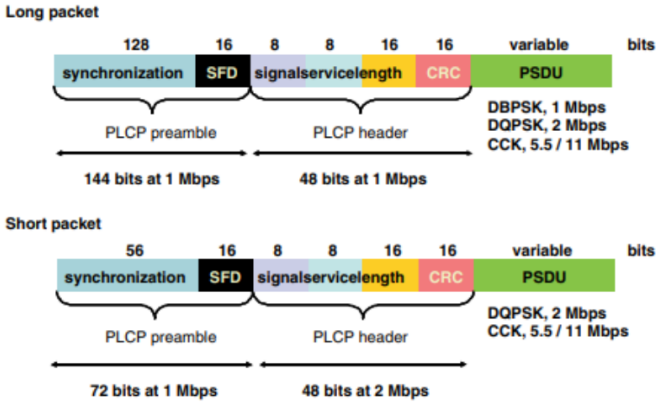


Fig. 3. 802.11b DSSS PHY Packet Formats



An optional mode that allows for data throughput at the higher rates (2, 5.5, and 11 Mb/s) is using *s*horter PHY preamble ("HR/DSSS/short"), and this shorter mode can coexist with DSSS, HR/DSSS under limited circumstances, such as on different channels or with appropriate CCA mechanisms. The packet formats for long and short preamble types are described in Figure 3. However, for the scope of this project, *l*ong packets are considered since it is mandatory.

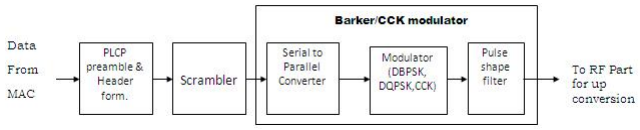
As seen in Figure 3, a preamble contains synchronization block (sequence of 128-bit long one's) and also specifies the start frame delimiter (SFD), which allows the receiver to find the beginning of the frame. This 2-byte SFD field is represented by the sequence [1111 0011 1010 0000] in the case of a long preamble, and its opposite [0000 1100 0101 1111] in the case of a short preamble. Note that the smaller size (56-bit set to 0, as opposed to the IEEE 802.11 standard 128-bit set to 1) of the scrambled bits for a short preamble (only for 2, 5.5, 11 Mbps) reduces the overhead. The preamble is transmitted at 1 Mbps with a DBPSK modulation for long packets, and at 2 Mbps with a DQPSK modulation technique to reduce the overhead time contribution. The signal block specifies the modulation scheme for the desired data rate – 0x0A for 1 Mbps with a DBPSK modulation, 0x14 for 2 Mbps with a DQPSK modulation, 0x37 for 5.5 Mbps with

a CCK4 modulation and 0x6E for 11 Mbps with a CCK8 modulation. Service blocks contains bits such as clocksbit, modulation type, length extension, and other reserved bits from MAC. Length denotes the length of the frame, and it can trigger length extension in the service block to flip. Lastly, there is 16-bit long CRC that checks that signal, service, and length header are all protected after transmission. Following the header, PSDU contains the data payload.

C. Physical Layer - Tx

The transmitter block is described in Figure 4, in which each packet, or PPDU, is composed of three parts – PLCP preamble, header, and data (PSDU). The PLCP preamble and header are generated by the requirements, scrambled and DSSS 1M modulated with Barker Sequence. Then it is sent through a carrier over to the channel.

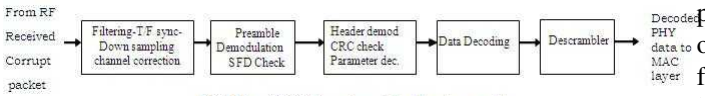
Fig. 4. 802.11b Transmitter Block Schematic



D. Physical Layer - Rx

In the receiver block, the preamble and header information is parsed in order to verify the statistics of the data decoding requirements. Once it is done, the payload component is taken and recovered.

