RESEARCH ARTICLE OPEN ACCESS

Verilog Based Design and Simulation of MAC and PHY Layers for Zigbee Digital Transmitter

Pasala Raja Prakasha Rao*, Dr.B.Rajendra Naik**
*Ph.D Scholar, Department of Electronics and Communication Engineering, JJT University, JhunJhunu, Rajasthan.
**Professor&Head, Department of Electronics and Communication Engineering, Osmania University, Hyderabad, Telangana.

Abstract:
The past several years have witnessed a rapid development in the wireless network area. So far wireless networking has been focused on high-speed and long range applications. Zigbee technology was developed for a Wireless Personal Area Networks (WPAN), aimed at control and military applications with low data rate and low power consumption. Zigbee is a standard defines the set of communication protocols for low-data-rate short-range wireless networking. Zigbee-based wireless devices operate in 868 MHz, 915 MHz, and 2.4 GHz frequency bands. The maximum data rate is 250K bits per second. Zigbee is mainly for battery-powered applications where low data rate, low cost, and long battery life are main requirements. This paper explores Verilog design for various blocks in Zigbee Transmitter architecture for an acknowledgement frame. The word digital has made a dramatic impact on our society. Developments of digital solutions have been possible due to good digital system design and modeling techniques. Further developments have been made and introduced VLSI in order to reduce size of the architecture, to improve speed of operation, improvements in predictability of the circuit behavior. Digital Zigbee Transmitter comprises of Cyclic Redundancy Check, Bit-to-Symbol block, Symbol-to-chip block, Modulator and Pulse shaping block. The work here is to show how we can design Zigbee transmitter with its specifications by using Verilog with less number of slices and Look up tables (LUTs).
Keywords: Zigbee, CRC, LUTs, occupied slice, mobility.

I. Introduction to wireless digital communication:

Over the last century, advances in wireless technologies have led to the radio, television, mobile telephone and communication satellites and all kinds of information can now be sent to any corner of the world. A wireless network is a flexible data communication system which has wireless media like radio frequencies to transmit and receive data over the air thereby minimizing the scope of wired communication.

Wireless networks use electromagnetic waves to communicate from one point to another without relying on any direct or physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end and this is called as modulation. Once data is modulated using a radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier signal.

Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted at different radio frequencies. To extract data, a radio receiver will be tuned to the corresponding carrier frequency while rejecting all other frequencies. The modulated signal will be received and the data is extracted from the modulated signal by separating the carrier, called as demodulation.

Wireless networks offer several advantages with respect to convenience, productivity and cost over traditional wired networks which are explained as follows:

Mobility: Provides mobile users with access to real-time information so that they can roam around in the network without getting disconnected from the network. This mobility supports productivity and service opportunities which are not possible with wired networks setups.
Installation speed and simplicity: Installing a wireless system can be fast and easy and can eliminate the need to pull cable through walls and ceilings which makes the setup process easier when compared with that of wired installations.

Reach of network: The network can be extended and shared to a new node into the network within the radius of the network coordinator even to places which cannot be wired.

More Flexibility: wireless networks are more flexible and can be adapted easily by changing the configuration of the network. The type of environment is not an issue while installing a wireless network which is the main factor for many of the clients to adopt wireless networking in offices, apartments and in general public places where frequent modifications are required as per the user flexibility.

Reduced cost of ownership: while the initial investment required for wireless network hardware can be higher than the cost of wired network hardware, overall installation expenses and life-cycle costs can be significantly lower in wireless environments. Moreover the maintenance of wired networks will be more than wireless network maintenance.

Scalability: wireless systems can be configured in a variety of topologies to meet the needs of specific application. Configurations can be easily changed and range from peer-to-peer networks suitable for a small number of users to large infrastructure networks that enable roaming over a broad area.

Many standards are developed with specific application, needs and characteristics required in the wireless communication. Of all these, Wi-Fi, Bluetooth and Zigbee are the most complementary standards popular round the globe. Brief introduction about Wi-Fi and Bluetooth are given below followed by the comparison of different standards with Zigbee standard.

