

Design and Implementation of MAC Layer of WiFiRe protocol

Dissertation

submitted in partial fulfillment of the requirements
for the degree of

Master of Technology

by

H Shravan Kumar

(Roll no. 05329018)

under the guidance of

Prof. Sridhar Iyer

and

Prof. Anirudha Sahoo



Department of Computer Science & Engineering (KReSIT)

Indian Institute of Technology Bombay

2007

Dissertation Approval Sheet

This is to certify that the dissertation entitled
**Design and Implementation of MAC layer of WiFiRe
protocol**

by

H Shravan Kumar

(Roll no. 05329018)

is approved for the degree of **Master of Technology**.

Prof. Sridhar Iyer

(Supervisor)

Prof. Anirudha Sahoo

(Co-Supervisor)

Prof. Purushottam Kulkarni

(Internal Examiner)

Dr. Vijay T Raisinghani

(External Examiner)

Prof. V M Gadre

(Chairperson)

Date: _____

Place: _____

INDIAN INSTITUTE OF TECHNOLOGY BOMBAY

CERTIFICATE OF COURSE WORK

This is to certify that **Mr. H Shравan Kumar** was admitted to the candidacy of the M.Tech. Degree and has successfully completed all the courses required for the M.Tech. Programme. The details of the course work done are given below.

Sr.No.	Course No.	Course Name	Credits
Semester 1 (Jul – Nov 2005)			
1.	HS699	Communication and Presentation Skills (P/NP)	4
2.	IT601	Mobile Computing	6
3.	IT605	Computer Networks	6
4.	IT619	IT Foundation Lab	8
5.	IT623	Foundation course of IT - Part II	6
6.	IT653	Network Security	6
Semester 2 (Jan – Apr 2006)			
7.	CS640	Formal Language and Models for Natural Computing	6
8.	HS700	Applied Economics	6
9.	IT628	Information Technology Project Management	6
10.	IT680	Systems Lab.	6
11.	IT694	Seminar	4
Semester 3 (Jul – Nov 2006)			
12.	CS601	Algorithms and Complexity	6
13.	IT625	ICT for Developing Countries	6
M.Tech. Project			
14.	IT696	M.Tech. Project Stage - I (Jul 2006)	18
15.	IT697	M.Tech. Project Stage - II (Jan 2007)	30
16.	IT698	M.Tech. Project Stage - III (Jul 2007)	42

I.I.T. Bombay

Dy. Registrar(Academic)

Dated:

Acknowledgements

I take this opportunity to express my sincere gratitude for **Prof. Sridhar Iyer** for his constant support and encouragement. His excellent and invaluable guidance has been instrumental in making this project work a success.

I would like to thank **Prof. Anirudha Sahoo** for his constant guidance and invaluable support throughout the project.

I would like to thank **Sameer Kurkure** for his invaluable support and for his helpful discussions through out my project. I would also like to thank my colleagues **Janak, Ranjith, Sudheer** and **Venkat** for helpful discussions through out my project, **Kushal, Anuj** for being supportive friends and the KReSIT department for providing me world class computing infrastructure.

I would also like to thank my **family** and **friends** especially the entire **MTech Batch**, who have been a source of encouragement and inspiration throughout the duration of the project.

Last but not the least, I would like to thank the entire KReSIT family for making my stay at IIT Bombay a memorable one.

H.Shravan Kumar

I. I. T. Bombay

July 16th, 2007

Abstract

WiFiRe (Wireless Fidelity Rural Extension) is an extension of the existing WiFi (802.11) protocol. The main aim of WiFiRe is to provide long range communications with high bandwidth, with low cost and easy availability of the chipsets. It mainly replaces the MAC mechanisms of existing WiFi (802.11b) so that it can be used for long range communication for about 15 – 20km, in contrast to existing technology which can support only upto a few hundreds of meters. It continues to use the existing Physical layer of WiFi (802.11b). WiFiRe MAC has many of the features similar to WiMAX (802.16).

WiFiRe provides long range communication by dividing the whole area into sectors, each sector having one Base Station (BS), which is a sectorized antenna. At each Subscriber Terminal (ST), a directional antenna is used to connect ST to BS. WiFiRe uses only one channel for both uplink and downlink, in which each sector is allocated slots based on Time Division Multiplexing-Multi-sector TDM(TDM-MSTDM) mechanism.

In this report we have designed and implemented the WiFiRe protocol and emulated in over a LAN. Problems associated with design and implementation and their plausible solutions are covered as a part of this report. Additionally, it also comprises of sequence diagrams, flow diagrams and state diagrams of working components of *WiFiRe*. We have emulated the protocol using C sockets and this report covers the details of the same. This report also contains how the slots are being scheduled to STs by BS.

Contents

Acknowledgements	vii
Abstract	ix
List of figures	xv
Abbreviations	xvii
1 Introduction and Motivation	1
1.1 Basic overview of <i>WiFiRe</i> protocol	2
1.2 Problem Statement	4
1.3 Thesis Outline	5
2 Literature Survey	7
2.1 WiFi(802.11b)	7
2.1.1 802.11 Reference Model	8
2.1.2 802.11 MAC	8
2.1.3 802.11 PHY	8
2.1.4 Pros and Cons	10
2.2 WiMAX(802.16d)	10
2.2.1 WiMAX MAC and PHY	11
2.2.2 MAC Layer Overview	12
2.2.3 Network Entry and Initialization	12
2.2.4 Request and Grant Services	13
2.2.5 Pros and Cons	13
2.3 Digital Gangetic Plains (DGP)	14

3	<i>WiFiRe</i> Protocol	15
3.1	WiFiRe: Wireless Broadband Access for Rural Areas	15
3.2	MAC Overview	17
3.2.1	Network Initialization	18
3.2.2	Ranging	18
3.2.3	Registration	18
3.2.4	Connection Management	19
3.2.5	Bandwidth Request Grant Service	19
4	Implementation Details	21
4.1	Design Phase	21
4.1.1	Ranging	22
4.1.2	Registration	22
4.2	Beacon and MAC Management Packets	23
4.2.1	Frame Structure of the MAC	24
4.2.2	Construction	26
4.3	LAN Emulation	28
4.3.1	What is LAN Emulation?	28
4.3.2	Why Emulation on LAN?	29
4.3.3	What we have achieved by Emulating on LAN	29
4.4	Memory Management	29
4.4.1	Fast Sockets	29
4.5	Modifications done in LAN Emulation	31
4.6	Scheduling	32
4.6.1	Round Robin Scheduling	33
4.6.2	Smoothed Round Robin Scheduling (SRR)	33
4.6.3	How did we implement it?	35
4.7	Framing Concepts	37
4.8	Real System Architecture	39
4.9	Implementation Issues and Surprises	41
4.10	Modifications in Draft	42

5	Conclusion and Future Work	43
5.1	Conclusion	43
5.2	Future Work	43
	Bibliography	45

List of Figures

1.1	WiFiRe Topology aadaptedfrom [1]	3
1.2	Basic communication sequence diagram	4
2.1	WiFi MAC and PHY Layer adapted from [2]	9
2.2	WiMAX MAC and PHY layers adapted from [3]	12
3.1	WiFiRe overview along with External world connections adapted from [1] .	16
3.2	Timing Sequence adapated from [1]	16
3.3	MAC Over PHY adapted from [1]	17
4.1	Ranging at ST	22
4.2	Registration at ST	23
4.3	MAC PDU Format	24
4.4	Generic MAC header	25
4.5	CID Format	25
4.6	Beacon header	26
4.7	Beacon Message	27
4.8	Overview of LAN emulation	28
4.9	Steps that were emulated on LAN	30
4.10	Tables maintained at BS	36
4.11	Allocation of Slots in a frame	38
4.12	Real System Components	40

Abbreviations and Notations

Abbreviations

BS	: Base Station
BWA	: Broadband Wireless Access
CID	: Connection Identifier
CRC	: Cyclic Redundancy Check
CSMA	: Carrier Sense Multiple Access
DCF	: Distribution Coordination Function
DL	: Downlink
DLMAP	: Downlink Allocation Map
FDM	: Frequency Division Multiplexing
GPC	: Grant Per Connection
GPSF	: Grant Per Service Flow
GPST	: Grant Per Subscriber Terminal
ID	: Identifier
IFS	: Internet Frame Space
LLC	: Logical Link Control
MAC	: Multi Access Control Layer
nrtPS	: non real-time Polling Service
QoS	: Quality of Service
rtPS	: real-time Polling Service
S	: System
SAP	: Service Access Point
SDU	: Service Data Unit
ST	: Subscriber Terminal

- TDD : Time Division Duplex
- TDM : Time Division Multiplex
- TDMA : Time Division Multiple Access
- UE : User Equipment
- UGS : Unsolicited Grant Service
- UL : Uplink
- ULMAP : Uplink Allocation Map
- VoIP : Voice over IP
- WDM : Wireless Distribution Media
- WiFi : Wireless Fidelity
- WiFiRe : Wireless Fidelity Rural Extension
- WiMAX : Worldwide Interoperability for Microwave Access

Chapter 1

Introduction and Motivation

Nowadays the use of Internet and mobile communication has grown to a large extent that their daily usage has become mandatory. Statistics shows that there are more than 100 million mobile users in India [as of June 10th 2006] [1] which shows its importance in daily routine. Major population in India resides in remote areas where access to basic amenities like telephony, internet, etc., are difficult to provide. Broadband wireless access (BWA) can become the best way to meet escalating business demand for rapid Internet connection and integrated data, voice and video services. BWA can extend fiber optic networks and provide more capacity than cable networks or digital subscriber lines (DSL). But deployment of BWA (*WiMAX*) compatible devices are much complex and costlier.

Rural areas are sparsely populated and the distance between village to village varies in few kilometers, unlike urban areas. Installation of more base stations will probably not solve this problem, which also costs more. Wireless Fidelity - Rural Extension (*WiFiRe*) introduces the concept of wireless communication over WiFi IEEE 802.11b physical layer (PHY) and WiMAX IEEE 802.16 MAC layer using low cost chip sets. 802.11b PHY has better availability of low cost chip sets which can operate on unlicensed 2.4 GHz frequency band and WiMAX has potential to work over larger distances of 30 – 40km.

Almost every rural area can avail fixed phone lines, but mobile communication and broadband are difficult to deploy. For this, *WiFiRe* can provide a very good solution. *WiFiRe* uses WiFi PHY which has got a free license band spectrum (IEEE 802.11b, 2.4 GHz Band), the easy availability of WiFi chip sets, and very good QoS features of WiMAX, which makes it suitable to provide long range communications for rural areas. *WiFiRe* uses a star topology network, in which main station (S) will be connected to set of Base Stations (BS) which in turn connected to sectorized antennas through which a Subscriber Terminal (ST) will communicate.

Other approaches to solve the problem such as WiMAX, Optical Networks, DSL etc. are not cost effective and do not provide affordable services to rural environment. The concept of *WiFiRe* seems to be good solution for this scenario and can satisfy bandwidth need at proper price that suits rural people. This protocol is combined effort of IIT Bombay (for the MAC part of [1]), IIT Madras (for the PHY of [1]), IISc Bangalore (for the Scheduler Part of [1]), and CeWIT organization.

1.1 Basic overview of *WiFiRe* protocol

The basic design of WiFiRe comprises of a single operator Station (S) which have licensed bandwidth like dedicated lines, fiber PoP etc. This operator provides the communication base for the outside world to rural environment. The total area is being sectorized and each sector will be having Base Station (BS), which is a sectorized antenna of height around 40m that lies near point of presence (PoP). BS are arranged such that they can simultaneously able to transmit or receive within the sectors. There are Subscriber Terminals (ST) situated at the villages which have 10 – 12m directional antennas. Both BS and ST are fixed whereas users within ST (e.g. building, house, small campus etc) can be either fixed or mobile, depending upon the internal network being used.

