WLAN IEEE 802.11b Standards Simulations

Jongoh (Andy) Jeong
jeong2@cooper.edu
The Cooper Union, New York, NY
February 26, 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 simulation project, the physical layer (PHY) of 802.11b ("WiFi-1") is implemented in MATLAB. The scope of this transmission standard implementation is strictly within the physical layer, primarily focused on modulation, pulse shaping, coding and equalization techniques, not 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 the OSI network model, the physical layer follows the data link (MAC) layer. While the MAC layer establishes connection between AP and STA (stations) by framing data differently by its type and subtype 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, which covers a distance of 38m (indoor) or 140m (outdoor), 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, symbol rates and duration for each data rate [5].

II. Specifications

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

TABLE I
802.11b Modulation Schemes by Data Rates

Data Rate	Chip Length	Modulation	Sym Rate	Sym Duration
1	11 (Barker)	DBPSK	1 Msps	1 bit
2	11 (Barker)	DQPSK	1 Msps	2 bits
5.5	8 (CCK)	DBPSK	1.375 Msps	4 bits
11	8 (CCK)	DQPSK	1.375 Msps	8 bits

The parameters for the preamble, modulation 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

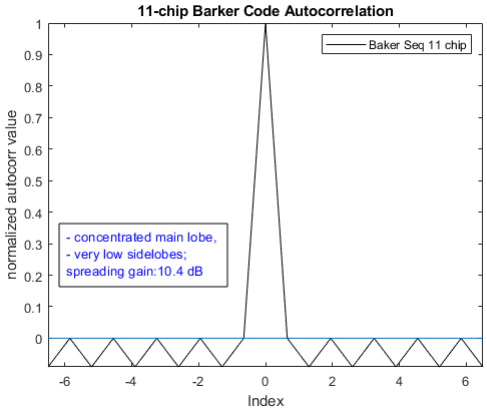
A. Modulation Techniques

DSSS. IEEE 802.11b DSSS modulation is performed by taking a data stream of binary bits and modulating it with a second pattern (chipping sequence). The static PN spreading code used for 1 and 2 Mbps data rates is Barker code, which uses an 11-bit binary sequence (10110111000). This spreading sequence is used to generate a redundant bit pattern and spread the data over a wider bandwidth. An advantage is that even if one or more 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 as in Equation 1 and as shown in Figure 1.

$$G = 10\ log_{10}(chiprate/datarate) = 10.4\ dB(1\ \text{Mbps}) \quad (1)$$

CCK. Complementary Code Keying (CCK), is also employed in 802.11b to increase the data rate up to 11 Mbps. 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 6 bits that can be represented by a code word. Each dibit (2-bit long) is mapped to a phase angle by Table II, which follows a binary (not Gray) format and assumes dibits

Fig. 1. Barker Sequence Autocorrelation



are counted from 0 (even). CCK is used for data rates of 5.5 and 11 Mbps.

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 rates of 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.

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

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

$$\psi_3 = 0$$

$$\psi_4 = bit_4 * \pi$$

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

B. Frame Structure

For 802.11a and b standards, packet transmission is performed using BPSK or DBPSK modulation schemes, 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 higher rate specified in the 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 Figures 2.

Fig. 2. Packet Transmission Data Rates

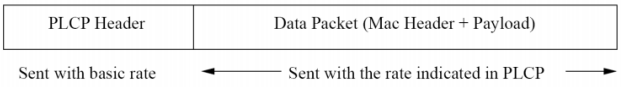
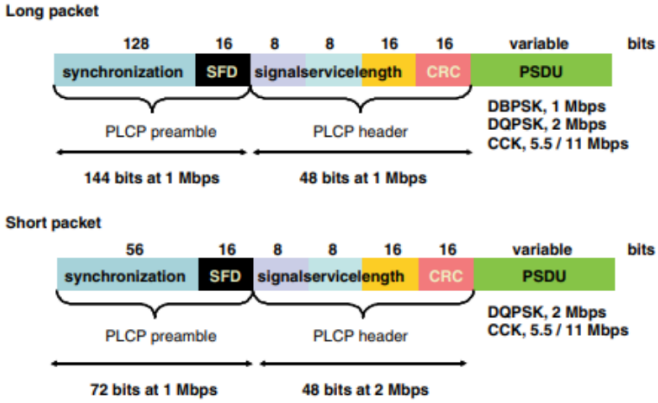


Fig. 3. 802.11b DSSS PHY Packet Formats



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.