IEEE standard 802.11: Wi-Fi

Wi-Fi is the wireless way to handle networking and it is also known as 802.11 networking [1]. The advantage of Wi-Fi is its simplicity as it provides mobile connectivity for a computer which is the rapidly growing requirement. Of all the schemes available, the IEEE 802.11 standard which is often termed Wi-Fi has become the general standard for mobile and computing devices because of its peak operating speeds of around 54 Mbps which made it to compete with wired networking. As a result of the flexibility and performance of this, many Wi-Fi hotpots have been set up which enabled people to use their laptops and other mobile devices when they are in hotels, airport lounges, cafes, and many other places using a wireless link rather than using a cable.

Standards

There are a number of standards under the IEEE 802 LAN / MAN Standard Committee (LMSC) [2]. Even

802.11 have variety of standards; each name will be formed with a letter appended to the standard formed based on the characteristics and features of that standard. These standards cover everything from the wireless standards themselves, to standards for security aspects, quality of service and the like. They are listed below along with their characteristics:

Standard	Characteristics / Specifications
802.11a	Wireless network bearer operating in the 5 GHz ISM band with data rate of up to 54 Mbps
802.11b	Wireless network bearer operating in the 2.4 GHz ISM band with data rates of up to 11 Mbps
802.11e	Quality of service and prioritization
802.11f	Handover
802.11g	Wireless network bearer operating in 24 GHz ISM band with data rates up to 54 Mbps
802.11h	Power control
802.11i	Authentication and encryption
802.11j	Internetworking
802.11k	Measurement reporting
802.11n	Stream multiplexing
802.11s	Mesh networking

The standards that are most widely known are the network bearer standards, 802.11a, 802.11b, and 802.11g.

Network types

There are two types of networks that can be formed: infrastructure networks and ad-hoc networks. The infrastructure network is aimed at office areas or to provide a Hotspot. It can be installed instead of a wired system, and can provide considerable cost savings, especially when used in established offices. A backbone wired network is still required and is connected to a server. Wireless network is then split into a number of cells, each serviced by a base station or Access Point (AP) which acts as a controller for the cell. Each Access Point may have a range between 30 and 300 meters dependent upon the environment and the location of the Access Point.

The other type of network that may be used is Ad-Hoc network. This is formed when a number of computers and peripherals are brought together. They may be needed when several people come together and need to share data or if they need to access a printer without the need for having to use wire connections. In this situation the users may only communicate with each other and not a larger wired network. As a result there is no Access Point and special algorithms within the protocols are used to enable one of the peripherals to take over the role of master to control the network with the others acting as slaves.

IEEE standard 802.15.1: Bluetooth

Bluetooth is based on IEEE standards 802.15.1 [3]. Bluetooth has now established itself in the market place enabling a variety of devices to be connected together using wireless technology. Bluetooth technology has come into use connecting remote headsets to mobile phones, but it is also used in a huge number of other applications as well. Bluetooth technology originated in 1994 when Ericsson came up with a concept to use a wireless connection to connect items such as an earphone a cordless headset and the mobile phone. Bluetooth is a wireless data system and can carry data at speeds up to 721Kbps in its basic form and in addition to this it offers up to three voice channels. Bluetooth technology enables a user to replace cables between devices such as printers, fax machines, desktop computers and peripherals, and a host of other digital devices. Furthermore, it can provide a connection between an ad-hoc wireless network and existing wired data networks. The technology is intended to be placed in a low cost module that can be easily incorporated into electronics devices of all sorts.

Bluetooth uses the license free Industrial, Scientific and Medical (ISM) frequency band for its radio signals and enables communications to be established between devices up to a maximum distance of 100 meters. Running in the 2.4 GHz ISM band, Bluetooth employs frequency hopping techniques with the carrier modulated using Gaussian Frequency Shift Keying (GFSK).

After a network connection is established between two devices they change their frequency 1600 times per second thus leaving no time for interference, and if by chance there is interference it will be for few microseconds. No other sub network will be working at the frequency at which other sub networks work, thus eliminating interference.