These are the basic points for the villages from where people will be able to communicate with the outer world. These STs should be at a minimum height of 10m so as to maintain a system gain of 150dB. Users may connect to these STs using wired or wireless means of communication. The system will be configured as a star topology. The network topology will be as shown in the Figure 1.1.[1]

Each BS can cover up to 15 – 20km range, covering around 100 villages. Each BS will be responsible for all the communication that takes place in its sector range. Each ST will be connected to voice and data terminals in the village by a local area network. As mentioned earlier these ST will be directional and will be connected to corresponding BS covering the sector, thus providing reliable data transfer. Chances of interference with the other transceivers can be solved by locking up ST with the BS with highest signal strength. BSs in the system (S) are configured to operate alternately or diagonally opposite BS for non-overlapping transmission. WiFiRe supports time division duplex (TDD) over single channel with multi-sector TDM (MSTDM) mechanism, which supports

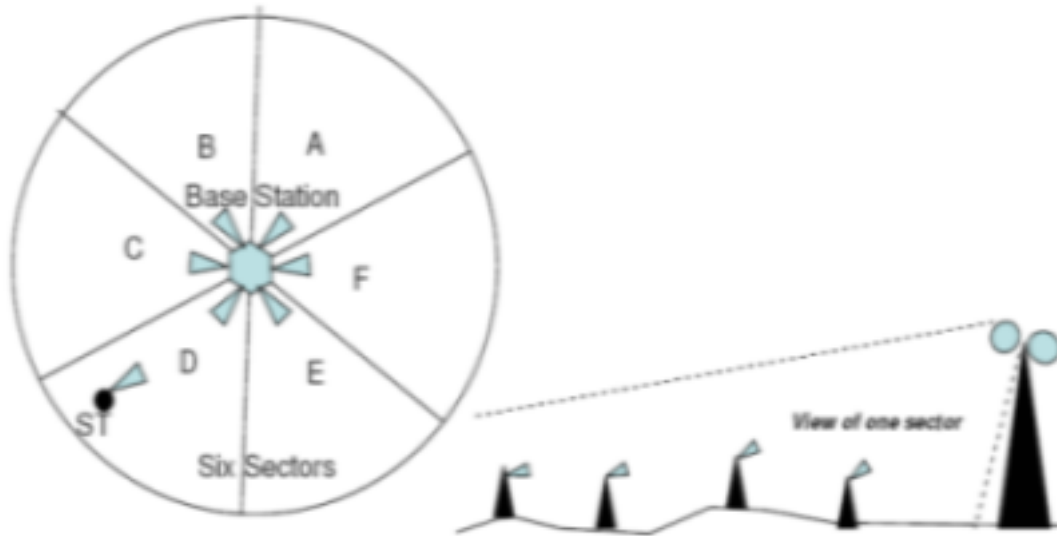


Figure 1.1: WiFiRe Topology aadaptedfrom [1]

about 25 Mbps (for both uplink and downlink) for a cell. In TDD, the uplink (ST to BS) and downlink (BS to ST) share the same frequency but are activated at different time. BS and ST operate in synchronization with each other. Time is divided into frames, which are further divided into DownLink (DL) and UpLink (UL) segments, which may not be of equal time intervals. In each DL slot zero or one transmissions can take place in each sector. Multiple BS antennas can transmit simultaneously provided they do so in a non-interfering manner.

Figure 1.2 is sequence diagram for basic working of WiFiRe protocol till registration. Beacons are being transmitted at the start of each DL segment, which contains information for time synchronization of the STs in that sector, information regarding the DL and UL slots allocations (which are called DL and UL maps respectively) for that frame, and other control information. These DL and UL maps are computed online because there may be site dependent or installation dependent losses and different time varying requirements at each point of time.

The basic assumptions for working for WiFiRe protocol are stated as:

- Wireless links in the system are fixed, single hop, with a star topology. Mobility and multi-hop wireless links are not considered.
- Fixed carrier frequency and WiFi radios operating at 11Mbps, except PHY operat-

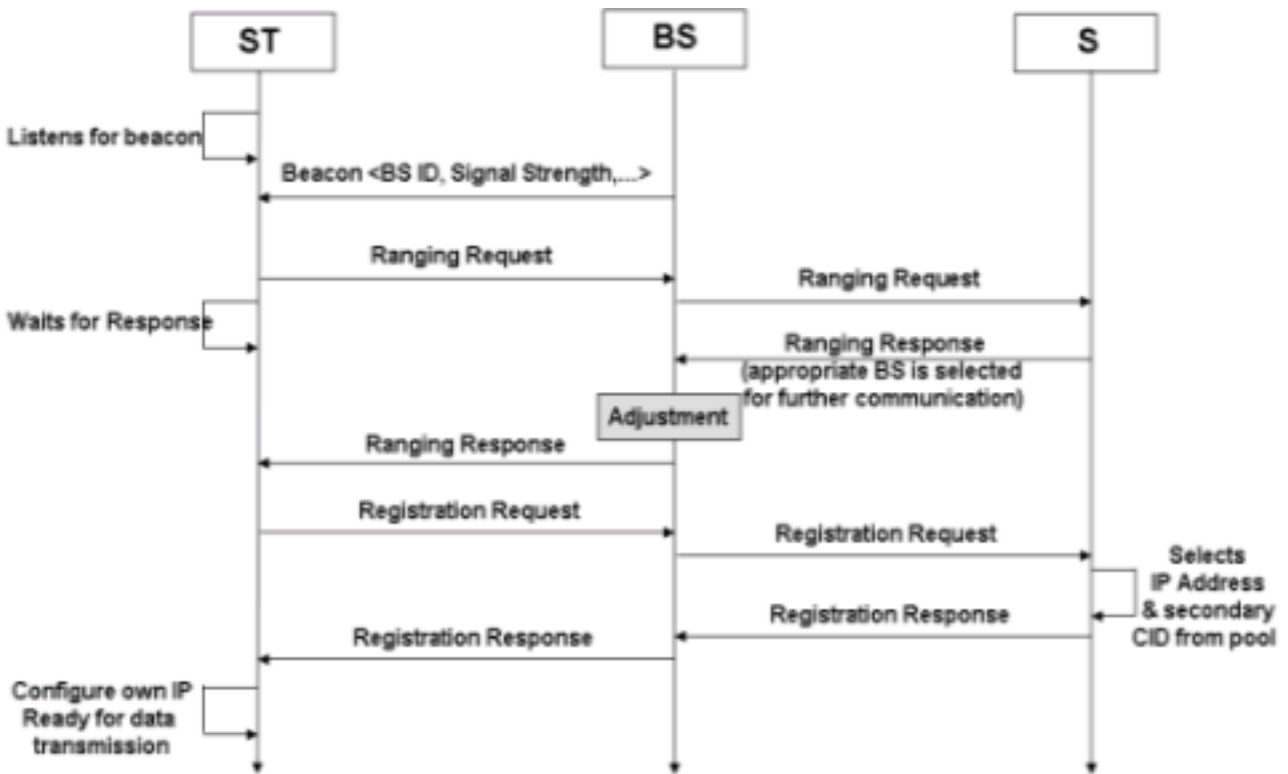


Figure 1.2: Basic communication sequence diagram

ing at 1 or 2 Mbps.

- Various components in the system will be having unique IP addresses.
- About 20MHz(1 carrier) of conditionally licensed spectrum is available for niche or rural areas.
- All nodes in the system are operated by a single operator who owns the conditional license.
- The availability of unlicensed or free spectrum in the 2.4GHz band.
- The existence of point of presence (PoP) every 25km or so, for backbone connectivity.

1.2 Problem Statement

Our problem focuses on implementing the MAC layer of the protocol, which primarily focuses on the basic communication between BS and ST. Our part includes the following steps

Beacon Transmission : Broadcasting beacon to all the ST of a sector which is being implemented by the concept of multi-unicast.

Ranging : Synchronizing clock and other physical layer parameters with respect to the System S is done. It is also performed periodically so that ST will keep in-sync with S. Here the ST will be given Basic and Primary Connection Identifiers(CID) by which the further communication between BS and ST take place. Detailed explanation is given in the following Design section.

Registration : This step ensures that the ST can establish a connection for data exchange as registered ST known to BS. This step is mandatory before any actual data transfer between ST and BS. Here operational parameters and capabilities are exchanged. After this step a IP is being assigned to the ST by BS. Detailed explanation is given in the following Design section.

Data Connection Creation : In this phase, control packet requesting for data connection (DSA) is sent by ST to BS for initiating actual data exchange. BS will assign a data CID to ST for further data communication which informs the nature of the bandwidth request service to be used with the connection.

QoS Management : It allows the existing CIDsto change the nature of the bandwidth allocation or for a new CID which does not have any specified/allocated bandwidth resource. This feature is currently not implemented as part of demonstration.

Data Connection Termination : In this phase the entity (BS or ST) which wants to terminate a data connection exchanges a management message to inform the peer entity.

Our task is to implement these steps and emulate the WiFiRe protocol over Ethernet LAN.

1.3 Thesis Outline

The major contributions of this work are :

- Design of the flow diagrams of ranging and registration process at ST.

- Emulation of the MAC layer of the protocol using C sockets, Signal handling, and Multi threading.
- Implementing the MAC management and scheduler for the system.
- A demonstration of the implemented MAC on a test bed to prove effectiveness of the approach.

In this thesis, chapter 2 discusses existing schemes for broadband access. It also discusses why they are not that much effective considering our rural Indian scenario.

In chapter 3, we present the details of the protocol, we then discuss about how we have gone about implementing the protocol in chapter 4. Finally we present conclusions and future work in chapter 5

Chapter 2

Literature Survey

In this chapter, we discuss work related to the WiFiRe protocol, the other alternative technologies such as WiMAX-d(802.16d), WiFi(802.11b), and Digital Gangetic Plain Project (DGP). First we will discuss the alternative technologies and their pros and cons. Then we will discuss WiFiRe in detail in next chapter. In India, where the telecom infrastructure is poor and last-mile connections are typically through copper cable, DSL and fiber optic, installation costs are high as it requires ripping up streets to lay cables. The ability to provide these connections without laying wire or cable in the ground, greatly lowers the cost of providing these services. This is why WiFiRe is an attractive alternative for providing broadband services in rural India. In developing countries that lack a well-developed wired infrastructure, WiFiRe offers a way to extend broadband Internet service to many different parts of the country. WiFiRe could thus bring broadband access into the homes and businesses of millions of people in rural areas.

2.1 WiFi(802.11b)

WiFi(802.11) stands for Wireless Fidelity, which is a standard protocol for Wireless communication. Except for 802.11a, which operates at 5 GHz, WiFi uses the spectrum near 2.4 GHz, which is standardized and unlicensed by international agreement, although the exact frequency allocations vary slightly in different parts of the world, as does maximum permitted power. This information is taken from [2]. 802.11b has a maximum raw data rate of 11 Mbps and uses the same CSMA/CA media access method defined in the original standard of 802.11. 802.11b is usually used in a point-to-multi point configuration, wherein an access point communicates via an omni-directional antenna with one or more clients that are located in a coverage area around the access point. Typical

indoor range is 30 m (100 ft) at 11 Mbps and 90 m (300 ft) at 1 Mbps. With high-gain external antennas, the protocol can also be used in mixed point-to-point arrangements, typically at ranges up to 8 kilometers(5 miles). 802.11 defines two different modes of operations: Infrastructure (based on AP) and ad-hoc(Independent Basic Service Set, IBSS). Infrastructure mode is a central administration that handles station authentication and association with the network. Multiple APs connected by a Distribution System(DS) can extend the range of wireless network to much more than what can be covered by any single AP. Wireless clients uses AP to access wired resources and Internet. The major advantage of this mode is that the link efficiency is good as AP controls and distributes the channel access to the clients. In Ad-hoc mode, wireless clients communicate directly with each other without the use of a wireless AP or central administrator. Because ad-hoc networks are more flexible and do not require a central administrator, they are more suitable for mesh networking. It facilitates frequency switching where different links connecting the same node can operate in different channels simultaneously. But efficiency of channel is very less compared to the AP mode, this is because of contention based technique. [4]

2.1.1 802.11 Reference Model

The standard presents the architectural view, emphasizing the separation of the system into two major parts: MAC and PHY. Figure 2.1 gives the architectural view.

2.1.2 802.11 MAC

The basic access method in this is the Distributed Coordination Function (DCF), which is a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The other method which can be used for accessing is Point Coordination Function (PCF), which uses polling technique to select which station to transmit.

