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

Kanwal Rekhi School of Information Technology

Indian Institute of Technology Bombay

2007

Dissertation Approval Sheet

This is to certify that the dissertation entitled

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

(Internal Examiner)

Dr. Krishna Paul

(Chairperson)

Date: ______________

Place: ______________

INDIAN INSTITUTE OF TECHNOLOGY BOMBAY

CERTIFICATE OF COURSE WORK

This is to certify that **Mr. H Shravan 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 10^{th}, 2007

Abstract

WiFiRe is a protocol which is an extension of the existing WiFi (802.11) protocol, which stands for Wireless Fidelity Rural extension. The main aim of WiFiRe is to provide long range communications with high bandwidth,with low cost and easy availability of the chipsets. WiFiRe uses most of the features of WiMAX (802.16). 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 will be able to provide long range communication by dividing the whole area into sectors, each sector will be having one base station which is directional so that it covers more distance. WiFiRe uses only one frequency channel for both uplink and downlink, in which each sector is allocated frequency based on Time Division Multiplexing- Multi-sector TDM(TDM-MSTDM).

Problems associated with design and implementation and their plausible solutions are covered as a part of report. Additionally, it also comprises of sequence diagrams, flow diagrams, state diagrams etc. of working components of *WiFiRe* along with design model in C sockets and describes the issues and challenges involving implementation of the projects.

By emulating WiFiRe protocol on LAN we want to show that our protocol works in real scenario.

Contents

List of Figures

Abbreviations and Notations

Abbreviations

AODV	: Ad hoc On Demand Distance Vector
DLE	: Drop-Least-Encountered
DLR	: Drop-Least-Recently-Received
DOA	: Drop-oldest
DRA	: Drop-Random
FIMF	: Ferry-Initiated Message Ferrying
p-AODV	: *proxy*-AODV
MANET	: Mobile Ad hoc networks
NIMF	: Node-Initiated Message Ferrying
p-RRER	: *proxy*-RRER
p-RREP	: *proxy*-RREP
p-RREQ	: *proxy*-RREQ
RERR	: Route Error
RREP	: Route Reply
RREQ	: Route Request

Chapter 1

Introduction and Motivation

Now-a-days the use of Internet and mobile communication has grown to a large extent such that it became mandatory for daily usage of life. The statistics in India shows that there are more than 100 million mobile users in India [as per June 10th] 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 their distances 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 2.4GHz 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 did not proved to 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.

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 sectored 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 where as users with in 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 t
system gain of 1
communication.
shown in the foll