Fig. 5. 802.11b Receiver Block Schematic



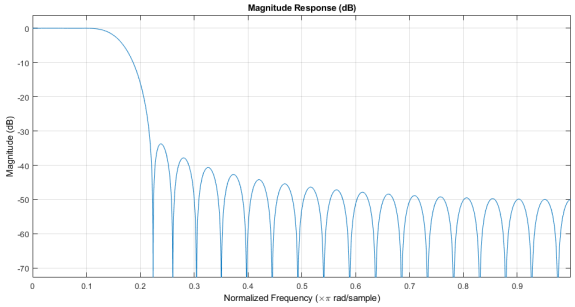
III. Approach

The general sequence of actions for this simulation goes as follows: a packet frame (“PPDU”, or a series of random bits) is generated for each iteration, SNR ratio and data rate. Then the portions for the preamble, header and PSDU are each modulated by its respective required modulation scheme, pulse-shaped by a root-raised cosine filter (after upsampling), and then is transmitted through a AWGN channel, with the signal-to-noise ratio adjusted for each bits-per-symbol and sampling rate. At the receiver side, the symbols are filtered again, assuming the receiver is perfectly aware of the impulse response of the filter used at the transmitter side. Then they are downsampled and demodulated. For this project, a ‘long’ type packet is considered throughout.

The purpose of pulse shaping is to generate bandlimited channels such that inter-symbol interference (ISI) from multi-path signal reflections is reduced among symbols. There are some filter shapes suggested by the standard release, but a root-raised cosine filter (see its magnitude response in Figure 6) is chosen for the purpose for a couple of reasons. While pulse shaping filter reduces overlapping symbol periods, a matched filter can reduce signal reflections during the transmission stage by attenuating the beginning and ending of each symbol period, thus reducing ISI as well. One commonly used matched filter is root raised cosine filter, and it is evidenced that its performance is suitable for pulse shaping purses. The parameters for filter order (M=40), Kaiser truncation window, roll-off factor (0.3), cutoff (7e6) and sampling frequencies (88e6) are selected by (CHOUKARI) paper, where the performance of a root raised cosine pulse shaping filter performance is evaluated for WLAN IEEE 802.11b channels (add cite to NASA, CHOUKARI paper) [1].

Filter. Root-raised cosine filter

Fig. 6. Mag. Resp. of Pulse Shaping Filter (M = 40, β = 0.3)



Modulation of binary bits and demodulation of symbols are performed as defined in the standards. Barker sequence of length 11 is taken as the static PN sequence to generate chipping code, and DQPSK on the first dibit, and QPSK for the rest or by Equation 2 are performed for modulation. Demodulation for Barker code was not to difficult as there were MATLAB built-in demodulator objects available for DBPSK for 1 Mbps and DQPSK for 2 Mbps. However, CCK demodulation was not available at hand; in fact, there have been numerous studies on predicting the phase angles using various techniques, such as maximum-likelihood sequence estimation (MLSE) which may not be practical for large channel delay spreads, minimum mean-squared error decision-feedback equalization (MMSE-DFE) which is of lower complexity than MLSE approach, and Fast Walsh Transform for decoding complex symbols. The employed decoding strategy is N-dimensional search of the first phase angle from the the last codeword (c7) from all possible states. Because there are maximum of 64 $(= 2^6)$ states for 11 Mbps and 4 $(= 2^2)$ states for 5.5 Mbps, it seemed suitable to perform full search and find the most likely phase angle, taking into account that each successive one depends on the previous one and there are offsets by even/odd numbering. This strategy seemed to work to a certain degree; however, there remains a room for more effective decoding prediction. For a future step could include employing the aforementioned MMSE-DFE approaches and Fast Walsh Transform [2]–[4].

PHY layer PPDU frames are generated as per the standard – PLCP preamble, PLCP header, and PSDU payload. Each

portion is different in its MSB/LSB order, scrambled state, CRC-16 protection and initial state. A constraint to note for Tx/Rx stages is that since the preamble, header and the data payload are all differently modulated, each is sent through AWGN channel and decoded separately, where only the data unit goes through pulse shaping filter. Attempts have been made in modulating by its own scheme and transmitting through the filter all at once and each separately over the channel, but the received bits for the preamble and header were not recovered reliably. A future improvement could be to use equalizer or perform effective CRC coding to correct the header information for the metadata [5].

