Design of Wi-Fi MAC Transmit and Receive Protocol Using Verilog HDL

Srihari Nannapaneni, Xingguo Xiong, Navarun Gupta
Department of Electrical & Computer Engineering,
University of Bridgeport, Bridgeport, CT 06604

Abstract

IEEE 802.11 is a wireless LAN technology based on a cellular architecture where the system is subdivided into cells. Each cell is called Basic Service Set (BSS) which is controlled by a base station called Accesses Point (AP). Access points are connected through Distribution System (DS), typically Ethernet or wireless itself. Ethernet LAN Technology uses CSMA/CD protocol; these protocols are very effective when medium is not heavily loaded. In this paper, the Wi-Fi MAC transmit and receive protocol is implemented with Verilog HDL. The individual modules of the Wifi MAC Layer Transmit and Receive Protocol confirming to the IEEE 802.11 specification have been designed. The whole Wi-Fi Mac Layer Transmitter and Receiver are integrated. The various blocks and integrated blocks are simulated and functionality of each block is verified with test benches. Simulation results verify the correct functions of the designed Wi-Fi MAC transmit and receive protocol. The logic synthesis of the designed Wi-Fi MAC Layer Transmitter and Receiver is performed with Xilinx Synthesis Tools. Wi-Fi allows LANs (Local Area Networks) to be deployed without cabling for client devices, typically reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs. A Wi-Fi enabled device such as a PC, game console, mobile phone, MP3 player or PDA can connect to the Internet when within range of a wireless network connected to the Internet. Wi-Fi installations can provide a secure computer networking gateway, firewall, DHCP server, intrusion detection system, and other functions.

I. Introduction

Modern world requires enterprises and individuals to be connected to the Internet. Initially all Internet access was achieved through wired network using dial up connections, which provided acceptable speeds to communicate short text files. As the volume of communication increased and files included audio, images and sophisticated graphics, this type of connectivity became very slow. As the use of computers became critical to businesses, efficient communication required faster connectivity to interconnect the different computers across the enterprise to the Internet. Ethernet became the standard wired technology of choice to interconnect within the company all the computers to printers and servers. Its popularity stems from the speed at which data can be transferred over an Ethernet connection. Ethernet is the faster mass used wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100Mbps and higher. High Speed connectivity to the Internet was accomplished over broadband digital lines offering different connection speeds. The advent of fiber optics for long haul transmission and primary distribution networks, made the availability of bandwidth plentiful. Connectivity in business districts and downtown areas has become readily available, while residential customers have more limited options. The general problem of reaching the individual consumers and provide connectivity is known as the last mile.

Two wired broadband solutions became available to the individual consumer and they are offered by two different sets of industries and technologies. DSL or Digital subscriber Line offered by the telephone companies sharing the same copper wires used to provide traditional voice telephone services and Cable Modems offered by the Cable TV providers, sharing the same coaxial cable used to distribute TV programming.

A new broadband distribution technology has emerged in the last few years named **Wireless Fidelity** (or Wi-Fi) which offers the ability to connect the computers 100 feet or so apart without the need of wires or wirelessly at speeds between 1Mbps to over 54Mbps. Wi-Fi is the commercial name given to the IEEE 802.11 communication standards. This technology extends current computer networking technology (Ethernet) from today's required physical wires to wireless radio waves through space. This technology has been widely adopted as it provides the following benefits:

- No government permits (licenses) are required to operate the radio equipment.
- No wiring is required to connect to the client or user devices.
- It is based on internationally adopted standards, enabling the creation of large markets.
- Service can be obtained without operator intervention or recurring fees.

This paper describes the wireless LAN architecture, various layers used in wireless LAN with a major focus on Wi-Fi MAC layer and MAC frame format. Verilog HDL is used to demonstrate the capabilities of this new technology, where the transmitter and receiver are designed and synthesized and the simulation results obtained. The next sections describe these topics in detail.

II. Wireless LAN Architecture

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells. Each cell (called Basic Service Set**,** or BSS, in the 802.11 nomenclature) is controlled by a Base Station (called Access Point or AP). Although a wireless LAN may be formed by a single cell, with a single Access Point, most installations will be formed by several cells, where the Access Points are connected through some kind of backbone called Distribution System or DS. This DS is typically the Ethernet and in some cases, is wireless. The whole interconnected Wireless LAN including the different cells, their respective Access Points and the Distribution System can be seen as a single 802 network to the upper layers of the OSI model and is known in the Standard as Extended Service Set (ESS). Figure 1 illustrates the diagram of a typical 802.11 LAN including the components described above.