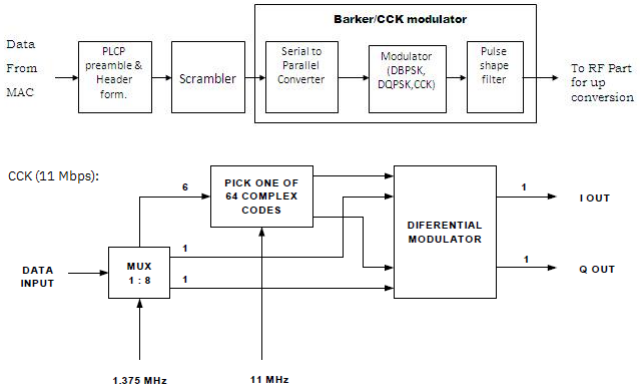
As seen in Figure 3, a preamble contains a synchronization (SYNC) block (sequence of scrambled 128-bit 1's with initial sequence of [1101 100]) and also specifies the start frame delimiter (SFD), which allows the receiver to find the beginning of the frame. This 2-byte SFD field (LSB to MSB) is represented by the sequence [1111 0011 1010 0000] in the case of a 'long' preamble, and the opposite order (MSB to LSB) in the case of a 'short' preamble. Note that the smaller size of the scrambled bits for a short preamble (56-bit set to 0, as opposed to the IEEE 802.11 standard 128-bit set to 1) can reduce the overhead for 2, 5.5, 11 Mbps. 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, a

16-bit long CRC based on the polynomial $1 + x^5 + x^{12} + x^{16}$ assures that signal, service, and length header are all protected after transmission. Following the header, the PSDU (MDPU) section contains data payload.

C. Physical Layer - Tx

In the transmitter block (see Figure 4), 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.

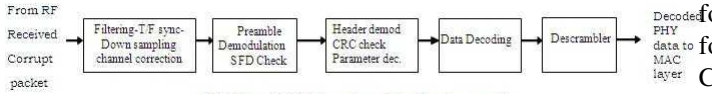
Fig. 4. 802.11b Transmitter Block Schematic



D. Physical Layer - Rx

In the receiver block (see Figure 5), the preamble and header information is extracted in order to verify the statistics of the data decoding requirements, from which the payload component is properly decoded.

Fig. 5. 802.11b Receiver Block Schematic

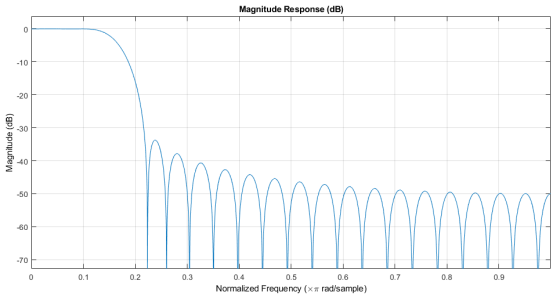


III. Approach

The simulation is implemented 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 transmitted through an 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, the mandatory 'long' type packet is considered throughout.

The role of pulse shaping is to generate band-limited channels such that inter-symbol interference (ISI) from multi-path signal reflections is reduced among symbols. There are a couple of filter shapes suggested by the standard release, and a root-raised cosine filter (see its magnitude response in Figure 6) is chosen for several reasons. While a pulse shaping filter reduces overlapping symbol periods, a matched FIR 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 (β = 0.3), cutoff (7 MHz) and sampling frequencies (88 MHz) are selected as in Choukari paper [1], where the performance of a root raised cosine pulse shaping filter performance is evaluated for WLAN IEEE 802.11b channels [1].

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



Modulation of bits and demodulation of symbols are performed as defined in the standards. Barker sequence of length 11 is taken as a static PN sequence to generate a chipping codeword, and DQPSK on the first dibit and QPSK for the rest or by Equation 2 are performed for modulation. Demodulation for Barker code is performed with MATLAB's built-in objects for DBPSK for 1 Mbps and DQPSK for 2 Mbps. However, CCK demodulation was not readily available; 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 searches for the first phase angle from the the last codeword (c7) from all possible states, including offsets for odd symbols. Because there are maximum of 64 $(= 2^6)$ states for 11 Mbps and 4 $(= 2^2)$ states for 5.5 Mbps, it seems suitable to perform a 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 works to a certain degree; however, there can be a room for more effective decoding predictions. For a future step could include employing the aforementioned MMSE-DFE

approaches and Fast Walsh Transform [2]–[4].

A PHY layer PPDU frame constructed from PLCP preamble, PLCP header, and pulse-shaped PSDU payload, each modulated differently and of different MSB/LSB order, scrambled state, CRC-16 protection and initial state. The preamble and header are to be verified with CRC bits, but this is yet to be implemented in this project. The preamble and header are then demodulated by the same DSSS-1M scheme and the data unit is demodulated by the scheme defined in the header. The bit error is then computed only if the preamble and header bits are verified to be the same as the original bits.