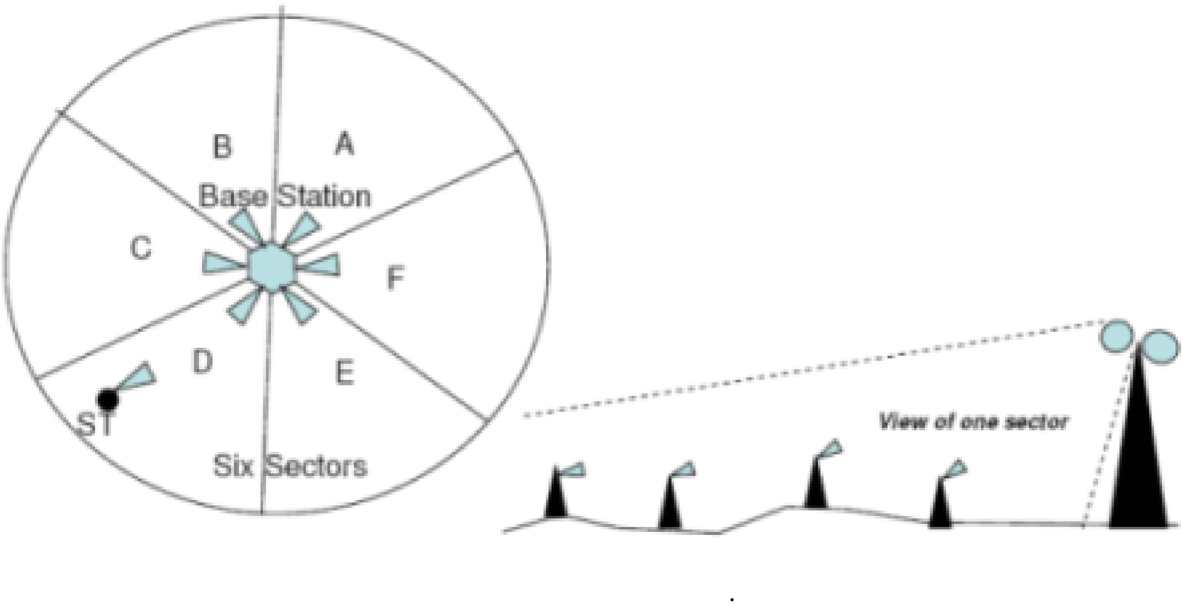

Figure 1.1: WiFiRe Topology

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 alternatively 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 about 25Mbps (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 with synchronization with each other. Time is divided into frames, which is further divided into DownLink (DL) and UpLink (UL) segments, which may not be of equal time intervals. In each DL slot one or zero transmissions can take place in each sector. Multiple BS antennas can transmit simultaneously provided they do so in a non-interfering manner.

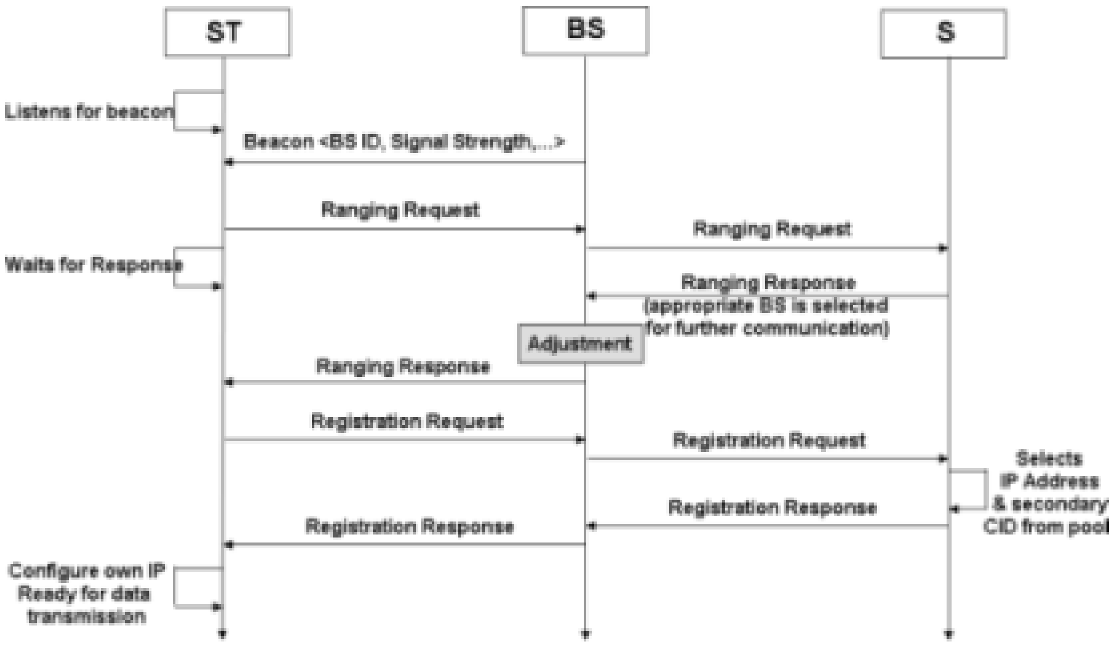

Figure 1.2: Basic communication sequence diagram

Figure 1.2 is sequence diagram for basic working of WiFiRe protocol. 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 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 operating 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 are being done. It is also being 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 being given in the following Design section.

Registration :- This steps 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 being exchanged. After this step a IP is being assigned to the ST by BS. Detailed explanation is being 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 CID's to 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 on Ethernet.