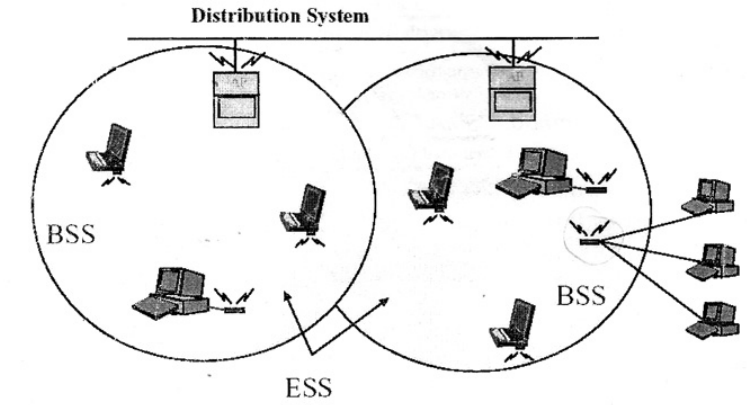

Figure 1. Distributed System

III. Wi-Fi MAC Layer

As any 802.xx protocol, the 802.11 protocol covers the MAC and Physical Layer. The Standard currently defines a single MAC, which interacts with three PHYs (all of them running at 1 and 2 Mbit/s) as follows.

- Frequency Hopping Spread Spectrum in the 2.4 GHz Band
- Direct Sequence Spread Spectrum in the 2.4 GHz Band, and
- InfraRed

Beyond the standard functionality usually performed by MAC Layers, the 802.11 MAC performs other functions that are typically related to upper layer protocols, such as Fragmentation, Packet Retransmissions, and Acknowledges.

In case of basic access method, the 802.11 uses a **Collision Avoidance (CA)** mechanism together with a **Positive Acknowledge** scheme. A station wanting to transmit senses the medium. If the medium is busy then it defers. If the medium is free for a specified time (called Distributed Inter Frame Space (DIFS) in the standard), then the station is allowed to transmit. The receiving station checks the CRC of the received packet and sends an acknowledgement, which signals the transmitter that no collision has occurred. If the sender does not receive the acknowledge signal, it will retransmit the fragment until gets acknowledged or thrown away after a given number of retransmissions.

In order to reduce the probability of two stations colliding because they cannot hear each other, the standard defines a **Virtual Carrier Sense** mechanism. A station waiting to transmit a packet first transmits a short control packet called RTS (Request To Send), which includes the source, destination, and the duration of the following transaction (i.e. the packet and the respective ACK), the destination station responds (if the medium is free) with a response control Packet called CTS (Clear to Send), which includes the same duration information.

All stations receiving either the RTS and/or the CTS, set their Virtual Carrier Sense indicator (called NAV, for Network Allocation Vector), for the given duration, and use this information together with the Physical Carrier Sense when sensing the medium. This mechanism reduces the probability of a collision on the receiver area by a station that is “hidden” from the transmitter to the short duration of the RTS transmission because the station hears the CTS and “reserves” the medium as busy until the end of the transaction. The duration information on the RTS also protects the transmitter area from collisions during the ACK (from stations that are out of range of the acknowledging station). It should also be noted that, due to the fact that the RTS and CTS are short frames, the mechanism also reduces the overhead of collisions; since these are recognized faster than if the whole packet was to be transmitted. (This is true if the packet is significantly bigger than the RTS, so the standard allows for short packets to be transmitted without the RTS/CTS transaction. This is controlled per station by a parameter called RTS Threshold). Figure 2 illustrates a transaction between stations A and B, and the NAV setting of their neighbors.

As mentioned earlier in this document, the MAC layer performs Collision Detection by expecting the reception of an acknowledge signal to any transmitted fragment (Packets that have more than one destination, such as Multicasts, are not acknowledged).

Typical LAN protocols use packets several hundred bytes long (the longest Ethernet packet could be up to 1518 bytes long). There are several reasons why it is preferable to use smaller packets in a Wireless LAN environment:

- Due to the higher Bit Error Rate of a radio link, the probability of packet getting corrupted increases with the packet size.

- In case of packet corruption (either due to collision or noise), the smaller the packet, and the less overhead it causes to retransmit it.
- On a Frequency Hopping system, the medium is interrupted periodically for hopping (in our case every 20 milliseconds), so the smaller the packet, the smaller the chance that the transmission will be postponed after dwell time.