2.1.3 802.11 PHY

Depending on the current infrastructure and the distance between the sender and receiver of 802.11b, system offers 11, 5.5, 2 or 1 Mbps. Maximum user data rate is approximately 6Mbps. Lowest data rates 1 and 2 Mbps use the 11 bit Barker sequence and DBPSK or DQPSK respectively. The new data rates 5 and 11 Mbps use 8-chip

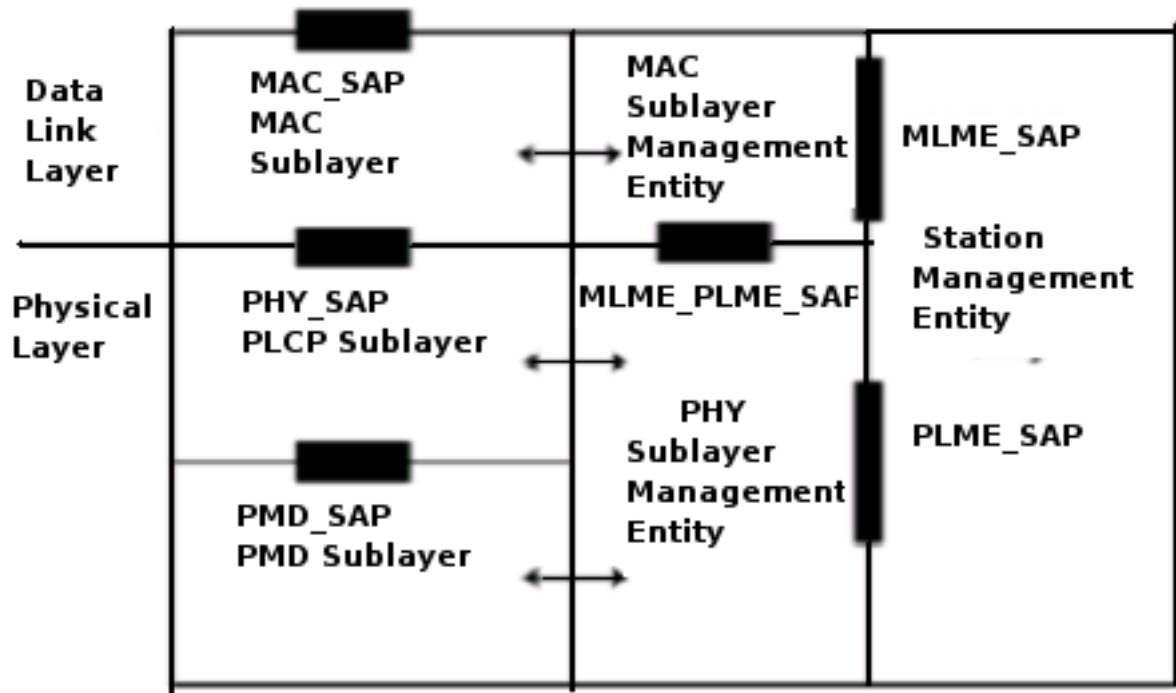


Figure 2.1: WiFi MAC and PHY Layer adapted from [2]

complementary code keyring(CCK).

2.1.3.1 Types

There will be three PHY types :

- Frequency Hop Spread Spectrum in 2.4GHz band
- Direct Sequence Spread Spectrum in 2.4GHz band
- Infrared

2.1.3.2 Sub Layers

There are two sub-layers in PHY :

- PLCP Sub-layer: The MAC layer communicates with the Physical Layer Convergence Protocol (PLCP) sub-layer via primitives (a set of instructive commands or fundamental instructions) through a service access point (SAP). When the MAC layer instructs it to do so, the PLCP prepares MAC protocol data units (MPDUs) for transmission. The PLCP minimizes the dependence of the MAC layer on the

PMD sub-layer by mapping MPDUs into a frame format suitable for transmission by the PMD. The PLCP also delivers incoming frames from the wireless medium to the MAC layer.

- PMD Sub-layer : Under the direction of the PLCP, the Physical Medium Dependent (PMD) sub-layer provides transmission and reception of Physical layer data units between two stations via the wireless medium. To provide this service, the PMD interfaces directly with the wireless medium and provides modulation and demodulation of the frame transmissions. The PLCP and PMD sub-layers communicate via primitives, through a SAP, to govern the transmission and reception functions.

2.1.4 Pros and Cons

WiFi is well suited for small distance communications like in Airports, Shopping malls, Restaurants etc. The attraction of WiFi technology is the de-licensing of its spectrum in many countries, including India. In rural areas, where the spectrum is hardly used, WiFi is an attractive option, provided its limitations when used over a wide area are overcome. But there are some disadvantages in using this in long distance communication. A Major problem is its CSMA/CA mechanism. It is designed for short distance wireless communication. DCF function does not provide any QoS guarantees, while PCF is inefficient with large number of nodes. When we use 802.11 to build WAN, the MAC efficiency becomes very poor. One solution for this problem is to replace the MAC protocol with one more suited to wide-area deployment.

2.2 WiMAX(802.16d)

WiMAX is Worldwide Inter-operability for Microwave Access. It is 802.16 Air Interface Standard. For a point-to-multi point (PMP) topology, a controlling base station (BS) connects multiple subscriber stations (SS) to various public networks. The standard defines a connection oriented MAC protocol, and a mechanism for QoS guarantee. WiMAX aims to provide wireless data over long distances, in a variety of different ways, from point to point links to full mobile cellular type access. The IEEE 802.16 media access controller (MAC) is significantly different from that of IEEE 802.11 WiFi MAC. In WiFi,

the MAC uses contention access to all subscriber stations which are wishing to pass data through an access point for the APs attention on a random basis. This can cause distant nodes from the AP to be repeatedly interrupted by less sensitive, closer nodes, greatly reducing their throughput. And this makes services, such as VoIP or IPTV which depend on a determined level of quality of service (QoS), difficult to maintain for large number of users. In contrast, the 802.16 MAC is a scheduling MAC where the subscriber station only has to compete once (for initial entry into the network). After that it is allocated a time slot by the base station. The time slot can enlarge and constrict, but it remains assigned to the subscriber station meaning that other subscribers are not supposed to use it but take their turn. This scheduling algorithm is stable under overload. It is also much more bandwidth efficient. The scheduling algorithm also allows the base station to control Quality of Service by balancing the assignments among the needs of the subscriber stations. WiMAX/802.16's use of OFDMA and scheduled MAC allows wireless mesh networks to be much more robust and reliable. The original WiMAX standard, IEEE 802.16, specifies WiMAX in the 10 to 66 GHz range. 802.16a, updated in 2004 to 802.16-2004, added support for the 2 to 11 GHz range, of which most parts are already unlicensed internationally and only very few still require domestic licenses. Most business interest will probably be in the 802.16-2004 standard, as opposed to licensed frequencies. IEEE 802.16 provides up to 50 km (31 miles) of linear service area range. The technology has been claimed to provide shared data rates up to 70 Mbps. [5]

2.2.1 WiMAX MAC and PHY

It can support multiple communication services (data, voice, video) with different QoS requirements by properly defining scheduler at MAC layer that can control BS and SS data transmissions. The downlink is broadcast-based, as only BS will transmit data and there is no problem of interference. The SS to which the concerned packet is delivered will respond to that packet. While in Uplink BS will be deciding the number of time slots that each SS will be allowed to transmit in the uplink sub-frame. This information is passed through the UL-MAP by the BS.

Figure 2.2 shows the layers of MAC and PHY.

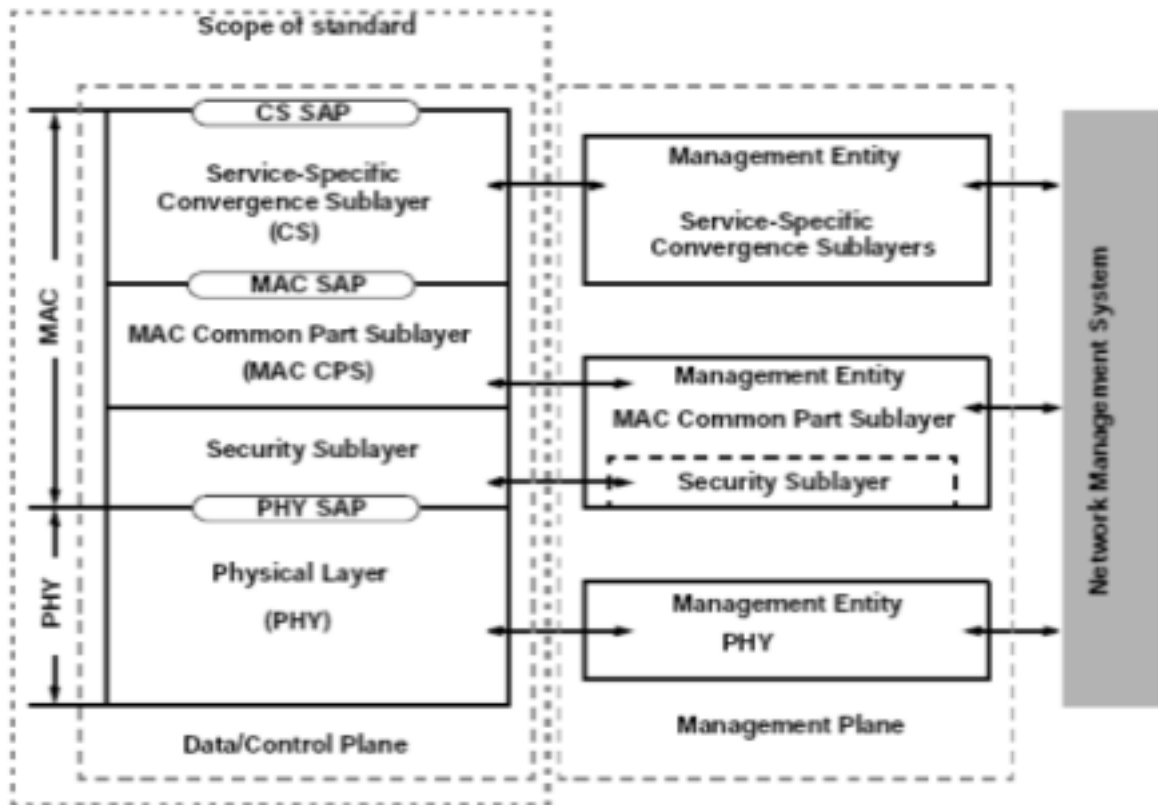


Figure 2.2: WiMAX MAC and PHY layers adapted from [3]

2.2.2 MAC Layer Overview

In this layer, QoS is done by service flow mechanism. It is a connection oriented mechanism, where all purposes of mapping to services on SS's, associating varying levels of QoS, and all data communications will be carried on per connection basis. After completion of registration process SS, connections are associated with these service flows. When a customer needs new service then new connections are established. These connections are needed active maintenance. When the data transfer is complete all connections are terminated.

The BS controls assignments on the uplink channel through the UL-MAP messages and determines which mini-slots are subject to collisions. Collisions may occur during the initial ranging. BS uses a random back-off algorithm to resolve contention.

2.2.3 Network Entry and Initialization

- Scanning the downlink channel and establishing synchronization with the BS.

- Obtaining the transmit parameters (from UCD message).
- Perform ranging process.
- Negotiating basic capabilities.
- Authorization of SS and performing key exchange.
- Performing registration process.
- Establishing the IP connectivity.
- Establishing the time of day.
- Transferring the operational parameters.
- Setting up connections.

2.2.4 Request and Grant Services

SS uses bandwidth request mechanisms to specify uplink bandwidth requirements to BS. There are two modes of transmitting the BW request:

- Contention mode - where SS sends BW-request in contention period.
- Contention free mode (polling) - where BS polls SS, and each SS reply by sending BW-request.

Due to predictable delays, contention-free mode is suitable for real time applications.

There are two modes of granting the bandwidth that is requested by SS

- Grant Per Connection (GPC) - explicitly grants for each connection
- Grant Per Subscriber Station (GPSS) - all connections from a single SS are treated as a single unit and bandwidth is allocated accordingly. An additional scheduler in SS determines in which order the service is being granted slot.

2.2.5 Pros and Cons

The main advantage of WiMAX is that it can transmit data at higher data rate. This is also one good alternative to deploy in rural areas. But only one problem is high cost for its broadband service. These high costs are not affordable to people in rural areas.

2.3 Digital Gangetic Plains (DGP)

DGP main goal is to enable low cost and rapid deployment of portable/mobile voice and data communication services in rural areas. Although 802.11 was primarily designed for indoor operation, but due to its low cost they tried to use this for extending its usage for long range communications. It is a 802.11 based Mesh Network, where it doesn't use the existing CSMA/CA technology in 802.11, instead it uses 2-phase TDMA based protocol. But the problem with the current approach is MAC of 802.11b standard. 802.11b doesn't provide any QoS mechanism except PCF. The DGP test bed has been built with the following three goals.