1.3 Thesis Outline

/********* TO BE MODIFIED *********/

Chapter 2

Literature Survey

In this chapter we discuss about related work of WiFiRe protocol, what are the other alternative technologies such as WiMAX-d(802.16d), WiFi(802.11b), cellular technologies (GSM, GPRS, and CDMA), and Digital Gangetic Plain Project (DGP). First we will here discuss the alternative technologies their's pros and corns, then we will go about discussing about 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 fibre optic, installation costs are high as it requires ripping up streets to lay cables. The ability to provide these connections without wireless, 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 GSM, GPRS, and CDMA

2.1.1 GSM

The acronym GSM stands for Global System for Mobile telecommunications. The digital nature of GSM allows data, both synchronous and asynchronous data, to be transported as a bearer service to or from an ISDN terminal. The data rates supported by GSM are 300 bps, 600 bps, 1200 bps, 2400 bps, and 9600 bps. The most basic tele-service supported by GSM is telephony. A unique feature of GSM compared to older analog systems is the Short Message Service (SMS). Supplementary services are provided on top of tele-services or bearer services, and include features such as international roaming, caller identification, call forwarding, call waiting, multiparty conversations, and barring of outgoing (international) calls, among others. Now GSM is deployed in large part of country. Because of GSM is circuit switched and it provides low data rates this is not suitable for providing broad band internet service. Despite of all these reason its cost of providing service is also very high that is not affordable to rural people.[2]

2.1.2 GPRS

The acronym GPRS stands for General Packet Radio Service (GPRS) is a mobile data service available to users of GSM mobile phones. It is often described as 2.5G, that is, a technology between the second (2G) and third (3G) generations of mobile telephony. It provides moderate speed data transfer, by using unused TDMA channels in the GSM network. GPRS is different from the older Circuit Switched Data (or CSD) connection included in GSM standards. GPRS is packet-switched which means that multiple users share the same transmission channel, only transmitting when they have data to send.This means that the total available bandwidth can be immediately dedicated to those users who are actually sending at any given moment, providing higher utilization where users only send or receive data intermittently. Web browsing, receiving e-mails as they arrive and instant messaging are examples of uses that require intermittent data transfers, which benefit from sharing the available bandwidth. Usually, GPRS data are billed per kilobytes of information transceiver while circuit-switched data connections are billed per second. A realistic bit rate GPRS provides is 30 to 80 Kbps. GPRS is also well deployed on top of GSM networks to provide internet service to its mobile customers. Problems of GRPS using in rural areas is that its pretty costly when comes to service and also it gives very less data rates.[3]

2.1.3 CDMA

The acronym CDMA stands for Code Division Multiple Access is a form of multiplexing and a method of multiple access that divides up a radio channel not by using TDM or FDM approach but instead uses different pseudo-random code sequences for each user. CDMA is a form of ”spread-spectrum” signaling, since the modulated coded signal has a much higher bandwidth than the data being communicated. CDMA also refers to digital cellular telephony ystems that make use of this multiple access scheme, such as those pioneered by QUALCOMM, and W-CDMA by the International Telecommunication Union or ITU. Main disadvantages of this technique include near-far problem, higher cost and low data rates.[4]

2.2 WiFi(802.11b)

The acronym WiFi stands for Wireless Fidelity. 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. It operates on 2.4 GHz frequency band. 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 Access Point is central administration that handles station authentication and association to the network. Multiple AP's connected by a Distribution System(DS) can extend the range of wireless network to a much more than 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. Because 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, it is more suitable for mesh networking. It felicitates 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. 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 for using this in long distance communication. 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 increase in number of nodes. When we used to build wide area network Medium Access (MAC) efficiency becomes very poor. One solution for this problem is to replace the MAC protocol with one more suited to wide-area deployment.[5]

2.3 WiMAX(802.16d)

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 all subscriber stations wishing to pass data through an access point are competing for the AP's 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 numbers 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. 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 rural areas people.[6]

2.4 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. 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 current approach is MAC of 802.11b. 802.11b doesn't provide any quality of service 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 chip set. 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 this is not ad-hoc, more computation power needed at each access point as each act as a router, and it doesn't give QoS guarantee.[7]

Chapter 3

WiFiRe Protocol

In this chapter we are going to discuss the WiFiRe protocol in detail and its related concepts of WiFi PHY and WiMAX MAC layer are also going to be discussed. 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 as it is low cost and easily available, but changes the MAC layer so that it can support long ranges instead of short ranges. 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 QUOS features of MAC.