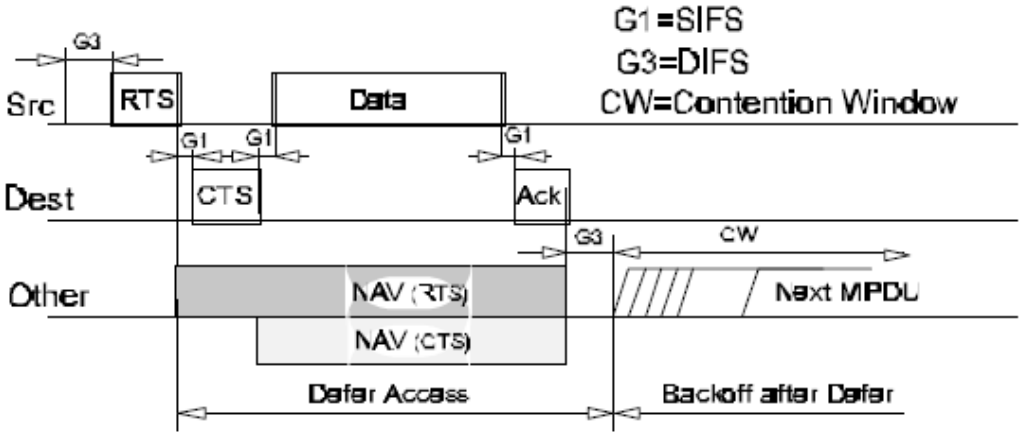

Figure 2. Transaction between Stations A and B

However, it doesn't make sense to introduce a new LAN protocol that cannot deal with packets 1518 bytes long which are used on Ethernet, so the committee decided to solve the problem by adding a simple fragmentation/reassembly mechanism at the MAC Layer. The mechanism is a simple Send-and-Wait algorithm, where the transmitting station is not allowed to transmit a new fragment until one of the following happens:

1. Receives an ACK for the said fragment, or
2. Decides that the fragment was retransmitted too many times and drops the whole frame.

It should be noted that the standard does allow the station to transmit to a different address between retransmissions of a given fragment. This is particularly useful when an AP has several outstanding packets to different destinations and one of them does not respond. Figure 3 shows a frame (MSDU) being divided to several fragments (MPDUs):

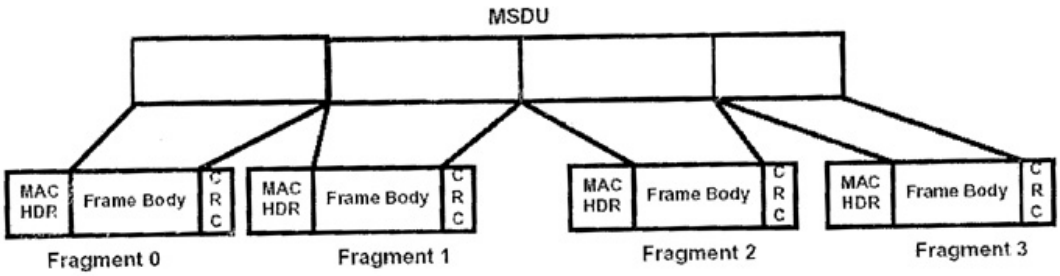

Figure 3. MAC Frame Fragmentations

The Standard defines 4 types of Inter Frame Spaces, which are used to provide different priorities:

- **SIFS** - **Short Inter Frame Space**, is used to separate transmissions belonging to a single dialog (e.g. Fragment-Ack), and is the minimum Inter Frame Space. There is always at most one single station to transmit at any given time, therefore giving it priority over all other stations. This value is a fixed value per PHY and is calculated in such a way that the transmitting station will be able to switch back

to receive mode and be capable of decoding the incoming packet. On the 802.11 FH PHY this value is set to 28 microseconds

- **PIFS-Point Coordination IFS** is used by the Access Point (or Point Coordinator, as called in this case), to gain access to the medium before any other station. This value is SIFS plus a Slot Time (defined in the following paragraph), i.e. 78 microseconds.
- **DIFS-Distributed IFS** is the Inter Frame Space used for a station willing to start a new transmission, which is calculated as PIFS plus one slot time, i.e. 128 microseconds.
- **EIFS-Extended IFS** is a longer IFS used by a station that has received a packet that it could not understand. This is needed to prevent the station (which could not understand the duration information for the Virtual Carrier Sense) from colliding with a future packet belonging to the current dialog.

Exponential Back off is a well-known method used to resolve contention between different stations wanting to access the medium. The method requires each station to choose a Random Number (n) between 0 and a given number, and wait for this number of Slots before accessing the medium, always checking if a different station has accessed the medium before. The Slot Time is defined in such a way that a station will always be capable of determining if another station has accessed the medium at the beginning of the previous slot. This reduces collision probability by half. Thus, exponential Back-off means that each time the station chooses a slot and happens to collide; it will increase the maximum number for the random selection exponentially.