- *Quantify 802.11 performance outdoors:* To conduct signal coverage and performance experiments under a variety of outdoor channel conditions, build empirical path loss models for outdoor 2.4GHz channels, understand link performance under different channel conditions and under adjacent/co-channel interference.
- *Range extension:* To test 802.11 radios beyond the prescribed limits by mounting radio transmitters and receivers on top of tall towers, and by joining multiple point-to-point links.
- *Cost reduction:* To experiment with techniques which can reduce overall system cost through judicious choice of antennae, cable length, tower height, etc., and through better network planning and engineering.

The outdoor long-distance use of 802.11 requires a revisit to the protocols at various layers of the OSI stack, as well as various system design issues. This project is the main basis for our project to show that we can change the MAC layer of 802.11 by keeping the same PHY chipset. In this project they have changed the MAC layer of 802.11 so that it works like a router. They have configured the network as a mesh network. Main disadvantages of this project include the fact that it is not ad-hoc, more computation power needed at each access point as each act as a router, and it doesn't provide any QoS guarantee [6].

Chapter 3

WiFiRe Protocol

In this chapter, we are discuss the WiFiRe protocol in detail and its related concepts of WiFi PHY and WiMAX MAC layer.

3.1 WiFiRe: Wireless Broadband Access for Rural Areas

WiFiRe stands for Wireless Fidelity-Rural extension. It has been proposed to provide rural communication with low cost hardware and network operations. WiFiRe is an extension to the existing WiFi protocol. It uses the WiFi(802.11b) PHY layer because of its low cost and easy availability, but changes the MAC layer to support longer range. It also avoids the frequency licensing costs by operating in the unlicensed 2.4 frequency band. WiFiRe uses most of the concepts of WiMAX MAC layer as there are very good QoS features of MAC.

The overview of the basic WiFiRe system when connected to the outside environment will look like the Figure 3.1.

Figure 3.2 shows how a WiFiRe frame is divided. A typical WiFiRe frame consists of beacon transmission, downlink and uplink slots. Beacons are transmitted periodically. Downlink slots are the one which are used by BS to transmit data to STs through broadcast, where are uplink slots are being used by STs to send data to BS.

Beacons are being transmitted at the start of each DL segment, which contains information for time synchronization of the ST(s) in that sector, information regarding the DL and UL slots allocations (which are called DL and UL maps respectively) for that frame, and other control information. These DL and UL maps are computed online because there may be site dependent or installation dependent losses and different time varying

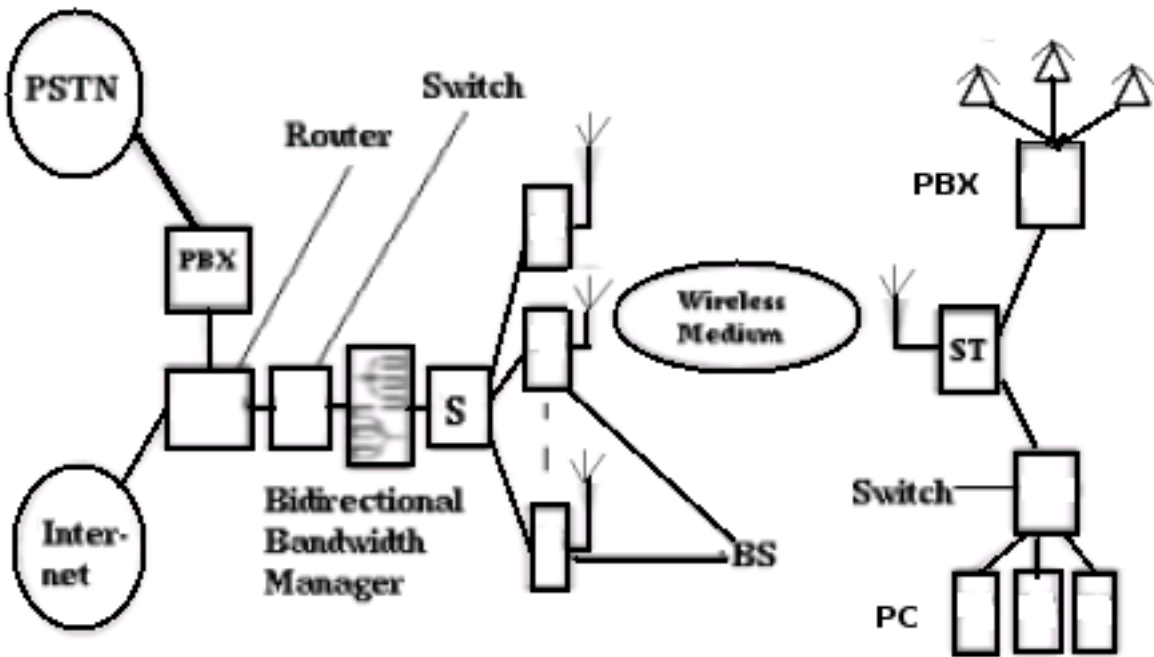


Figure 3.1: WiFiRe overview along with External world connections adapted from [1]

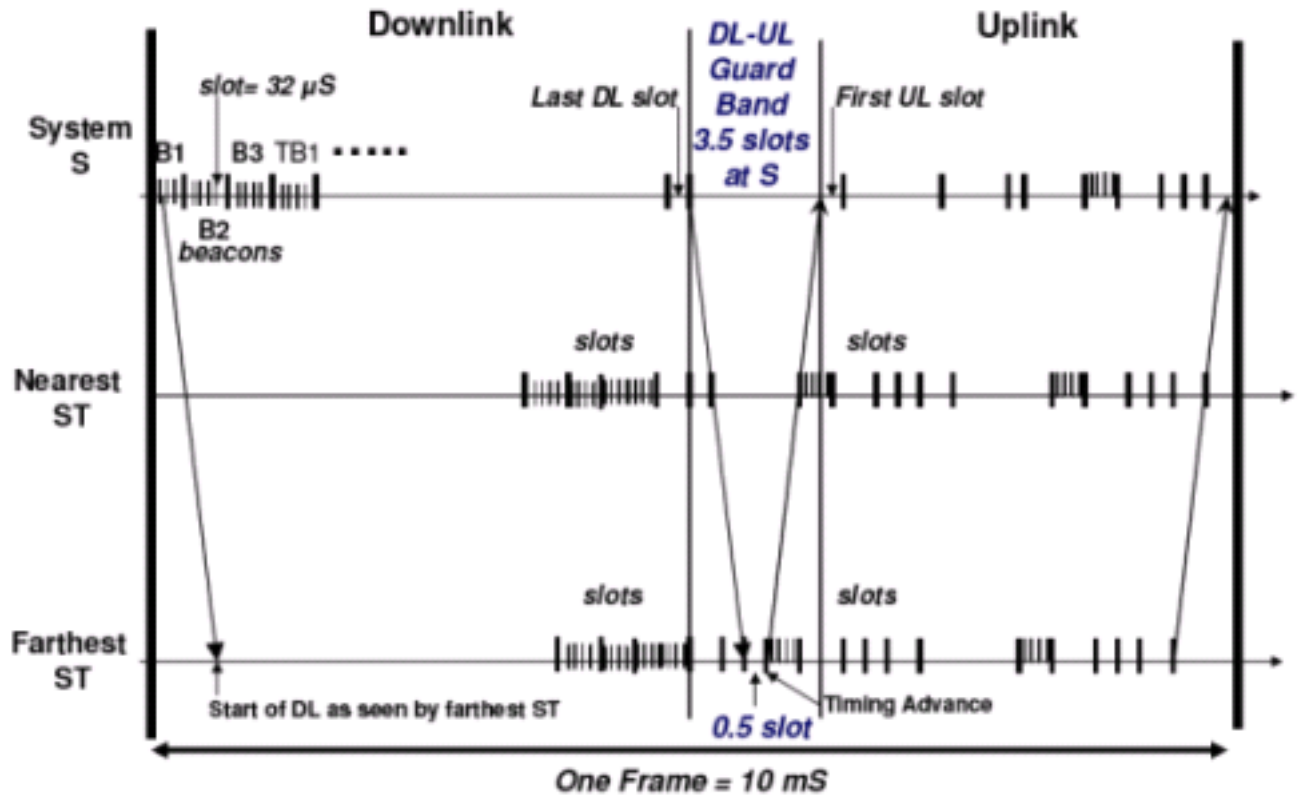


Figure 3.2: Timing Sequence adapted from [1]

requirements at each point of time.

3.2 MAC Overview

The following section describes how the MAC protocol is designed and how it works.

Each BS antenna is controlled by an IEEE 802.11b PHY. MAC layer will be on the top of all the BS's. Each BS can be distinguished separately by MAC, a single MAC controls more than one PHY, as shown in the Figure 3.3 and is responsible for transmitting MAC packets while resolving the collisions. These packet transmission can be done in serial or in parallel.

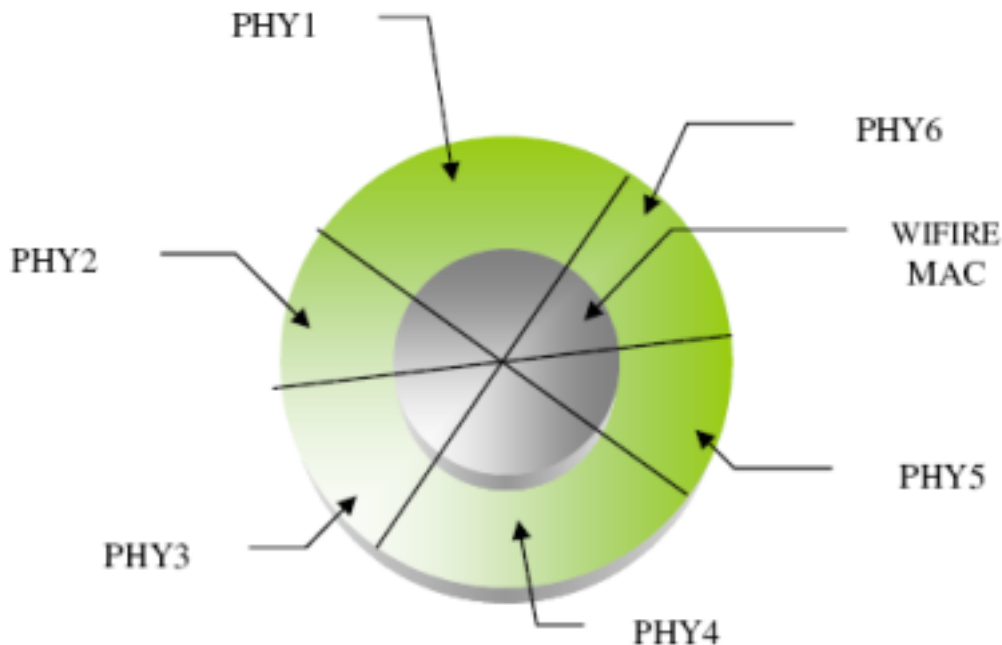


Figure 3.3: MAC Over PHY adapted from [1]

The BS's which are neighbors cannot transmit simultaneously because there is chance of interference between the ST's while receiving. So the BS's which are in opposite to each other can send simultaneously (based on the Figure 3.3). The MAC will be following TDD-MSTDM mechanism for scheduling of slots. The DL segment begins with each BS in the system transmitting a Beacon packet, in a non-interfering manner. Even though beacons can be transmitted simultaneously they need not be the same. Each beacon will be of the structure (Operator ID, System ID, BS ID, All registered ST(s) scheduled for that frame and there corresponding slot assignments). There is a guard bit of a

few slots between the end of DL segment and the start of UL segment that ensures that it covers the propagation delay.

The MAC is a connection-oriented. A connection defines both the mapping between peer data link processes that utilize the MAC and a service flow. Service flow defines the QoS parameters for Protocol Data Units (PDU's), which is a mechanism which manages uplink and downlink management. ST will request uplink bandwidth on a per connection basis. A system S may grant the request by polling or contention procedures. The operation of the WiFiRe MAC described here is a summary of [1]

3.2.1 Network Initialization

The association between a ST and a System S is static. But deciding on which BS to use for communication is done through ranging and registration. An ST should communicate with only one S.

3.2.2 Ranging

New and Unsynchronized ST's are allowed to range and register. When power-up sequence and self-initialization are done the ST enters the process of *Ranging* in order to synchronize the clock and other physical parameters with the system S. It is also performed periodically to keep in synchronization with S. In this process S assigns ST two connection-ID's (CIDs) called the Primary CID, which is used further for exchange of management services, and the other is Basic CID, which is used further for further periodic ranging requests. After this ranging is completed the next step is to get registered to the network.