IEEE 802.15.4

IEEE 802.15 is the working group 15 of the IEEE 802 which specializes in Wireless PAN-standards. It includes four task groups numbered from 1 to 4 which are as follows:

Task group 1 (WPAN/Bluetooth): It deals with Bluetooth, having produced the 802.15.1 standard, published on June 14, 2002. It includes a medium access control and physical layer specification adapted from Bluetooth 1.1.

Task group 2 (coexistence): It deals with coexistence of Wireless LAN 802.11 and Wireless PAN.

Task group 3: It is in fact two groups: 3 (WPAN High Rate) and 3a (WPAN Alternate Higher Rate), both dealing with high-rate WPAN standards (20 Mbit/s or higher).

Task group 4 (WPAN Low Rate): It deals with low rate but very long battery life (months or even years). The first edition of the 802.15.4 [4] standard was released in May 2003. In March 2004, after forming Task Group 4b, task group 4 put itself in hibernation. The new Task Group 4b aims at clarifying and enhancing specific parts of the Task Group 4 standard.

Components of IEEE 802.15.4

IEEE 802.15.4 networks use three types of devices.

i. The network coordinator maintains the overall network knowledge. It is the most sophisticated one of the three types and required the most memory and computing power.
ii. The Full Function Device (FFD) supports all IEEE 802.15.4 functions and features specified by the standard. It can function as a network coordinator. Additional memory and computing power make it ideal for network router functions or it could be used in network-edge devices (where the network touches the real world).
iii. The Reduced Function Device (RFD) carries limited (as specified by the standard) functionality to lower cost and complexity. It is generally found in network-edge devices.

Zigbee

Zigbee is a wireless networking standard that is aimed at remote control and sensors based applications which is suitable for operation in harsh radio environments also in isolated locations. It builds on IEEE standard 802.15.4 which defines the physical and MAC layers. Above this Zigbee defines the application and security layer specifications enabling inter-operability between products from different manufacturers. In this way Zigbee is a superset of the 802.15.4 specification.

With the applications for remote wireless sensing and control growing rapidly, it is estimated that the market size could reach hundreds of millions of dollars in the near future. This makes Zigbee a very attractive proposition, and one which warrants the introduction of a focused standard.

Relation between IEEE 802.15.4 & Zigbee

The relationship between IEEE 802.15.4 and Zigbee is similar to that between IEEE 802.11 and the Wi-Fi Alliance. The Zigbee 1.0 specification was ratified on 14th December 2004 and is available to members of the Zigbee Alliance. Most recently, the Zigbee 2007 specification was posted on 30th October 2007. The first Zigbee Application Profile, Home Automation, was announced on 2nd November 2007.

Zigbee operates in the Industrial, Scientific and Medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in most jurisdictions worldwide. The technology is intended to be simpler and less expensive than other WPANs such as Bluetooth. Zigbee chip vendors typically sell integrated radios and microcontrollers with between 60K and 128K flash memory. Radios are also available to be used with any processor or microcontroller. Generally, the chip vendors also offer the Zigbee software stack, although independent versions are also available.

Because Zigbee can activate (go from sleep to active mode) in less than 15msec, the latency can be very low and devices can be very responsive — particularly compared to Bluetooth's wake-up delay, which is typically around three seconds. Because Zigbee can sleep most of the time, average power consumption can be very low, resulting in longer battery life.

The first stack release is now called Zigbee 2004. The second stack release is called Zigbee 2006, and mainly replaces the MSG/KVP structure used in 2004 with a Cluster Library. The 2004 stack is now more or less obsolete. Zigbee 2007, now the current stack release, contains two stack profiles, stack profile 1 (simply called Zigbee), and stack profile 2 (called Zigbee Pro). Zigbee Pro offers more features, such as multi-casting, many-to-one routing and high security with Symmetric-Key Key Exchange [5] (SKKE), while Zigbee offers a smaller footprint in RAM and flash. Both offer full mesh networking and work with all Zigbee application profiles.