The 802.11 standard defines an Exponential Back-off Algorithm that must be executed in the following cases:

1). When the station senses the medium before the first transmission of a packet, and the medium is busy
2). After each retransmission, and
3). After a successful transmission

The only case when this mechanism is not used is when the station decides to transmit a new packet and the medium has been free for more than DIFS. Figure 4 shows a schematic of the access mechanism:

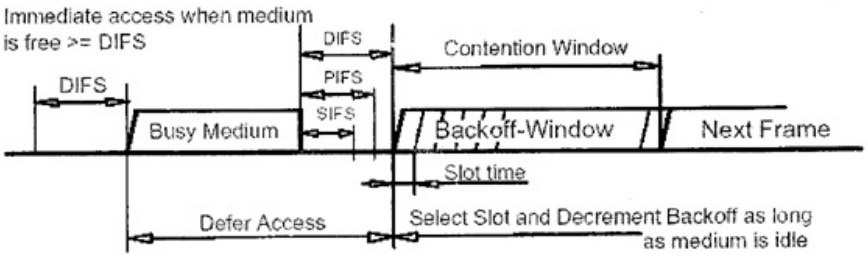

Figure 4. schematic of access mechanism

Security is one of the first concerns that people have when deploying a Wireless LAN. The 802.11 committee has addressed the issue by providing what is called WEP (Wired Equivalent Privacy). Users are primarily concerned that an intruder should not be able to:

1). Access the Network resources by using similar Wireless LAN equipment
2). Capture Wireless LAN traffic (eavesdropping)

This is done by the use of an Authentication mechanism where a station needs to prove knowledge of the current key. This is very similar to Wired LAN privacy, in the sense that an intruder needs to enter the premises (by using a physical key) in order to connect his workstation to the wired LAN.

Using the WEP algorithm, which is a Pseudo Random Number Generator, initialized by a shared secret key, prevents eavesdropping. This PRNG outputs a key sequence of pseudo-random bits equal in length to the largest possible packet, which is combined with the outgoing/incoming packet producing the packet transmitted in the air. The WEP is a simple algorithm based on RSA's RC4, which has the following properties:

- **Reasonably strong:** Brute-force attack to this algorithm is difficult because every frame is sent with an Initialization Vector, which restarts the PRNG for each frame.

- **Self synchronizing**: The algorithm re-synchronizes for each message. This is necessary in order to work in a connection-less environment, where packets may get lost (as any LAN).

Wireless LANs are typically related to mobile applications. In this type of application, battery power is a scare resource. This is the reason why the 802.11 standard directly addresses the issue of Power Saving and defines an entire mechanism which enables stations to go into sleep mode for long periods of time without losing information. The main idea behind the Power Saving Mechanism is that the AP maintains a continually updated record of the stations currently working in Power Saving mode, and buffers the packets addressed to these stations until either the stations specifically request the packets by sending a polling request, or until they change their operation mode.

IV. MAC Frame Format

There are mainly three types of frames which are used for the transmission:

- **Data Frames**: These are used for data transmission.
- **Control Frames**: These are used to control access to the medium (e.g. RTS, CTS, and ACK), and
- **Management Frames**: These are transmitted in the same manner as data frames to exchange management information, but are not forwarded to upper layers (e.g. beacon frames). Each frame type is subdivided into different Subtypes according to their specific function.

All 802.11 frames are composed of the following components:

Preamble: This is PHY dependent, and includes:

- **Synch**: An 80-bit sequence of alternating zeros and ones, which is used by the PHY circuitry to select the appropriate antenna (if diversity is used), And to reach steady-state frequency offset correction and synchronization with the received packet timing.
- **SFD**: A Start Frame Delimiter which consists of the 16-bit binary pattern 0000 1100 1011 1101, which is used to define frame timing.
- **PLCP Header:** The PLCP Header is always transmitted at 1 Mbit/s and contains logical Information used by the PHY Layer to decode the frame. It consists of:
- **PLCP_PDU Length Word**: this represents the number of bytes contained in the packet. This is useful for the PHY to correctly detect the end of packet.
- **PLCP Signaling Field**: this currently contains only the rate information, encoded in 0.5 Mbps increments from 1 Mbit/s to 4.5 Mbit/s.

- **Header Error Check Field:** The **HEC** field is a16 bit **CCIT CRC-16** error detection field. The HEC uses the **CCIT CRC-16** generator polynomial **G(x)** as follows

$$G(x) = x(16)+x(12)+x(5)+1$$

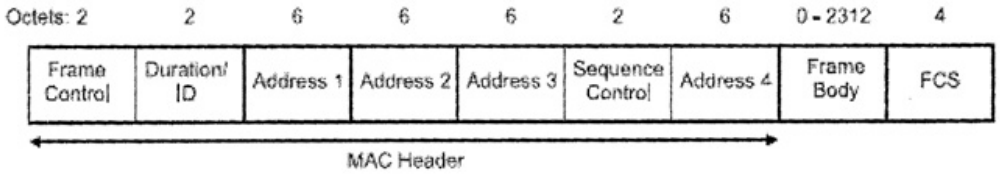

Figure 5. General MAC Frame Format

- **Frame Control Field:** The Frame Control field contains the following information:

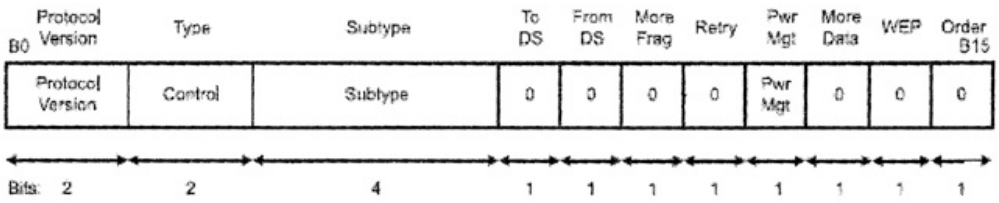

Figure 6. Frame Control Field of MAC Frame

- **Protocol Version:** This field consists of 2 bits which are invariant in size and placement across following versions of the 802.11 Standard, and will be used to recognize possible future versions. In the current version of the standard the value is fixed as 0.
- **Type and Subtype:** This 6 bits define the Type and Sub-type of the frame as indicated in the following table:

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Association Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-0001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-ACK + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
10	Data	0000-1111	Reserved

Figure 7. Different MAC Frames

The following Table summarizes the usage of the different Addresses according to ToDS and FromDS bits setting:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	**1**	**RA**	**TA**	**DA**	**SA**

Figure 8. Usage of different Addresses according to ToDS and FromDS bits setting

Sequence Control: The Sequence Control Field is used to represent the order of different fragments belonging to the same frame, and to recognize packet duplications. It consists of two subfields, Fragment Number and Sequence Number, which define the frame and the number of the fragment in the frame.
CRC: The CRC field is a 32 bit field containing a 32-bit Cyclic Redundancy Check (CRC) which is calculated over all the fields of the MAC header and the Frame Body field. The FCS is calculated using the following standard generator polynomial of degree 32.

G(x)=x(32)+x(26)+x(23)+x(22)+x(16(1)+x(11)+x(10)+x(8)+x(7)+x(5)+x(4)+x(2)+x(1)+1

RTS Frame Format

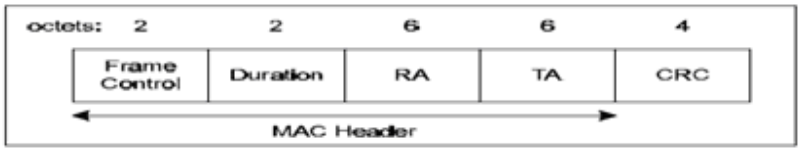

Figure 9. RTS frame format

The RA of the RTS frame is the address of the STA on the wireless medium that is the intended immediate recipient of the next Data or Management frame. The TA is the address of the STA transmitting the RTS frame. The Duration value is the time, in microseconds, required to transmit the next Data or Management frame, plus one CTS frame, plus one ACK frame, plus three SIFS intervals.

CTS Frame Format

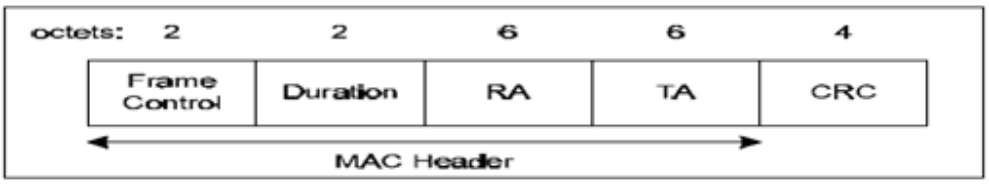

Figure 10. CTS frame format

The Receiver Address (RA) of the CTS frame is copied from the Transmitter Address (TA) field of the immediately previous RTS frame to which the CTS is a response. The Duration value is the value obtained from the Duration field of the immediately previous RTS frame, minus the time, in microseconds, required to transmit the CTS frame and its SIFS interval.

ACK Frame Format

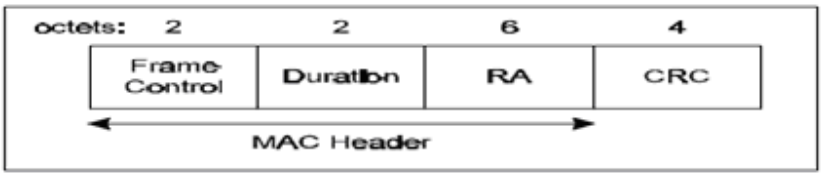

Figure 11. ACK frame format

The Receiver Address of the ACK frame is copied from the Address 2 field of the immediately previous frame. If the More Fragment bit was set to 0 in the Frame Control field of the previous frame, the Duration value is set to 0, otherwise the Duration value is obtained from the Duration field of the previous frame, minus the time, in microseconds, required to transmit the ACK frame and its SIFS interval.