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

The following figure 3.2 gives us how exactly a wifire frame is being divided. A typical wifire frame consists of beacon transmission, downlink and uplink slots. Beacons are being transmitted periodically. Downlink slots are the one which are used by BS to transmit data to ST's through broadcast, where are uplink slots are being used by ST's 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 requirements at each point of time.

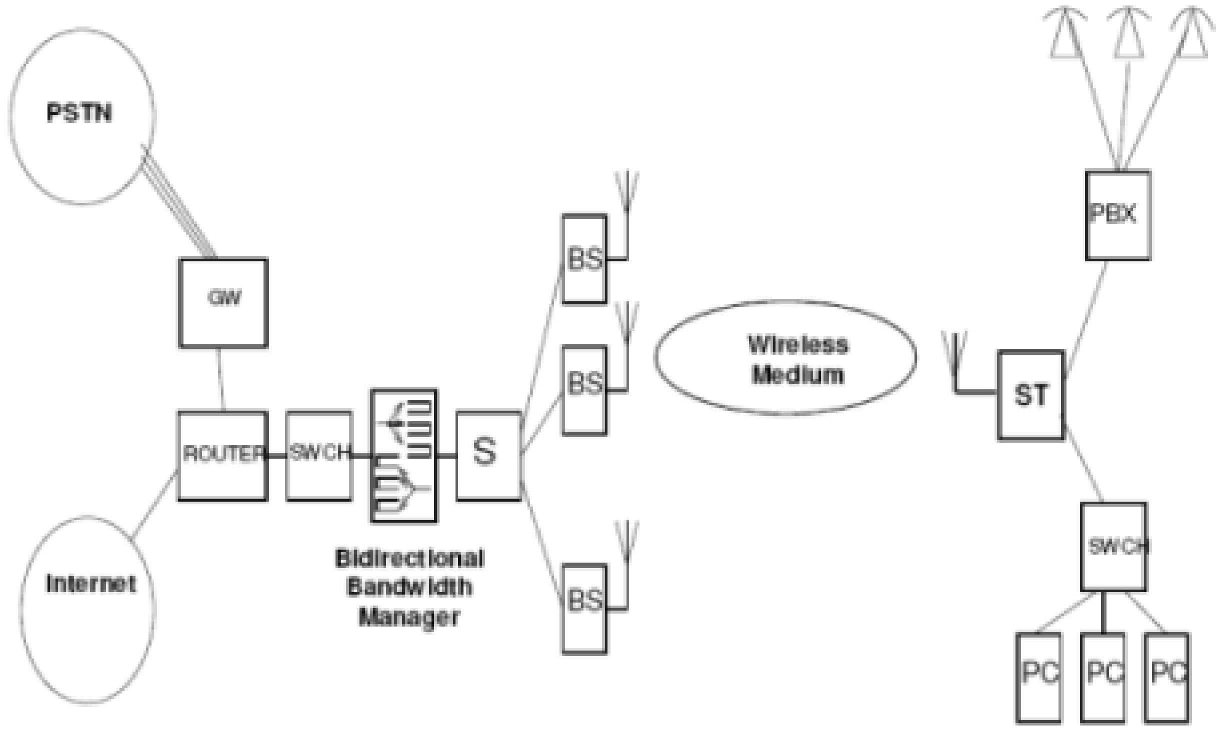

Figure 3.1: WiFiRe overview along with External world connections

3.0.1 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 as shown in the figure. Each BS can be distinguished separately by MAC, thus single MAC controls more than one PHY and responsible for transmitting MAC packets while resolving the collisions from the perspective of receivers. These packet transmission can be done in serial or in parallel.