3.2.3 Registration

In this process ST informs S that it is entering into its service set. The registration process is required prior to any data connection. The process involves a registration request from the ST, followed by a registration response from S. During this process, ST and S exchange operational parameters and capabilities. This process enables the ST to acquire an IP address to set-up provisioned connections.

3.2.4 Connection Management

After registration, the ST can send requests for any number of further connections. The MAC is connection-oriented and data flow between BS and ST occurs as per the service flow type associated with that particular data flow. A new service can be added, or an existing service can be modified, or a service can be deleted. So the connection management consists of procedures to perform these functions. Later data connections are established on which data is transmitted.

3.2.5 Bandwidth Request Grant Service

The following section describes how the WiFiRe services and gives grants to the requests.

- Types of Services

The following are the services that are given by WiFiRe

- *Unsolicited Grant Service* (UGS) - Designed to support real-time flows that generate fixed size data packets on a periodic basis, such as T1/E1 and Voice over IP Without silence suppression. When a data CID is associated with UGS service flow type, the ST does not have to send periodic bandwidth request to the BS for that connection (data CID). The UGS service offers fixed size grants on a real-time periodic basis, which eliminate the overhead and latency of ST requests and assure that grants are available to meet the flow's real-time needs. The BS shall provide fixed size data grant slots at periodic intervals to the service flow.
- *Real-time Polling Service* (rtPS) - Designed to support real-time flows that generate variable size data packets on a periodic basis, such as MPEG video. The service offers real-time, periodic, unicast request opportunities, which meet the flow's real-time needs and allow the ST to specify the size of the desired grant. This service requires more request overhead than UGS, but supports variable grant sizes for optimum data transport efficiency. The BS shall provide periodic unicast request opportunities, by assigning appropriate polling slots in the uplink.

- *Non Real-time Polling Service* (nrtPS) - The Non-Real-Time Polling Service (nrtPS) is designed to support non real-time flows those require variable size data grant slots on a regular basis, such as high bandwidth FTP. The service offers unicast polls on a regular basis, which assures that the flow receives request opportunities even during network congestion. The BS typically polls nrtPS connections on an interval (periodic or non-periodic). The BS shall provide timely unicast request opportunities by assigning appropriate polling slots in the uplink frame.
 - *Best Effort Service* (BE) - The intent of the Best Effort (BE) service is to provide efficient service to best effort traffic . These flows served by contention slots or whenever there are no other flows.
- Types of Grants

The following are the types of grant bandwidth that are given when requested

- *Grant Per Connection Mode* (GPC)- explicitly grants for each connection.
- *Grant Per Subscriber Terminal Mode* (GPST)- granted collectively to all the connections belonging to a ST.
- *Grant per Service Flow type* (GPSF)- It is intermediate between GPC and GPST, which will be granting as per the flow type.

Chapter 4

Implementation Details

In this chapter we discuss our implementation of the WiFiRe Protocol. The outline of this chapter is as follows.

- Section 4.1 concentrates on the design of the ranging and registration procedures.
- In Section 4.2, we give an overview of how we construct beacons and management packets.
- In Section 4.3, we give an overview of emulation of the protocol on LAN.
- In Section 4.4, we have explained how we have improved the LAN emulation.
- Section 4.6 is about scheduling the packets that arrive at BS.
- Section 4.7 deals with the framing concept which gives the details of how we went about fragmentation and de-fragmentation of the frame if the frame size is large.
- Section 4.8 gives overview of the actual scenario of our test bed where we have implemented the protocol.
- Section 4.9 gives issues that we faced during our implementation.
- Section 4.10 gives some of the modifications or additions that we have suggested to the draft [1].

4.1 Design Phase

We have designed the flow of ranging and registration phases at ST.

4.1.1 Ranging

Ranging is done in order to synchronize clocks and other physical parameters with the system (S). Figure 4.1 gives the overview of ranging procedure done at Subscriber Terminal(ST) at design level. In our emulation over a LAN, there is no need of ranging as the propagation delay is negligible, so we are not using it for synchronization instead we are doing ranging in order to exchange primary and basic cids between ST and BS.

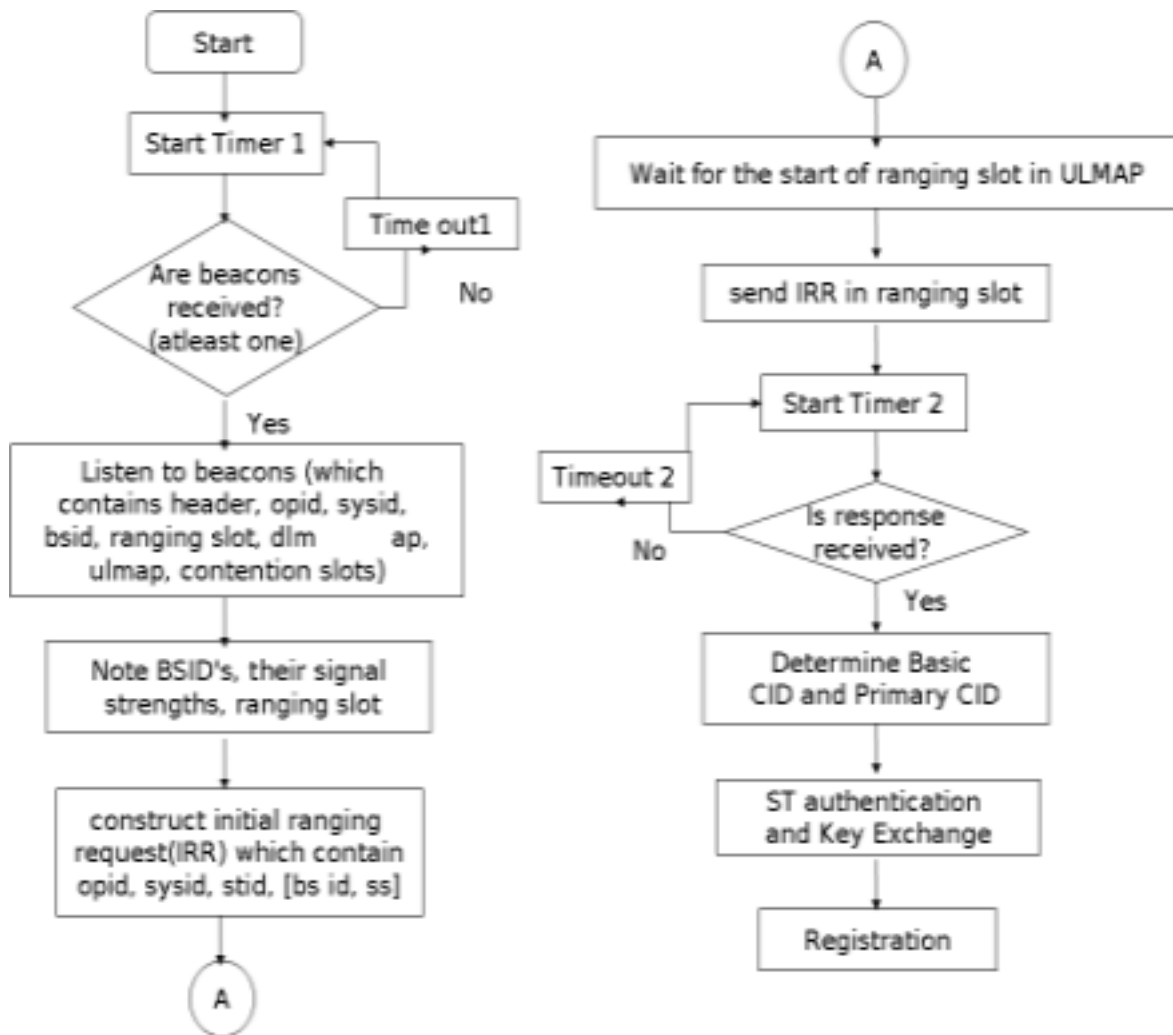


Figure 4.1: Ranging at ST

4.1.2 Registration

Registration happens for getting an IP address, the details of IP version from S, which can be used for further communication. This process involves a Registration request from ST and registration response from S. During this process the operational parameters and

capabilities are exchanged. Figure 4.2 gives the overview of the registration steps that take place at the ST. In this procedure we just use to exchange the IP packets.

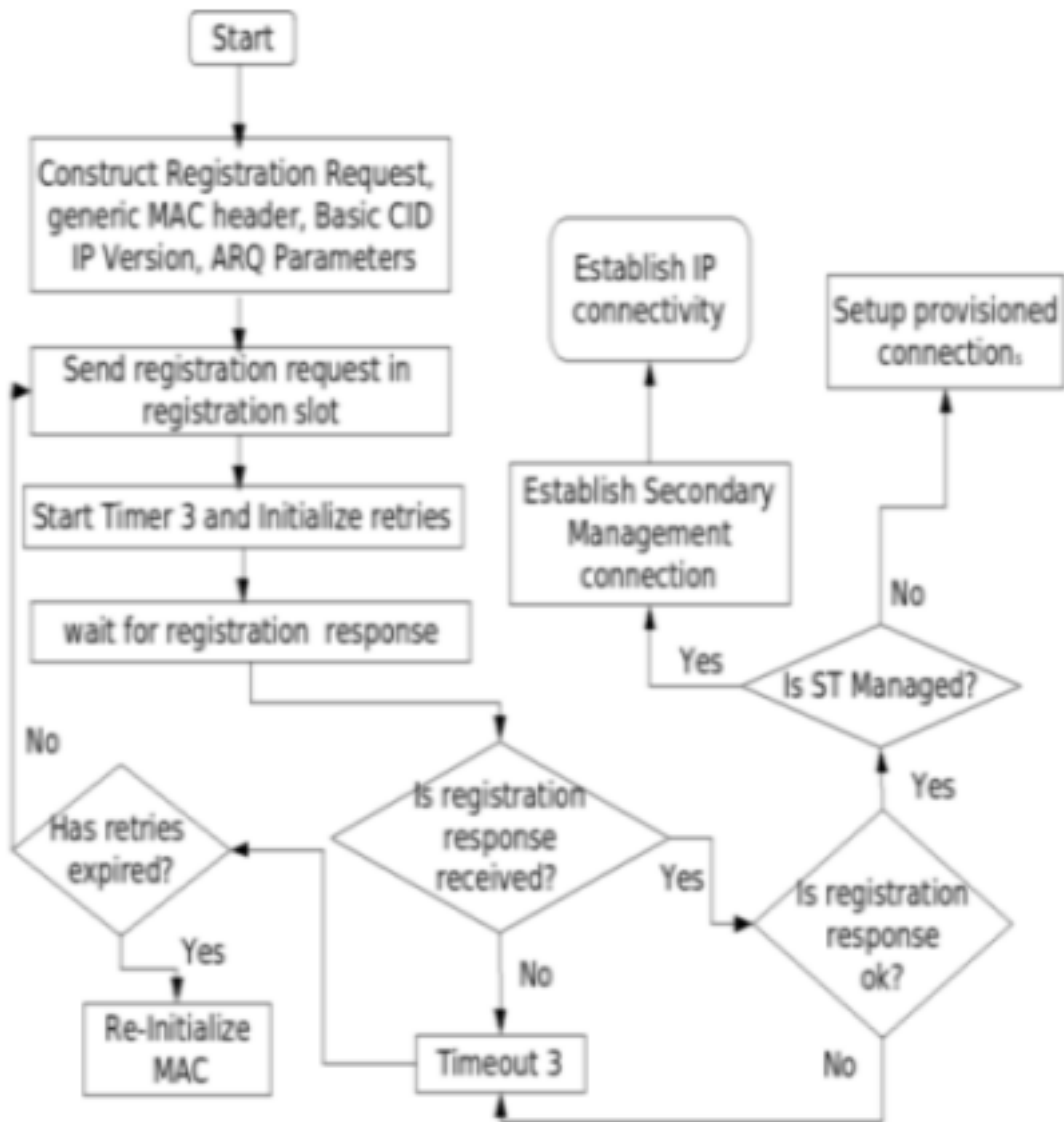


Figure 4.2: Registration at ST

4.2 Beacon and MAC Management Packets

This section gives frame structure of the MAC packets and how they are constructed.