IV. Results

Points for modulated signal, AWGN transmitted signal, and demodulated signal for Barker-11 and CCK coding are plotted in the I-Q domain (see Figures 7, 8, 9, 10). Note that as we go from lower to higher data rates where modulation scheme varies from Barker1 to CCK8, the noise becomes more concentrated. The BER curve (see Figures 11, 12) shows that at lower data rates, BER falls pretty quickly; however, for higher rates with CCK mdulations it is relatively lower, due to the poor decoding strategy. BER for 1 Mbps reached 10e-4, 2 Mbps reached 10e-3, and 5.5 Mbps and 11 Mbps reached 10e-1. One odd observation would be CCK8 performing better than CCK4 due to the ineffective employed demodulation strategy.

V. Conclusion

This simulation project allowed me to understand modulation and coding schemes for 802.11b – DSSS/CCK – as well as pulse shaping and PHY layer packet generation in depth, and see difficulties in each of the transmission stages. From the acquired insights on these constraints and issues, further improvements could be made.

Fig. 7. Barker Code 1 Mbps at Eb/No = 10

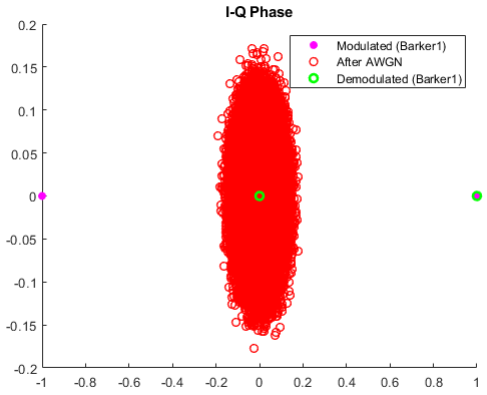


Fig. 8. Barker Code 2 Mbps at Eb/No = 10

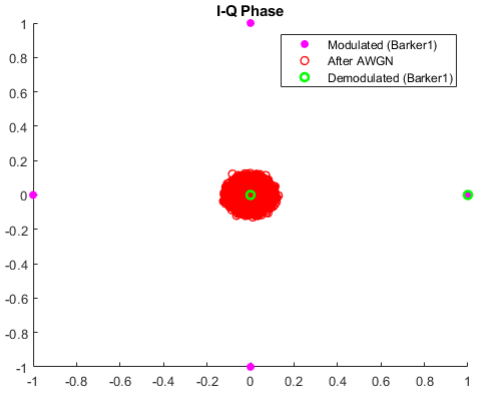


Fig. 9. CCK Code 5.5 Mbps at Eb/No = 10

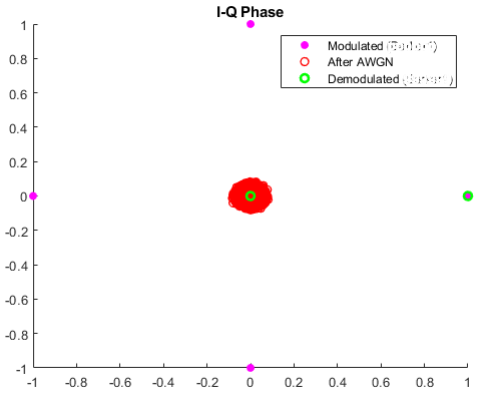


Fig. 10. CCK Code 11 Mbps at Eb/No = 10

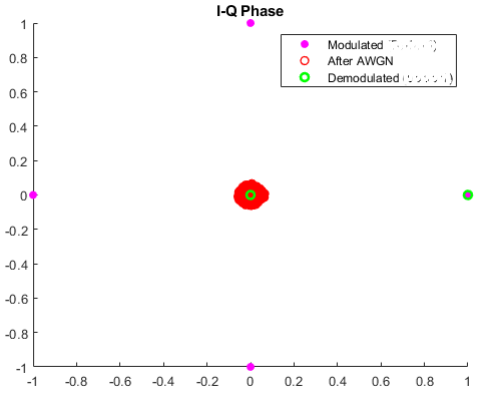


Fig. 11. Bit Error Rate for Each Data Rate

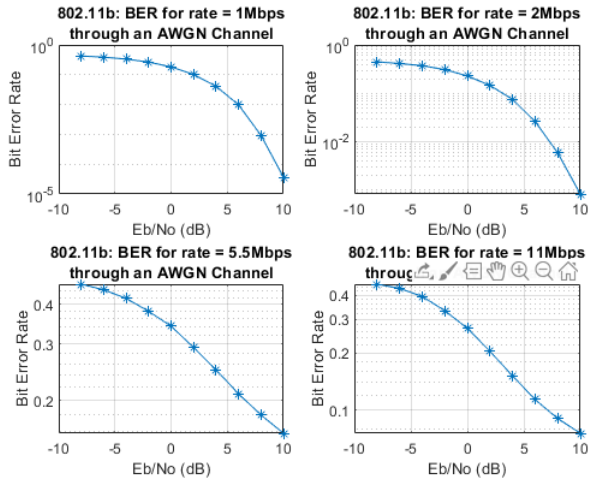
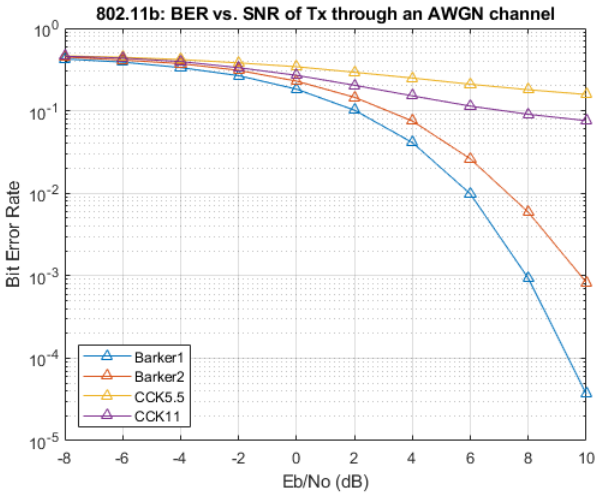


Fig. 12. Bit Error Rates for All Data Rate



REFERENCES