V. Results and Discussions of the Proposed Wi-Fi Architecture

This section describes the main transmitter and receiver modules and the associated waveforms. The Wi-Fi MAC Transmit and Receive Protocol has been successfully implemented with Verilog HDL. The design has been simulated with Xilinx simulator to verify its correct function. The Verilog design of the Wi-Fi MAC layer transmitter and receiver has been further synthesized with Xilinx Synthesis tools to achieve gate-level netlist. The transmitter top Module is shown in Figure 12.

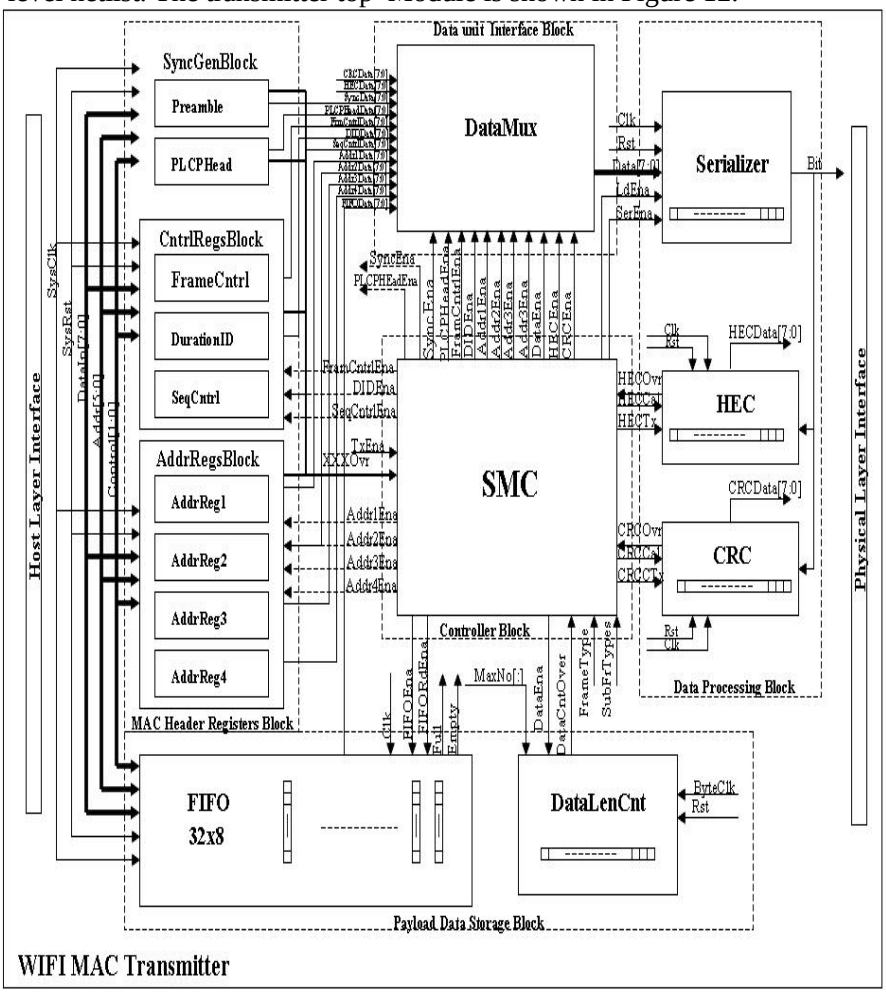

Figure 12. Wi-Fi Transmitter Architecture

The receiver top module is shown in Figure 13. As an example, the simulated waveforms of the transmitter top module is shown in Figure 14. Due to page limit, the waveforms for other simulated waveforms are not shown here.