4.2.1 Frame Structure of the MAC

4.2.1.1 MAC PDU Format

The basic structure of MAC PDU is of the form Figure 4.3. Each PDU shall begin with a fixed-length Generic MAC Header. The header may be followed by the Payload of the MAC PDU. If present, the Payload shall consist of zero or more sub-headers and zero or more MAC SDU(s) (Service Data Units). The payload information may vary in length, so that a MAC PDU may represent a variable number of bytes. A MAC PDU may contain a CRC (Cyclic Redundancy Check). The maximum size of a single MAC PDU is bounded by the maximum size payload accepted by the WiFi PHY. Larger MPDU(s) may be fragmented and transmitted.

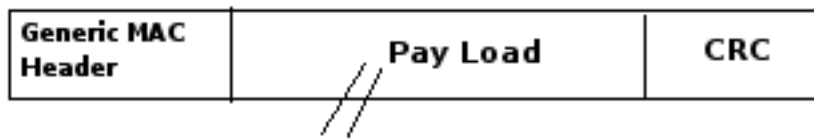


Figure 4.3: MAC PDU Format

4.2.1.2 MAC Header Format

There are two MAC header formats defined in the protocol. They are Generic MAC header and Beacon header. The Generic MAC Header is used for Management and Data PDU(s). The Beacon Header used to transmit a beacon message. The single-bit Header Type (HT) field distinguishes the Generic and Beacon Header formats. The HT field shall be set to zero for the Generic Header and to one for a Beacon Header.

- *Generic MAC Header*: The fields of Generic MAC header are as shown in Figure 4.4.
 - HT is set to 0 for Generic MAC header.
 - Len represents length of the MAC PDU including header length.

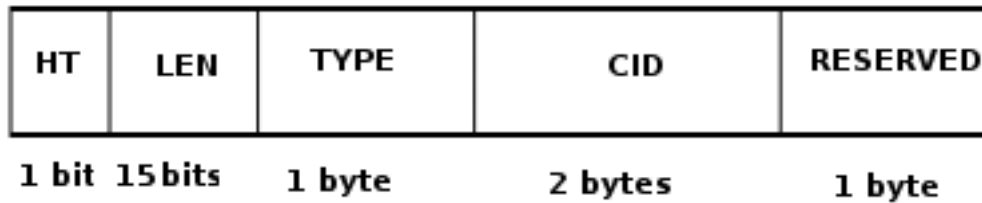


Figure 4.4: Generic MAC header

- CID represents Connection to which the MPDU belongs to. Figure 4.5 shows the basic format of CID. First two bytes represents type of CID: *(00)* for basic CID, which is used by the BS MAC and ST MAC to exchange short, time-urgent MAC management messages, such as ranging; *(01)* for primary CID, which is used by the BS MAC and ST MAC to exchange longer, more delay tolerant MAC management messages, such as creation of data connections; both *10* and *11* represents data CID, which is used by BS MAC and ST MAC to exchange data packets. The reason for having different types of CID(s) is mainly to facilitate the QoS scheduler. In case of Data CID, the next two bits implicitly identify the type of associated service flow: *(00)* for UGS, *(01)* for rtPS, *10* for nrtPS, and *11* for BE.

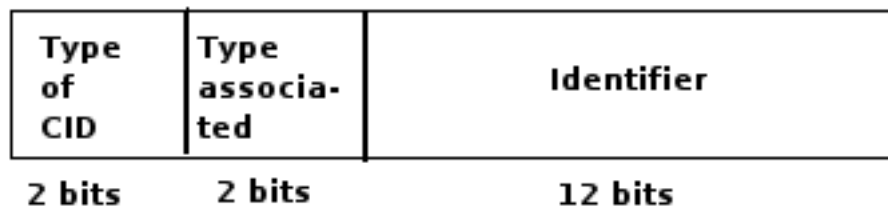


Figure 4.5: CID Format

- Reserved is reserved for future use.
 - Type specifies which type of packet it is. The table 4.1 gives value and its corresponding meaning.
- *Beacon Header*: Figure 4.6 gives list of fields present in beacon header.
 - HT value is 1.



Figure 4.6: Beacon header

- Length represents the length of the beacon including the header length.
- Reserved is kept for future use.

4.2.2 Construction

Construction of beacon requires scheduling of the STs which are up at that particular interval of time in the DL and UL map of the beacon that is going to be transmitted. The typical beacon is as shown in Figure 4.7.

- Opr ID is for identifying the Operator of the network.

Table 4.1: Type field values

<i>Value</i>	<i>Description</i>
0x00	no sub headers present
0x01	sub header present
0x03	Management PDU of type Initial Ranging Request
0x04	Management PDU of type Initial Ranging Request Response
0x05	Management PDU of type Registration Request
0x06	Management PDU of type Registration Response
0x07	Management PDU of type Dynamic Service Addition Request
0x08	Management PDU of type Dynamic Service Addition Response
0x09	Management PDU of type Dynamic Service Change Request
0x10	Management PDU of type Dynamic Service Change Response
0x11	Management PDU of type Dynamic Service Deletion Request
0x12	Management PDU of type Dynamic Service Deletion Response
0x14	MAC PDU with data Payload

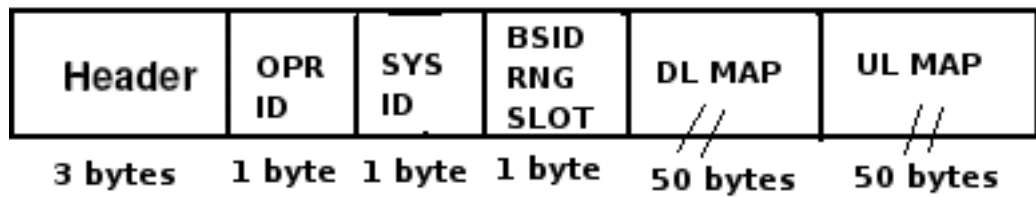


Figure 4.7: Beacon Message

- Sys ID is for identifying the System (S).
- BS ID is a 7 bits value identifying the BS in the System that is transmitting this Beacon.
- RNG Slot is 1 bit which gives whether it is initial ranging or periodic ranging.
- DL-MAP is 50 bytes. It is a 50 element vector of $\langle \text{ST ID} = (1 \text{ byte}) \rangle$. ST ID = 0x11 value implies that the message in the corresponding DL slot is a broadcast message for all ST(s).
- UL-MAP is 50 bytes. It is a 25 element vector of $\langle \text{ST ID} = (1 \text{ byte}), \text{Slot id} = (1 \text{ byte}) \rangle$.

We used round robin scheduling algorithm for scheduling the ST's in the frame, this scheduling concept is explained in detail in Section 4.6. MAC Management packets are created as and when required. Based on the packet received from ST, the BS will send the corresponding reply and at ST, based on the response from the BS, it will create corresponding next packet to be transmitted. Then this packet is transmitted through the network.

4.3 LAN Emulation

This section will give a detailed explanation of how we went about emulating the protocol using LAN, why we have to do this, and what we have achieved by doing this.

4.3.1 What is LAN Emulation?

We have emulated the WiFiRe Protocol using LAN as the basic medium of propagation between ST and BS. Here in emulation WiFiRe MAC layer will be over application layer using C sockets on ethernet LAN where it will construct, process and execute the packets on the WiFiRe MAC and will pass the packet to socket layer assuming it to be the PHY layer of WiFi 802.11. The concept of emulating the protocol on LAN is by using C sockets. The assumption here is that the Application Layer of the Ethernet act as the MAC layer of our protocol and assuming the layers down to it as the PHY. Here the characteristics of PHY layer can be ignored while implementing the MAC layer through C sockets as the device driver will take care of the PHY at lower levels.

Figure 4.8 is the overview of the LAN emulation of the protocol.

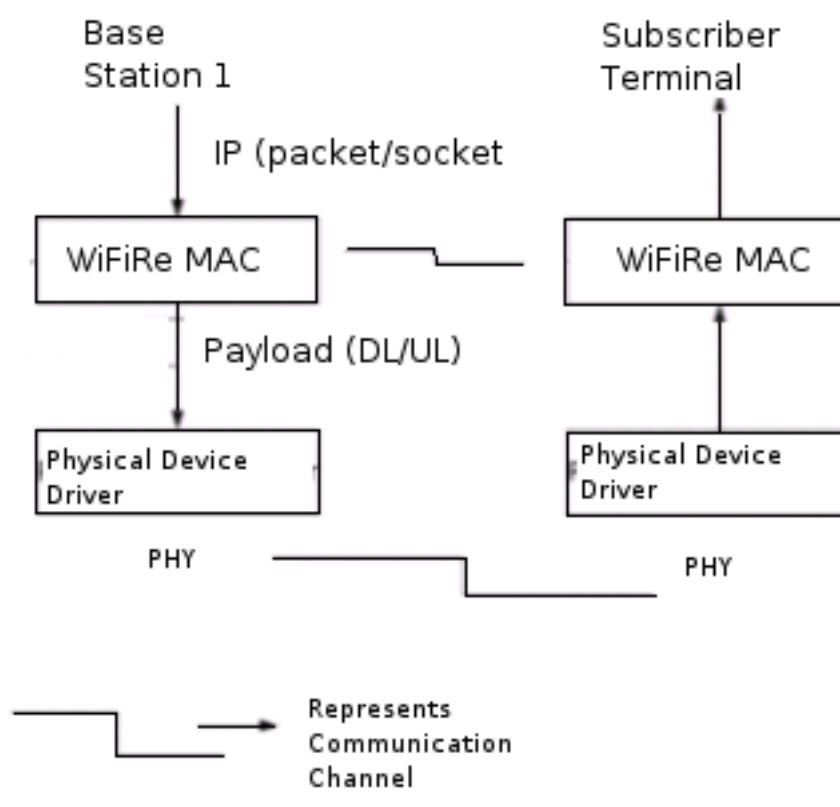


Figure 4.8: Overview of LAN emulation

4.3.2 Why Emulation on LAN?

- To understand and ensure that steps involved in WiFiRe protocol works.
- It is comparatively easy to debug and make changes at the application layer rather than at kernel level.
- WiFiRe hardware is not ready and in order to test the protocol, there is need of already setup network infrastructure which is already setup(i.e. LAN in this case).
- Design and implement data structures and small working modules in order to test and reuse them with minimum changes when implementing the protocol in the kernel level.

4.3.3 What we have achieved by Emulating on LAN

We have shown that the basic protocol steps of WiFiRe are correct. We have emulated Beacon broadcast, Ranging, Registration, Data Service Addition, and Data Connection Termination. Figure 4.9 shows the basic steps that were processed while emulating the protocol.

4.4 Memory Management

This section gives the overview of how we have improved the LAN emulation work further.

4.4.1 Fast Sockets

For high performance in the local area networks fast sockets concept is used. Fast Sockets is an implementation of the Sockets API that provides high-performance communication and inter-operability with existing programs. It yields high-performance communication through a low-overhead protocol layered on top of a low-overhead transport mechanism such as Active Messages, which is an asynchronous communication mechanism intended to expose the full hardware flexibility and performance of modern interconnection networks. Inter-operability with existing programs is obtained by supporting most

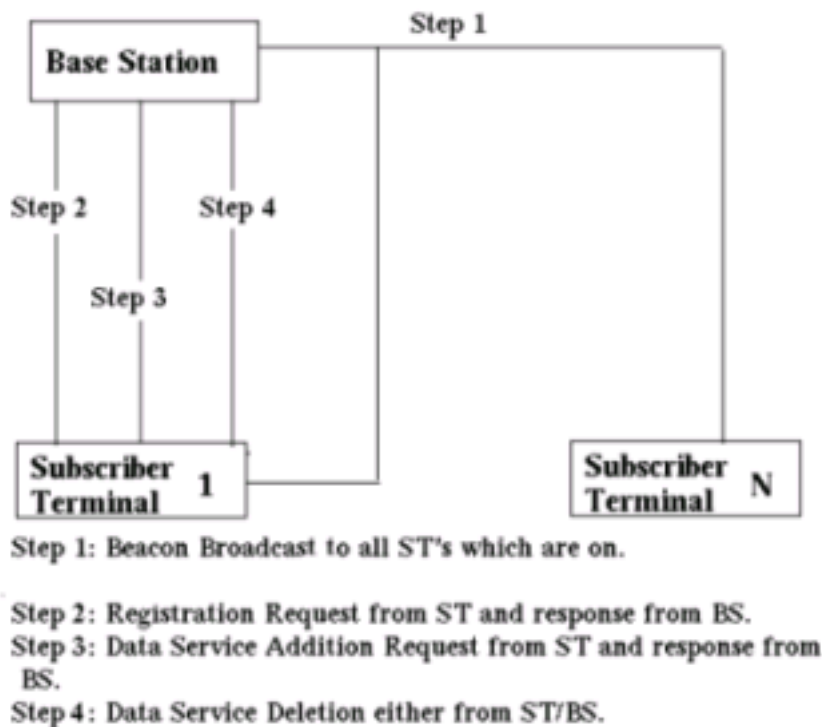


Figure 4.9: Steps that were emulated on LAN

of the Sockets API and transparently using existing protocols for communication with non-Fast Sockets programs [7].