Zigbee 2007 is fully backward compatible with Zigbee 2006 devices: A Zigbee 2007 device may join and operate on a Zigbee 2006 network and vice versa. Due to differences in routing options, Zigbee Pro devices must become non-routing Zigbee End-Devices (ZEDs) on a Zigbee 2006 or Zigbee 2007 network, the same as Zigbee 2006 or Zigbee 2007 devices must become ZEDs on a Zigbee Pro network. The applications running on those devices work the same, regardless of the stack profile beneath them.

CHAPTER II

II. Literature Review:

Several wireless monitoring and control applications for industrial and home applications which require longer battery life, lower data rates and less complexity than those from existing standards are present. The market requirement is a globally designed standard which is reliable, secure, with low power and cost. Zigbee defines a set of communication protocols for low data rate short range wireless networking with various topologies. Since Zigbee and its underlying standard IEEE 802.15.4 are recent, there has been little research investigating the power consumption/dissipation and silicon occupancy, speed of operation and performance. The broad area of problem is that designing a Zigbee transmitter in order to attain improvements in terms of area, power and performance.

The Zigbee standard is developed by Zigbee Alliance, which has adopted IEEE 802.15.4 for Zigbee Physical layer (PHY) and Medium Access Control (MAC) protocols. Zigbee standard is developed to fulfill the need for very low cost implementation of lower data rate wireless networks with reduced power consumption. The Zigbee standard helps to reduce the implementation cost by simplifying the communication protocols and reducing the transmission rate. The minimum requirements to meet Zigbee and IEEE 802.15.4 specifications are relatively relaxed compared to other standards such as IEEE 802.11, which reduces the complexity and cost of implementing Zigbee Transceivers. Zigbee protocol layers are based on the Open Source Interconnect (OSI) reference model [6]. The stack architecture of Zigbee is as shown below. It consists of all the layers from OSI reference model where the MAC and PHY layers are from the standard IEEE 802.15.4. The main internal contents of the stack are also represented in the picture.