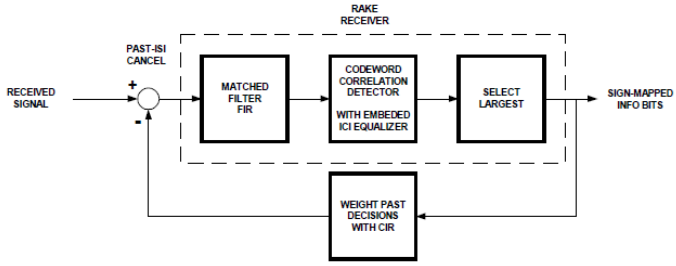
IV. Results

Points for modulated signal, AWGN transmitted signal, and demodulated signal for Barker-11 and CCK coding are plotted in the In-phase – Quadrature space (see Figures 8). Note that complex symbols are modulated well by DBPSK/DQPSK schemes and demodulated rather well. As shown in Figure 10, Barker scheme is decoded rather well, whereas CCK is somewhat poorly recovered. Also, CCK at 11 Mbps seems to outperform 5.5 Mbps performance at higher SNR values. The BER vs. SNR values for each scheme are tabulated in Table III. This may be due to poor decoding predictions, and a possible improvement could include use of an ISI equalizer or an RAKE receiver, such as in Figure 7 [5].

TABLE III
BER vs. SNR Results

Modulation	Data Rate	BER	SNR
Barker	1 Mbps	2.035e-5	28
Barker	2 Mbps	0.0008791	30
CCK	5.5 Mbps	0.1844	30
CCK	11 Mbps	0.1269	30

Fig. 7. RAKE Receiver with ISI/ICI Equalizer



V. Conclusion

In this simulation, WLAN IEEE 802.11b the core physical layer is implemented. This project allowed deeper understanding of the modulation and coding schemes for 802.11b standard (DSSS/CCK), pulse-shaping parameters, and PHY layer packet generation and recovery. The data payload on the receiver side is not fully processed by the metadata indicated in the PLCP header for now, but it does verify that the header bits are recovered properly. From the insights and difficulties encountered in equalization and decoding stages, further improvements could be made on the receiver side (decoding).

Fig. 8. Constellations at Eb/No = 10

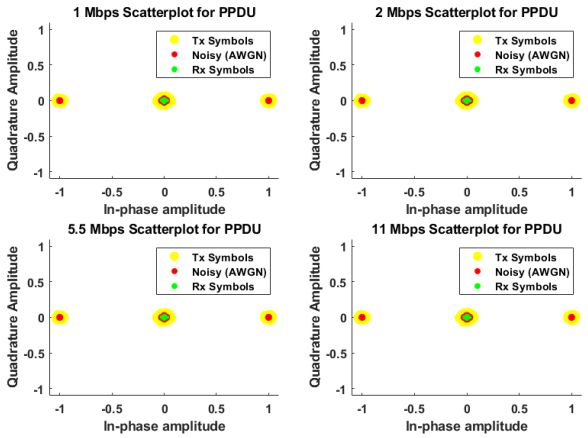
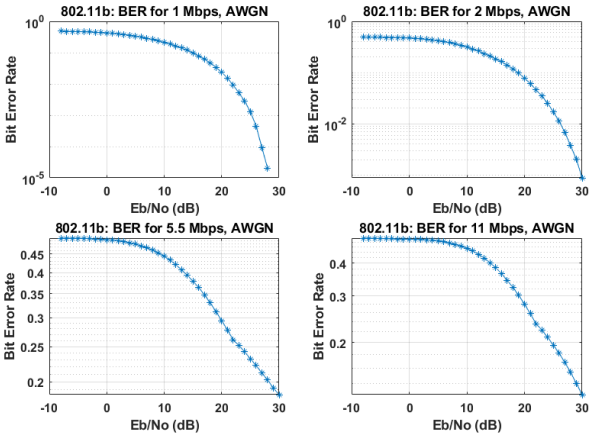


Fig. 9. Bit Error Rate for Each Data Rate



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].

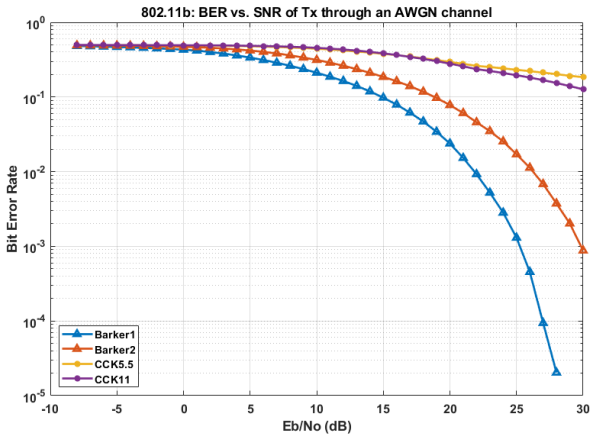
[2] C. Jonietz, W. H. Gerstacker, and R. Schober, "Receiver Concepts for WLAN IEEE 802.11b" (2004). Accessed on Feb. 15, 2020. [Online].

[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

Fig. 10. Bit Error Rates for all Data Rates



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