[1] S. A. Chouakri, M. A. Berber, A. Taleb-Ahmed, "The Role of Raised Cosine Shaping Filter Parameters in ECG Transmission Quality via WLAN IEEE802.11b Channel," in GLOBAL TELEMEDICINE AND eHEALTH UPDATES KNOWLDGE RESOURCES, 2013, pp. 487-490. Accessed on Feb. 15, 2020. [Online].

[2] C. Jonietz, W. H. Gerstacker, and R. Schober, "Receiver Concepts for WLAN IEEE 802.11b" (2004). Accessed on Feb. 15, 2020. [Online].

[3] T. D. Ta, A. V. Trinh, "Novel Low-Complexity CCK Decoder for IEEE 802.11b System," in VNU Journal of Science, Natural Sciences and Technology 27, 2011, pp. 264-270.

[4] J. Mikulka and S. Hanus, "CCK and Barker Coding Implementation in IEEE 802.11b Standard," 2007 17th International Conference Radioelektronika, Brno, 2007, pp. 1-4.
- 802.11b standards

[5] IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band," in IEEE Std 802.11b-1999 , vol., no., pp.1-96, 20 Jan. 2000

APPENDIX

A. *802.11b Glossary*

- CCK: Complementary Code Keying
- CRC: Cyclic Redundancy Code
- DFE: Decision Feedback Equalizer
- DQPSK: Differential Quadrature Phase Shift Keying
- DS: Direct Sequence
- DSSS: Direct Sequence Spread Spectrum
- Eb/No Energy per bit to Density of Noise ratio
- FHSS: Frequency Hopping Spread Spectrum
- FWT: Fast Walsh Transform
- HR: High Rate
- ISI: Inter-Symbol Interference
- LSB: Least Significant Bit
- MSB: Most Significant Bit
- MAC: Medium Access Control
- Mbps: Millions of bits per second
- PBCC: Packet Binary Convolutional Coding
- PHY: Physical Layer
- PLCP: Physical LAyer Convergence Protocol
- PPDU: PLCP Protocol Data Unit
- PSDU: PLCP Service Data Unit
- MPDU: MAC Protocal Data Unit
- SFD: Start Frame Delimiter
- WLAN: Wireless Local Area Network