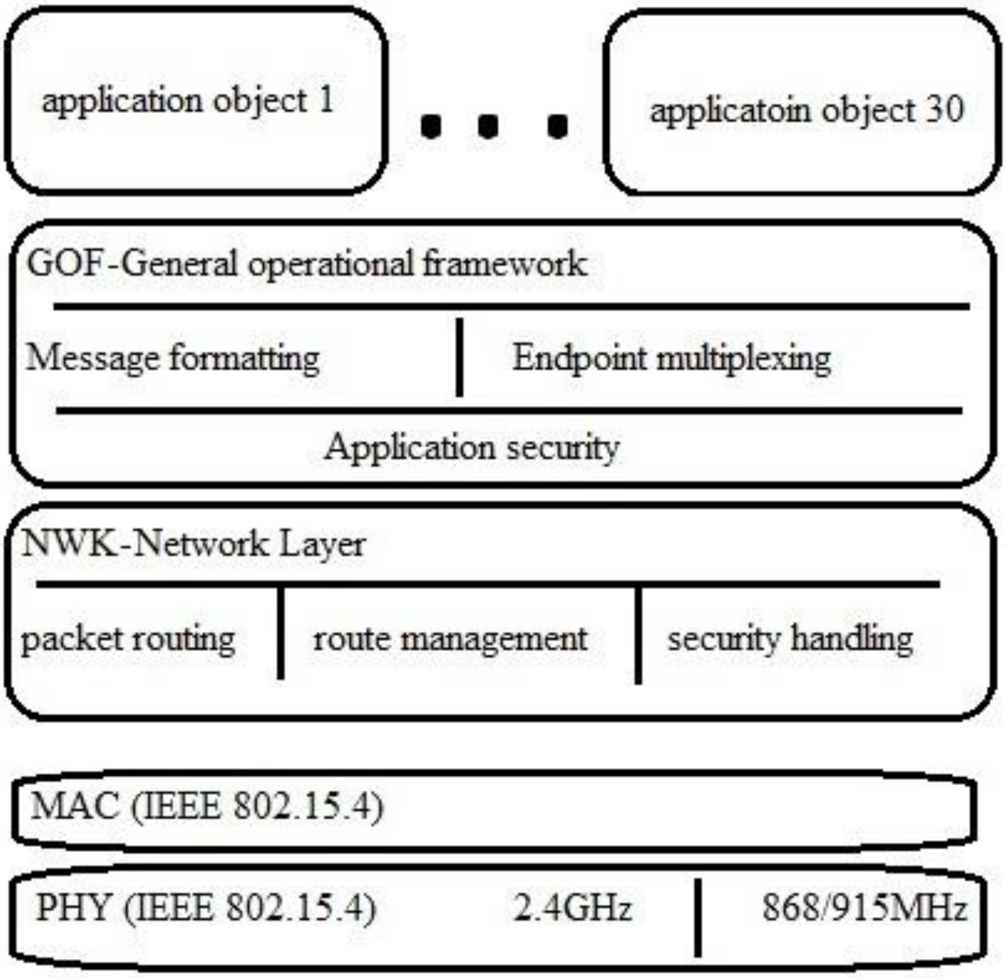

Fig: Stack architecture

Dividing a network protocol into layers has more advantages. The lower layers of the protocol are independent of the application and can be obtained from a third party, so all that needs to be done is to make changes in the application layer of the protocol. The Zigbee standard defines only the networking, application and security layers of the protocol and adopts IEEE 802.15.4 PHY and MAC layers as part of Zigbee networking protocol as shown above. The advantage of custom proprietary networking/application layers is the smaller size memory footprint is required to implement the entire protocol which results in the reduction of implementation cost. There are three important factors which induces the selection of Zigbee for Wireless PAN:

1. The low cost allows the technology to be widely deployed in wireless control and monitoring applications
2. The low power-usage allows longer power-up times with smaller batteries
3. The mesh networking provides high reliability and more extensive range

Rafidah Ahmad et al. has designed and implemented a Zigbee digital transmitter for an acknowledgement frame alone [7]. It is modeled using Verilog Hardware Description Language and is then implemented on Spartan 3E FPGA. This digital transmitter consists of Cyclic Redundancy Check (CRC) [8], Bit to Symbol, Symbol to Chip and OQPSK modulator, a pattern generator and logic analyzer. Since Verilog is used, it shows 35% improvement in number of slices used, 11% in Flip flops used, 30% in Look Up tables used and 92% in number of multiplexers used. The transmitter is designed in a shorter timeframe because of combined usage of FPGA and Verilog.

The modulation techniques used in Zigbee are mentioned as follows:

ZigBee uses Offset Quadrature Phase-Shift Keying (OQPSK) and DSSS (Direct Sequence Spread

Spectrum) for modulating radio-signals in physical layer [9]. Spread Spectrum is the spreading of the original bandwidth of the signal into a much wider frequency range. It offers interesting advantages. For example, these signals can coexist with narrow band signals and they appear as noise for other receivers thus increasing the security of the data transmitted or received.

Original signal is multiplied by a noise signal generated by a pseudorandom sequence that oscillates between +1 and -1 with a chip time (T_c) much less than the bit time of the signal (T_b). These PN sequences are not completely random (deterministic). The longer the period is, the more similar is the resulting signal to white-noise.

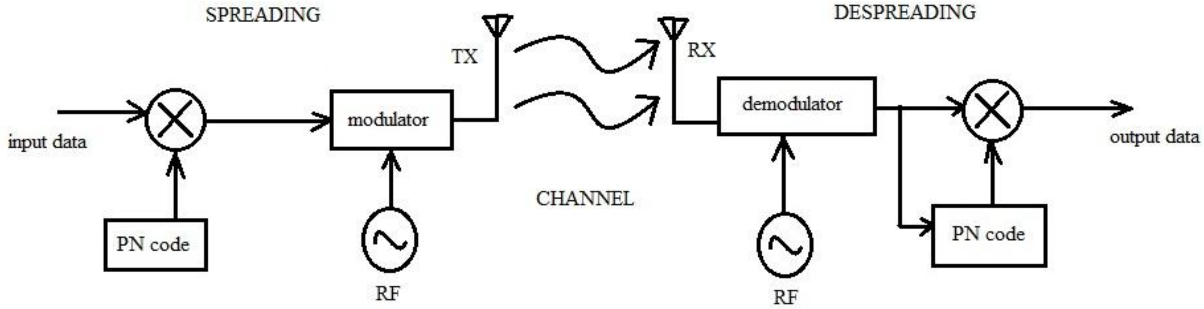

Fig: organization of blocks for spreading and de-spreading in the Zigbee organization