4.4.1.1 Simple Buffer Management

Fast Sockets avoids the complexities of mbuf-style memory management by using a single, contiguous virtual memory buffer for each socket. Data is transferred directly into this buffer via Active Message data transfer messages. The message handler places data sequentially into the buffer to maintain in-order delivery and make data transfer to a user buffer a simple memory copy. The argument words of the data transfer messages carry packet meta data because the argument words are passed separately to the handler, there is no need for the memory management system to strip off packet headers.

Fast Sockets eliminates send buffering. Because many user applications rely heavily on small packets and on request-response behavior, delaying packet transmission only serves to increase user-visible latency. Eliminating send-side buffering reduces protocol overhead because there are no copies on the send side of the protocol path - Active Messages already provides reliability.

A `send()` call transmits the data directly from the user buffer into the network. When it arrives at the remote destination, the message handler places it into the socket buffer, and a subsequent `recv()` call copies it into the user buffer.

4.4.1.2 Problems With Fast Sockets

Although Fast sockets gives better performance but there are a few disadvantages of using them.

- It may consume more memory than the global mbuf pool, which is used in kernel implementations.
- Fast Sockets cannot currently be shared between two processes (for example, via a `fork()` call), and all Fast Sockets state is lost upon an `exec()` or `exit()` call.

4.5 Modifications done in LAN Emulation

We have used dynamic memory allocation for creating packets in our lan emulation. This consumes more cpu cycles. It also creates problems when structure a pointer to a variable in is sent through the network, because the pointer will not contain the actual data, its just an address. Because of these reasons we have replaced the dynamic memory allocation with static buffers and copying data of the structure into those static buffers.

The following code snippet shows how a structure is copied into a buffer. It uses `memcpy()` for copying each and every data type into the buffer.

```
struct wifire_mac_pdu{
    struct wifire_generic_header header;
    char *payload;
}; struct wifire_generic_header{
    unsigned short ht_len;
    unsigned char type;
    unsigned short cid;
    unsigned char reserved;
};
/* Buffer which is going to be sent through socket */
```

```

unsigned char sbuff[MAX_PKT_LEN];
void copy_to_buffer(struct wifire_mac_pdu *mpdu) {
    int bufflen=0;
    memcpy(sbuff,&(mpdu->generic_header.ht_len),
sizeof(unsigned short));
    bufflen = sizeof(unsigned short);
    memcpy(sbuff+bufflen,&(mpdu->generic_header.type),
sizeof(unsigned char));
    bufflen += sizeof(unsigned char);
    memcpy(sbuff+bufflen,&(mpdu->generic_header.cid),
sizeof(unsigned short));
    bufflen += sizeof(unsigned short);
    memcpy(sbuff+bufflen,&(mpdu->generic_header.reserved),
sizeof(unsigned char));
    bufflen += sizeof(unsigned char);
    memcpy(sbuff+bufflen, mpdu->payload,strlen((char *)
(mpdu->payload))+1);
    bufflen += strlen((char *) (mpdu->payload))+1;
    sbuff[bufflen] = '\0';
}

```

This copying into buffer procedure is used to copy the structure contents into a buffer and send that buffer through the network. The reverse procedure is followed after receiving at the other end i.e. the contents of the buffer are again transferred into the corresponding data structure format.

4.6 Scheduling

Scheduling of the frame is basically defined as allocating slots to ST's which are currently up. Lets say we have to schedule a frame of size 2317 slots, in which we have to schedule for some slots for downlink, some for uplink and one or two for beacon broadcast. Typically the data that comes during download from BS is much more than the data that

is requested from the ST, so the number of slots allocated to downlink are more than the slots allocated to uplink. Here downlink slots and uplink slots are of contiguous slots. For making this schedule there are number of scheduling algorithms. We explain two such algorithms here and also say how we implemented.

4.6.1 Round Robin Scheduling

This is a basic scheduling algorithm. Downlink and Uplink slots can further be divided into slots. These both are contiguous in a frame. In our protocol as we are following Multi Sector TDM approach, opposite sectors can be transmitted in parallel. Slots are assigned STs's in a round robin fashion. It doesn't have any priority while scheduling. It is starvation-free algorithm.

4.6.2 Smoothed Round Robin Scheduling (SRR)

Ordinary round robin schedulers are well known for their burstiness in the scheduling output. In order to overcome this problem, SRR codes the weights of the flows into binary vectors to form a Weight Matrix, then uses a Weight Spread Sequence (WSS), which is specially designed to distribute the output more evenly to schedule. It preserves $\Theta(1)$ time complexity by avoiding the time-stamp maintenance employed in various Fair Queueing schedulers. The basic idea of SRR is scanning of the WSS and the corresponding Weight Matrix. The WSS is scanned term by term. When the current term is element i , $column_{k-i}$ of the Weight Matrix (where k is number of columns of Weight Matrix) is selected[8].

Table 4.2 are used in the algorithm that is going to be described.

Algorithm There are three asynchronous actions, namely, Schedule, Add_flow, and Del_flow. Each action is triggered by some events. The Schedule function is as listed in Algorithm 4.6.2.

local variable: f, col { f, col are the current row and current column of the M respectively}

$P_c = 1$

$P_{dl} = header_{k-1} \rightarrow next$ {initialization}

Table 4.2: Symbols used in Algorithm

<i>Symbol</i>	<i>Description</i>
K_{max}	The maximum order of the WSS used by SRR
M	Weight Matrix of all the active flows
S^k	The kth WSS currently used by the scheduler
k	The order of the current WSS used by SRR
P_c	Index of the current scanning position of the WSS, ranging from 1 to $2^k - 1$
$queue_f$	Queue of the received packets of $flow_f$, which is a FIFO
P_f	Packet that is at the head of $queue_f$
L_f	Length of P_f
w_f	Weight of $flow_f$, it is a normalized value
$deficit_f$	A register to memorize how many bytes $flow_f$ should bring to the next round
P_{dl}	Pointer to a node of a doubly linked list
L_{max}	The upper bound of packet's length of the output link
C	Normalized bandwidth of the output link.

while in busy-period **do**

$f = P_{dl} \rightarrow fid$

$deficit_f+ = L_{max}$

while $deficit_f > 0$ **do**

if $L_f \leq deficit_f$ **then**

dequeue(P_f)

send(P_f)

$deficit_f- = L_f$

if $queue_f$ is empty **then**

$Del_{flow}(f)$

break

end if

else

break

end if

end while

```

if  $P_{dl} \rightarrow next! = tail_{col}$  then
     $p_{dl} = p_{dl} \rightarrow next$ 
else
    while ever do
         $P_c + = 1$ 
        if  $P_c == 2^k$  then
             $P_c = 1$ 
        end if
         $col = k - S^k[P_c]$ 
        if  $CL_{col}$  is empty then
             $P_{dl} = head_{col} \rightarrow next$ 
        else
            break
        end if
    end while
end if
end while

```

4.6.3 How did we implement it?

Two tables are maintained at BS. One table is created which contains Primary CID, Basic CID and ST ID, at the time of creation of ranging response. Another is created which consists of Primary CID, Data CID, number of times Data CID has been processed. Table 4.10 gives the snapshot of the same.

Four queues are also maintained at BS for four different service flows. Each queue consists of the corresponding data cids. Data cids are taken from these queues at the time of scheduling the slots. This is not required in our scenario as we are not considering multi sector BS's.

Round Robin We first used round robin algorithm for scheduling of the dlmap and ulmap just based on the number of ST's that are available at that point of time, for example say if the size of the beacon is 10 bytes, each slot is of one byte, and the ratio of DL and UL slots is 2:1 and there is one byte for beacon transmission. Say there are three

Primary CID	Basic CID	ST ID
2 bytes	2 bytes	4 bytes

While creating ranging response

Primary CID	Data CID	Count
2 bytes	2 bytes	1 byte

While assigning Data CID to ST

Figure 4.10: Tables maintained at BS

ST's at that point of time i.e at the time of scheduling the beacon packet, then those three ST's are given two slots each for downlink and one slot each for uplink. This is the way we implemented the round robin algorithm.

Smoothed Round Robin SRR, which is a very good algorithm for scheduling of packets in Multi-service packet networks which suits exactly to our scenario, where we

have UGS, rtPS, nrtPS, and BE service packets to be scheduled. Whenever a request for service is received from ST, BS will categorize it and based on the type it will be enqueued into that particular queue. The Weight Matrix is adjusted dynamically in SRR. Whenever a new flow comes, a new row is added into M as the last row of that matrix similarly when a flow leaves the corresponding row will be deleted and order is adjusted in both the cases. There are K_{max} doubly linked lists named $DL_0, DL_1, \dots, DL_{K_{max}-1}$, which are having three fields prev, next and fid (flow id). DL_i will be empty if all terms in the corresponding column are zero. Doubly linked list data structures are chosen to reduce the complexity of the flow detection.

At the starting of SRR, M and double links are initially empty. When the first flow comes in then `Add_flow` will be called, which in turn calls the Scheduler function. Whenever the process is complete `Del_flow` is called deletes the last flow, and system again enters into busy-period.

4.7 Framing Concepts

Figure 4.11 shows how the frame is slotted and sent through the ethernet.

Control Packet : (starting slot-id, number of slots) = 2B every DL-TB.

- DL-TB is group of slots which belongs to same BS will be packed in a single Ethernet packet.
- Control packet is padded at the beginning of every DL-TB.

Below are some of the assumptions that we made

- Scheduler will take care of allocation of slots such that slots which belongs to same BS will be consecutive.
- No packet drop and CRC errors.
- PHY over head(3 slots allocation) is taken care by scheduler.