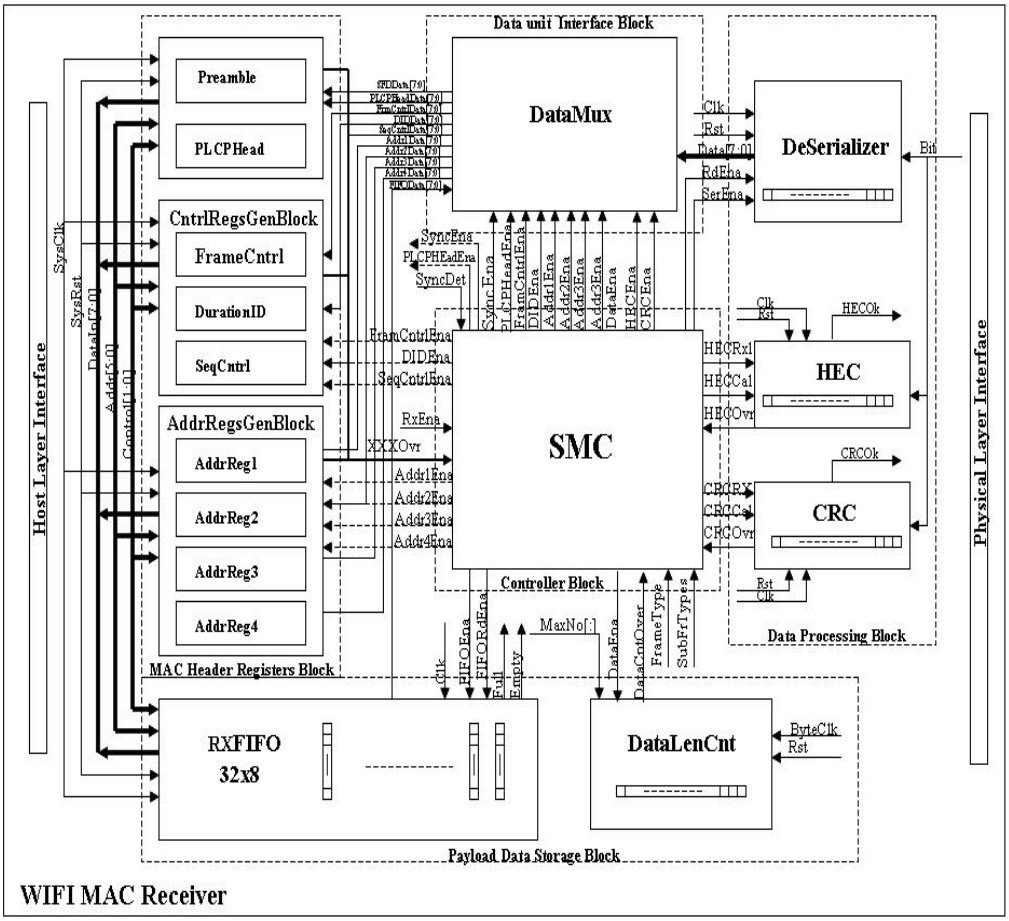

Figure 13. Wi-Fi Receiver Architecture

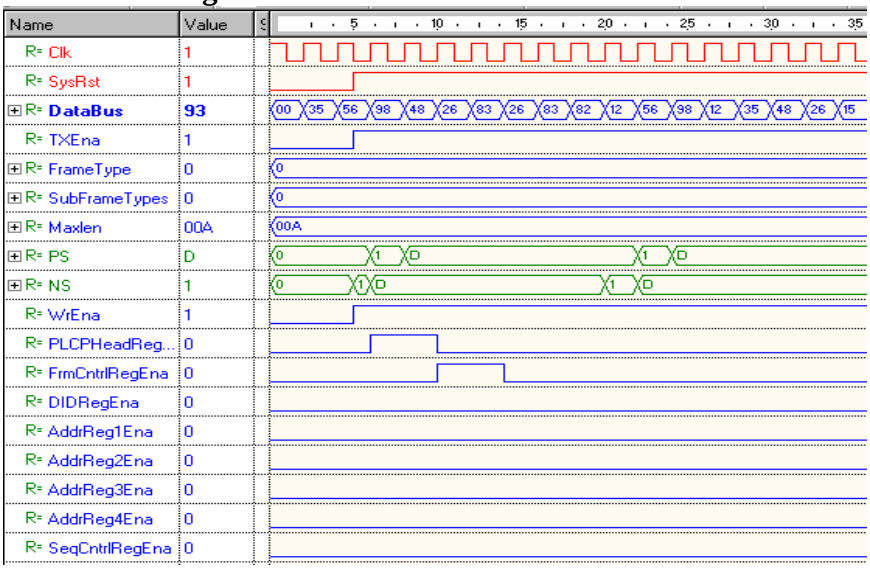

Figure 14. Part of the simulated waveforms of the transmitter top module

As an example, the RTL level schematic of the receiver after logic synthesis with Xilinx is shown in Figure 15.