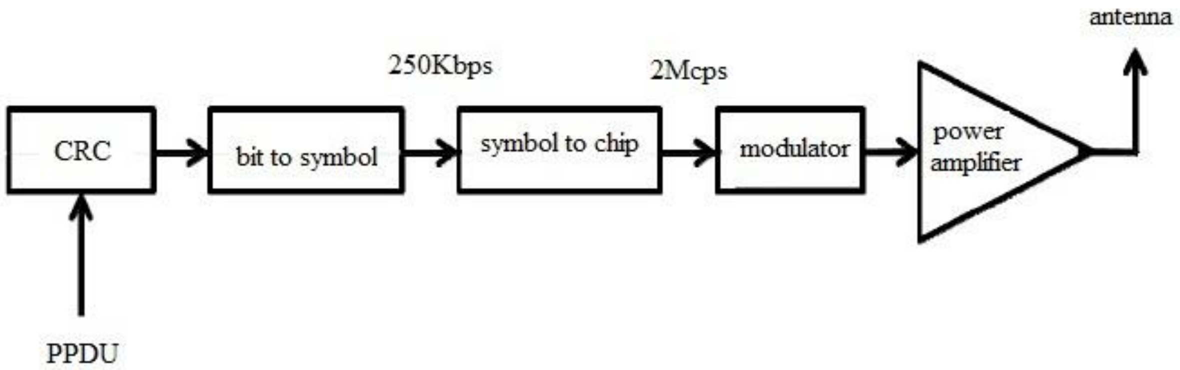

Fig: organization of blocks in Zigbee transmitter

Ting Ting Meng et al. has designed, implemented and tested the Zigbee receiver with a commercially available off-the-shelf Zigbee transceiver [10]. The receiver was defined in Harris System-in-package (SIP) and implemented through Xilinx Virtex-4 LX60 field-programmable gate array (FPGA). The receiver consists of carrier synchronization, IF down-conversion, filtering quadrature demodulation, chip synchronization, and dispreading blocks. The Harris SIP platform was equipped with high resolution ADC and Xilinx Virtex-4 FPGAs and all digital PLL and demodulator have been created to operate inside FPGA. The implementation results showed that the slices used are up to 11% of 26624, with 6% flip-flops and 7% look-up-tables (LUTs) usages.

Zigbee transmitter was designed by Rahmani using VHDL and implemented on Spartan-2 FPGA board [11]. The transmitter architecture comprised of bit-to-symbol converter, symbol-to-chip and offset quadrature phase-shift keying (OQPSK) modulator. The implementation result obtained was 150,000 gates have been used. The efficient generation of the transmit signal according to the IEEE 802.15.4 PHY can be achieved by using single step I/Q conversion or VCO modulation transmitter topologies. Synplify Pro was used as the synthesis tool and net list is created from the VHDL source. The transmitter is then test on-board.

These two papers prove that the VHDL instruction involves a large number of slices. Therefore, it contributes to a large design size. The digital part of Zigbee transmitters can be designed either with schematic, Matlab, or very high-speed integrated circuit hardware description language (VHDL). Shuaib et al. developed and simulated the transmitter design using Matlab/Simulink and its performance was evaluated. In PHY layer, Zigbee uses DSSS as spreading technique, which is to increase its power and reduce the influence of noise from nearby network. The 2.4GHz band used OQPSK technique for chip modulation. Each 4-bit symbol is mapped into 15 chip PN sequence. In 915 MHz and 868 MHz bands 1-bit symbol is mapped and uses BPSK for modulation. Having several frequency bands makes it possible to relocate within the available spectrum.