Some assumptions that we made about the IIT Madras Board

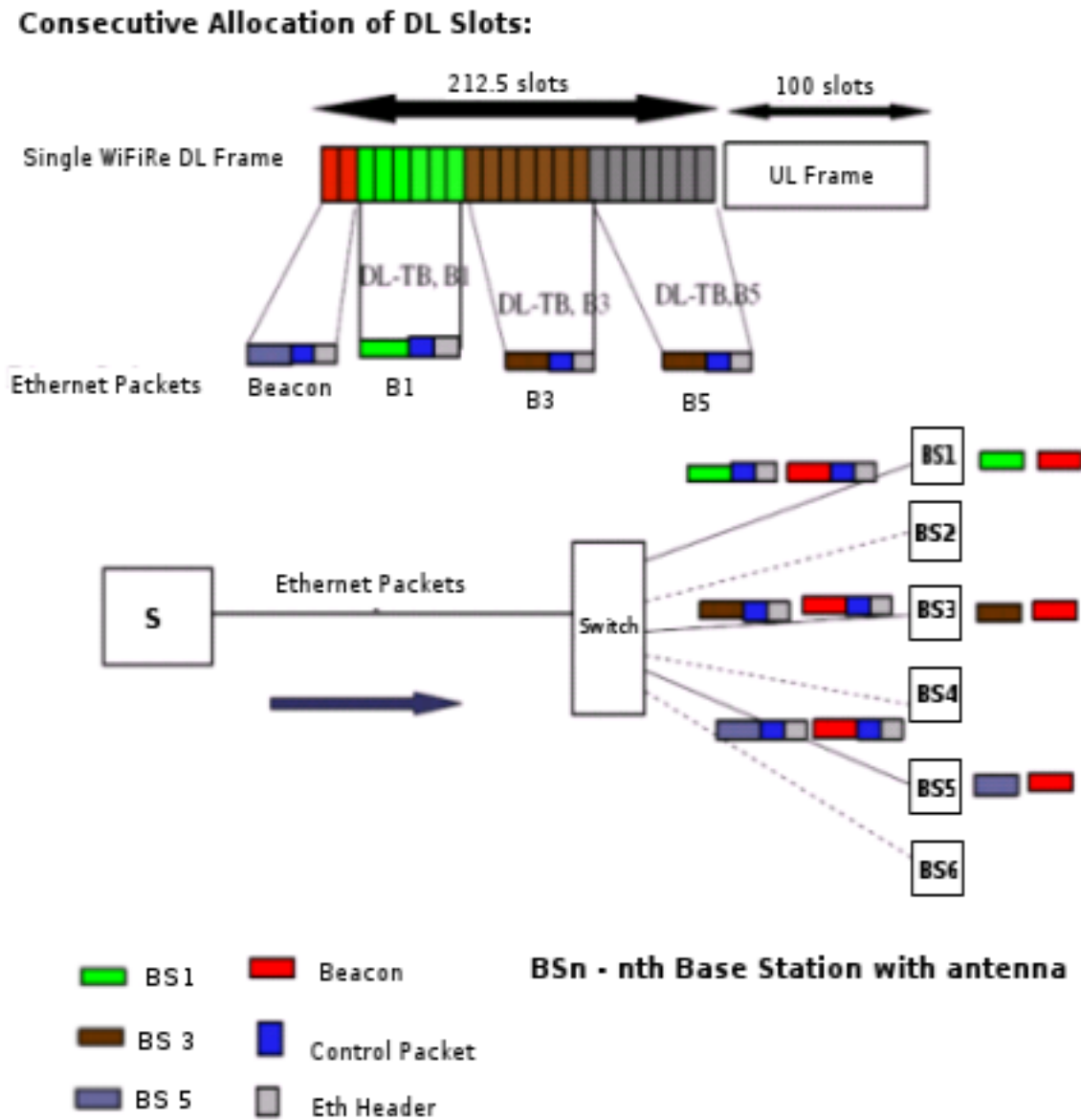


Figure 4.11: Allocation of Slots in a frame

- The board has a clock have capable of generating 1 tick every time slot.
- Some processing for reading control packet and transmitting time slot at appropriate time.
- Every DL-TB has two bytes of control packet. Board has to transmit the packet based on control packet.
- Handling multiple Ethernet Packets at Board. Because some times single DL-TB may not be sufficient for transmitting all slots which belongs to single BS.

- Buffer with minimum size of a complete frame ($210 * 44B$) is required. Which is equivalent to 7 Ethernet Packets(1500B). Assuming that only one frame will present at a given frame interval.
- FCFS queue at BS.

Advantages:

- Low PHY overhead (3 PHY + 1 slots per frame)
- Low control overhead (2B per DL-TB).

Later we went about discarding the fragmentation concept because the IITM board is not readily available for testing so we have created our own format of fragmenting and de-fragmenting the packets.

4.8 Real System Architecture

Figure 4.12 gives a overview of our actual scenario. Consider a scenario where a client sitting at ST wants to browse some HTTP page. The following steps will explain how the communication goes on. Here assumption is that Ranging and Registration has already happened, ST has got its primary CID.

- When a client has some HTTP request, it first sends a request to ST.
- At ST, MAC address of the client and type of request is stored. Further, it sends a DSA request to BS asking for a Data CID for that service flow.
- BS processes the request from ST and if there are slots available it allocates a Data CID to the ST in the response. This Data CID is chosen based on the type of the request that it received from ST. It maintains a table which consists of Data CID, MAC ID and corresponding ST ID.
- When the ST receives the Data CID, it transmits the actual request packet to the BS and stores the Data CID and its corresponding MAC address.
- When BS receives the actual packet request it stores the port number of the socket through which it communicating with ST and data CID, and forwards that packet

to System S, which acts as a proxy and forwards the request further to Internet Service Provider (ISP) or GATEWAY.

- When response is received from ISP or GATEWAY, S sends response based on the corresponding BS ID (which is typically MAC ID of BS).
- BS further process it, based on the corresponding Data CID and port number it sends on that port to the ST.
- ST based on the Data CID and MAC address table if forwards that to the corresponding client.

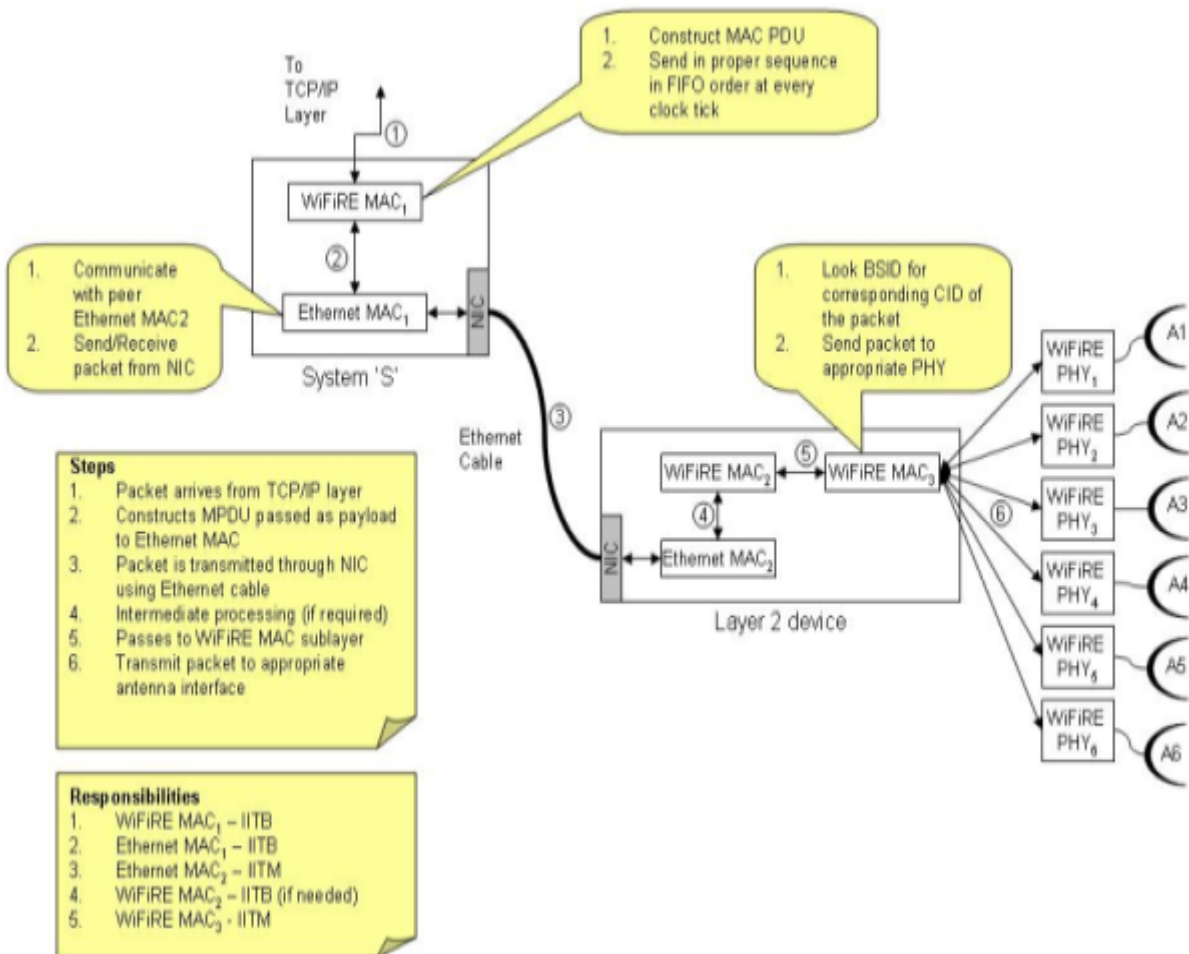


Figure 4.12: Real System Components

4.9 Implementation Issues and Surprises

There were some challenges and surprises which were faced during the implementation. Some of them along with their appropriate solutions are as follows:

Case 1 : In the project, BS is implemented as a socket server and ST as socket client.

When ever an ST comes up, BS needs to instantiate a separate subroutine which take cares of ST and BS itself should again go back on listening mode on some designated port. At the same time BS need to store the assigned FDs to the pool for broadcasting beacon. This pool is nothing but a data structure which is global to the main BS process. Now whenever a *fork()* is called it creates a new process which have its own text, data and stack segments which even did not allow the global data of one process visible to other process. IPC could be another solution for this. Messages can be passed through pipes but still the problem remains the same. Every process has its own file descriptor table and no process and send or receive data on other's file descriptor set in C. The possible remaining solution are the use of threads. POSIX threads are light weighted process which share the same code and data segment of the process, through which common data can be access through shared memory.

Case 2 : Broadcasting the packets to all STs which are currently active over established TCP connections which became difficult to accomplish on a 802.3 ethernet protocol. To overcome this, one of the possible ways could be having a virtual socket at BS end and unicast the packet to this virtual socket. A small subroutine will be initiated which will perform unicast to all the FDs which are currently associated with the BS.

Case 3 : Time synchronization is always being a problem in TDM based systems. It can be implemented using 3-sync mechanism similar to that is being used by TCP, but this may give some variance which is not acceptable at granularity of microseconds. Possible solution is using machines which share collision free media for communication like cross cable over LAN, or test experiments can be run over single machine which share system clock.

Case 4 : Design of a BS scheduler is a complex task because of the dynamic allocation of

DL and UL slots in the time frame. So the possible solutions could be fetching the schedules from the static read only files in which schedules are defined depending upon the number of active STs or designing our own scheduling routine using simple scheduling strategies like round-robin etc. (as in our case).

Case 5 : Structure alignment problem, when a packet is sent over network, the original size of packet does not match with the length field specified inside the packet because of the extra alignment bytes padded by the compiler. One solution could be sending each element individually over network but this will result in increase in system calls and highly depends on structure of packet. Packing the structures to one byte (smallest size data type) will solve this as number of bytes required for padding will be zero.

4.10 Modifications in Draft

Some of the modifications/additions in the draft:

- According to [1], length field of the frame is 7 bits, where as the size of the frame may be maximum of 2317 bytes, which means we cannot specify the size of frame in seven bits. This has been changed to 15 bits.
- There is mismatch in the draft, i.e "Type" field values of Generic Mac Header (Section 4.4.1 of the draft [1]) and type field values of Network Initialization Sub-procedures(4.7) varies.
- Inclusion of flow diagrams of ranging and registration procedures at the ST.

Chapter 5

Conclusion and Future Work

5.1 Conclusion

From the discussion in the previous chapters, we have seen that our WiFiRe protocol is a very cost effective solution for providing broadband access as well as voip access to rural areas.

We have shown that our protocol works in real scenario also by emulating it on ethernet. We have concentrated on one sector region (one BS) assuming ST as direct client. We have just implemented ranging for exchanging of Basic CID and Primary CID but not done synchronization as we assumed LAN is tightly synchronized. We have implemented our own scheduler for scheduling the DL and UL map. We haven't handled Dynamic Service Change.

5.2 Future Work

This project can be enhanced in the following areas

- Changing the features of ST such that it works like in a real scenario.
- Implement the concept of Timers.
- Ranging part should be completed so that it handles the synchronization.
- Enhancing it to multi sector BS.
- Implementing it actually into the board i.e. Physical Hardware.

By implementing the above features makes our protocol a full fledged one.

Bibliography

- [1] Sridhar Iyer (IIT Bombay), Krishna Paul (Intel), Anurag Kumar (IISc Bangalore), and Bhaskar Ramamurthi (IIT Madras). Broadband wireless for rural areas—*WiFiRe*: medium access control (mac) and physical layer (phy) specifications. August 2006.
- [2] LAN/MAN standards Committee. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. In *IEEE-SA Standards Board*, June 2003.
- [3] LAN/MAN standards Committee, IEEE Microwave Theory, and Techniques Society. Part 16: Air interface for fixed broadband wireless access systems. In *IEEE-SA Standards Board*, June 2004.
- [4] Wikipedia. Ieee 802.11 — wikipedia, the free encyclopedia, 2007. [Online; accessed 30-June-2007].
- [5] Wikipedia. Ieee 802.16 — wikipedia, the free encyclopedia, 2007. [Online; accessed 30-June-2007].
- [6] Bhaskaran Raman and Kameswari Chebrolu. Revisiting mac design for an 802.11-based mesh network. In *San Diego, CA, USA: HotNets-III*, November 2004.
- [7] Steven H. Rodrigues, Thomas E. Anderson, and David E. Culler. High-performance local area communication with fast sockets. In *USENIX Annual Technical Conference*, January 1997.
- [8] Guo Chuanxiong. Srr: An $o(1)$ time complexity packet scheduler for flows in multi-service packet networks. In *Institute of Communication Engineering, Nanjing, China*, 2001.