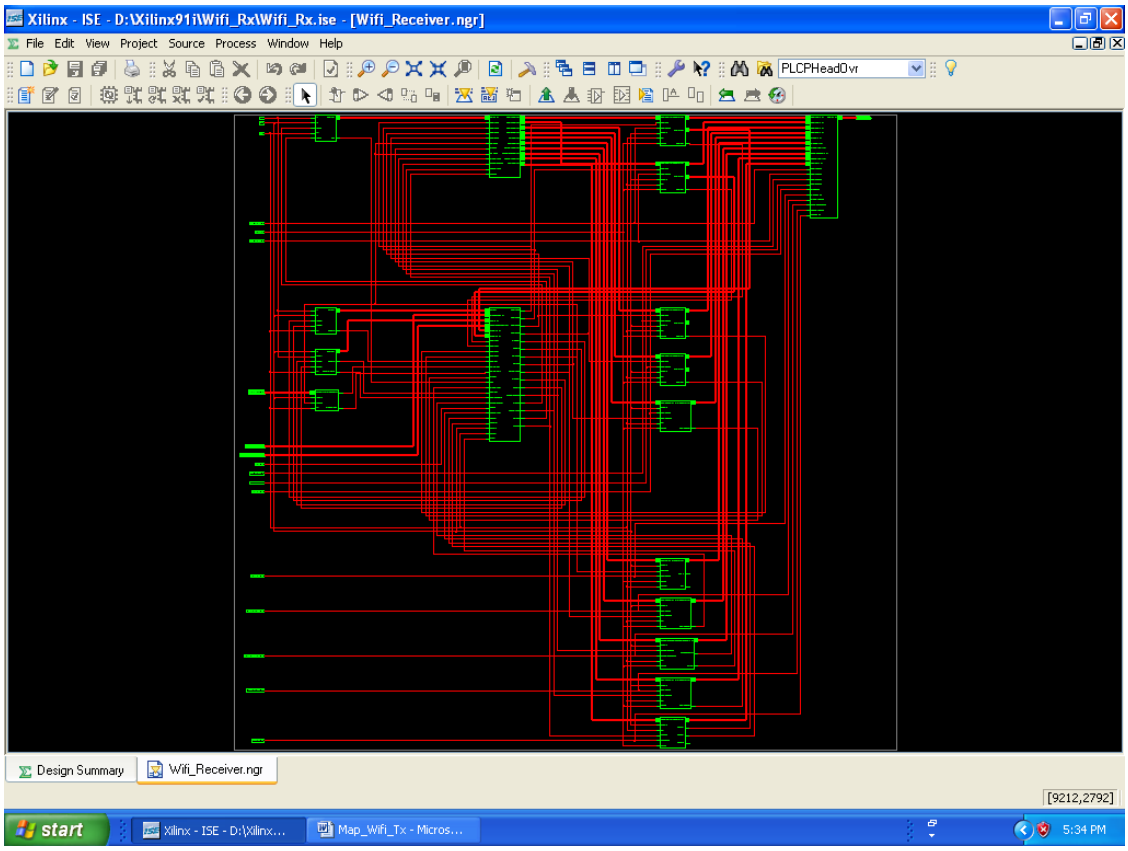

Figure 15. RTL level schematic of the receiver in Xilinx logic synthesis

VI. Conclusions

In this paper, the individual modules of the Wifi MAC Layer Transmit and Receive Protocol confirming to the IEEE 802.11 specification have been designed. The whole Wi-Fi Mac Layer Transmitter and Receiver are integrated. The various blocks and integrated blocks are simulated and functionality of each block is verified test benches. The synthesis for Wi-Fi MAC Layer Transmitter and Receiver has been performed using Xilinx Synthesis Tool. Wi-Fi allows LANs (Local Area Networks) to be deployed without cabling for client devices, typically reducing the costs of network deployment and expansion. In addition to restricted use in homes and offices, Wi-Fi can make access publicly available at Wi-Fi hotspots provided either free of charge or to subscribers to various providers.

References

[1]. Douglas A. Pucknell, Kamran Eshraghian, *Basic VLSI Design*, Prentice Hall, 3rd Edition, Jan. 1995.

[2]. W. Fletcher, *An Engineering approach to Digital Design*, Prentice Hall, 1st edition, Feb. 19, 1997.
[3]. William Stallings, Data and Computer Communications, Prentice Hall, 8th edition, Aug. 12, 2006.
[4]. Andrew S. Tannenbaum, *Computer Networks*, Prentice Hall, Nov. 1985.
[5]. Michael John Sebastian Smith, *Application-specific Integrated Circuits*, Addison-Wesley Professional, Jun. 20, 1997.
[6]. URL: www.digitalcoredesign.org

Biographies

Srihari Nannapaneni was a master student in Department of Electrical Engineering, University of Bridgeport, USA. His research areas include VLSI, Computer Architecture and wireless communications.

Dr. Xingguo Xiong is an assistant professor in Department of Electrical and Computer Engineering, University of Bridgeport, CT. He received his Ph.D degree in electrical engineering from Shanghai Institute of Microsystem and Information Technology, China, in 1999. He received his second Ph.D degree in computer engineering from University of Cincinnati, OH, USA in 2005. His research interests include microelectromechanical system (MEMS), nanotechnology, as well as VLSI design and testing.

Dr. Navarun Gupta is an assistant professor in Department of Electrical and Computer Engineering, University of Bridgeport, CT. He obtained his MS in Electrical Engineering at Mercer University in Atlanta in 1998. He received his Ph.D. in Electrical Engineering at Florida International University in 2003. His current research interests include audio signal processing, bio-signal processing, signal processing in Astronomy.