The MAC layer controls the access to the communication channel. It provides flow control through acknowledgements and retransmission. Three models for the three physical layer Zigbee bands are designed. However, schematic is inappropriate for large designs, where more logic functionality is usually involved. From the above survey, we can easily analyze that many scholars have designed the Zigbee transmitter using Matlab/Simulink, Schematic and also using VHDL and implemented through Spartan and Virtex. Transmitter designed using Verilog uses lesser number of slices, LUTs, etc. Thus, my paper is designing of Zigbee transmitter for PHY & MAC layer of IEEE 802.15.4 standard using Verilog and is to be analyzed with the simulated results obtained through Xilinx in order to reduce cost and complexity. Acknowledgement frame structure in Zigbee transmission is as shown below:

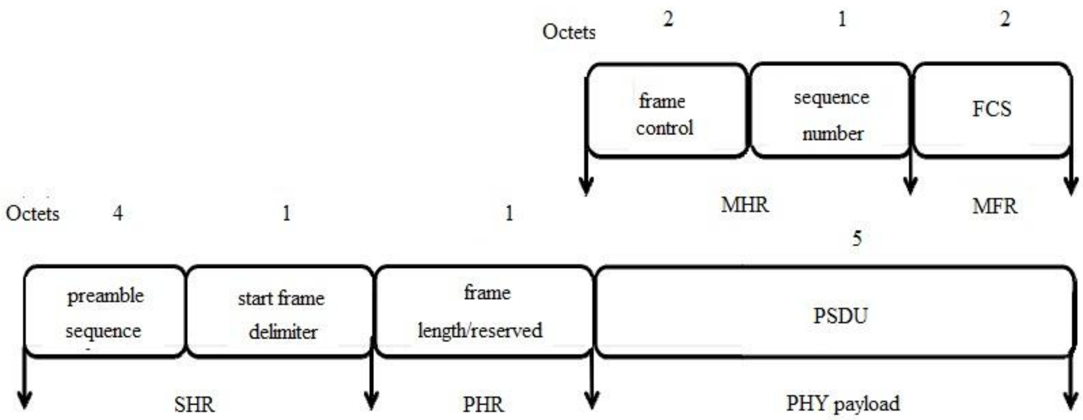

Fig: Acknowledgement frame structure

The IEEE 802.15.4 defines four MAC frame structures: beacon, data, acknowledgement and MAC command frames. The beacon frame is used by a coordinator to transmit beacons. The function of beacons is to synchronize the clock of all the devices within the same network. The data frame is used to transmit data. The acknowledgment frame is used to confirm successful frame reception. A MAC command is transmitted using MAC command frame.

III. Objectives:

A Zigbee transmitter is to be designed for PHY and MAC layers for an acknowledgement frame. This design is going to be modeled using Verilog HDL and simulated using Xilinx ISE simulator. The performance of operation of the proposed design should satisfy the theoretical specifications and will be verified with the simulation results.

The proposed system can be represented as block diagram as follows:

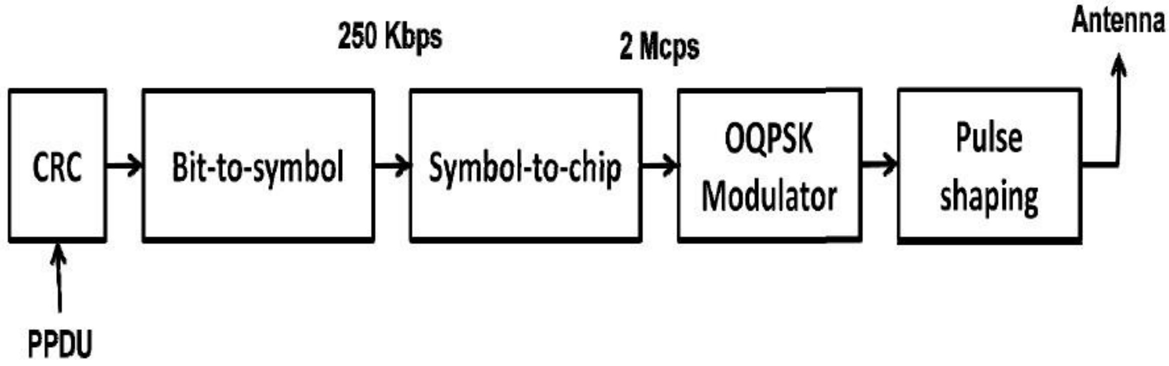

Fig: proposed Zigbee transmitter

IV. Assumptions:

The transmitter is assumed to be working at the ISM frequency 2.4GHz and the modulation technique adopted is OQPSK. The system is designed with the following specifications:

Data rate: 250 Kbps
No. of channels: 16
Operating frequency: 2.4 GHz
Channel spacing: 5 MHz
Spread spectrum: Direct Sequence Spread Spectrum
Chip rate: 2 Mega chips per second
Modulation: OQPSK with half sine Pulse shaping

V. Research methodology:

The most common error detection techniques are redundancy checking, checksum, longitudinal redundancy checking, and cyclic redundancy checking.

CRC polynomial:

Using CRC will detect approximately 99.99% of all errors occur during transmission. 16 bits are used for the block check sequence in CRC-16 where the entire data stream is treated as a long continuous binary number. As the Block Check Sequence (BCS) is separate from the message but transported within the same transmission, CRC is considered as Systematic Code. Cyclic Block codes are often written as (n, k) where n is the bit length of transmission and k is the bit length of the message. The length of the Block Check Character (BCC) in bits is

BCC = n-k

The mathematical expression for CRC-16 is evaluated in this paper.

VI. Expected outcome:

Waveforms which are generated by the Simulator corresponding to the Verilog code are expected which is the bit sequence representing the Acknowledgement frame in the Zigbee transmitter.

VII. Potential for future research:

The outputs of each block are to be verified in order to feed the next block without any mismatch. For this the blocks are to be synthesized and then it should be verified.

The modulation technique can be altered or improved to reduce inter symbol interference.

Research has to be done to optimize the symbol-to-chip block for improvement in time and occupancy.

References

[1] Brian P. Crow et al., IEEE 802.11 *Wireless Local Area Networks*", IEEE Communications Magazine, September 1997.

[2] IEEE 802 LMSC Policies and Procedures, v13.

[3] 802.15.1-2002 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs).

[4] 802.15.4-2011 - IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)

[5] Xiangdong Li, Lin Leung et al, "*Post-Quantum Diffie-Hellman and Symmetric Key Exchange Protocols*", Information Assurance, Proceedings of the 2006 IEEE.

[6] John D. Day and Hubert Zimmermann, "*The OS1 Reference Model*", Proceedings of the IEEE, VOL. 71, NO. 12, DECEMBER 1983.

[7] Rafidah Ahmad, Othman Sidek, Wan Md. Hafizi Wan Hassin, Shukri Korakkottil

Kunhi Mohd, and Abdullah Sanusi Husain, "*Verilog-Based design and implementation of Design Tansmitter for Zigbee Applications*", International Journal of Emerging Sciences, 723-724, December 2011, ISSN: 2222- 4254, © IJES.

[8] Khalifa. O, Islam. MDR and Khan.S, "*Cyclic redundancy encoder for error detection in communication channels*", RF and Microwave Conference, 2004.

[9] Shudong Fang, Stevan Berber, Akshya Swain and Saeed Ur Rehman, "*A Study on DSSS Transceivers Using OQPSK Modulation by IEEE 802.15.4 in AWGN and Flat Rayleigh Fading Channels*", TENCON 2010, 978-1-4244-6890-4/10$26.00 ©2010 IEEE.

[10] Ting Ting Meng, Chen Zhang, Peter Athanas, "*An FPGA-Based Zigbee Receiver on the Harris Software Defined Radio SIP*", SDR Forum Technical Conference, Denver, Colorado, 2007.

[11] Rahmani.E, "*Zigbee/IEEE 802.15.4*", University of Tehran, 2005.

[12] Wayne Tomasi, "*Advanced Electronic Communication System*", 6th Edition, Pearson Education.

[13] Zigbee Alliance, available at: www.zigbee.org.