The BS's which are neighbors cannot transmit simultaneously because there are chances 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).

As said earlier 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 there content 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 their corresponding

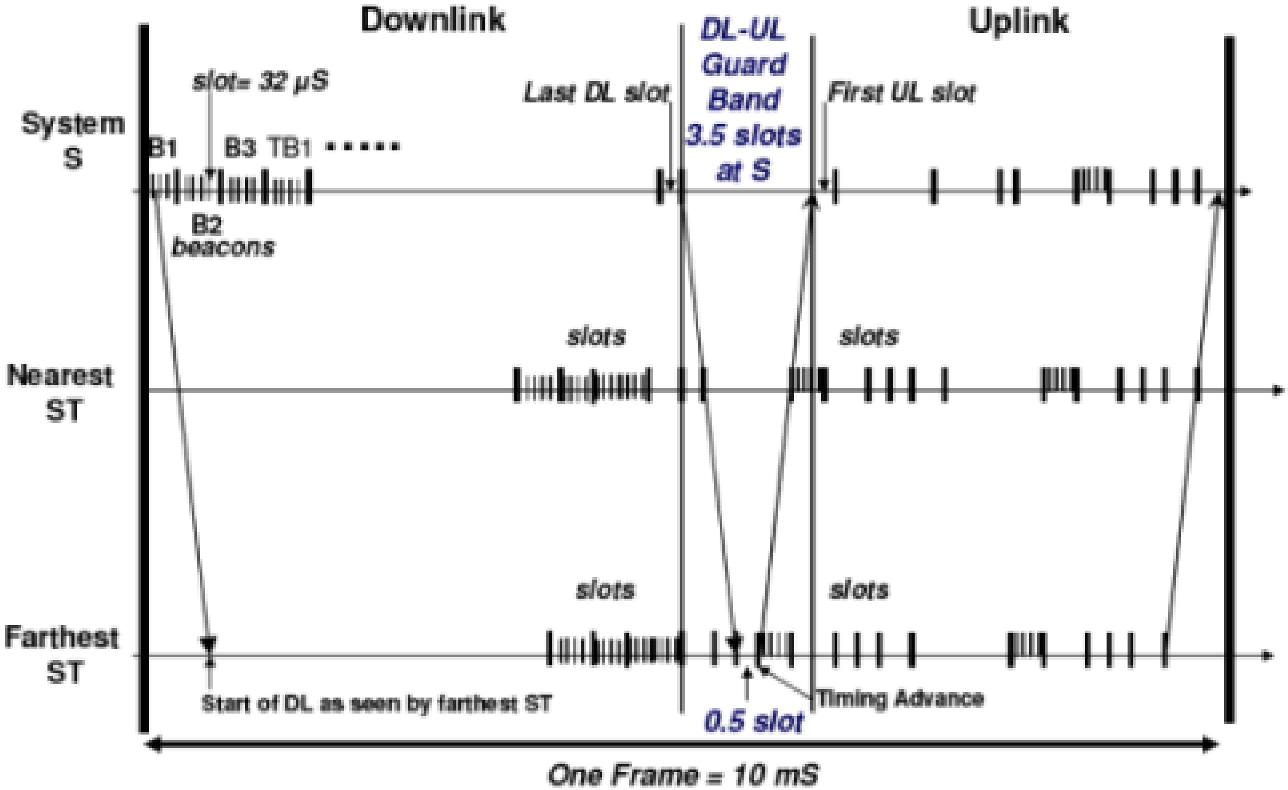

Figure 3.2: Timing Sequence

slot assignments¿. There is a guard bit of few slots between the end of DL segment and the start of UL segment so that it ensures that it covers the propagation delay.

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 be requesting uplink bandwidth on a per connection basis. A system S may grant the request by polling or contention procedures.[1]

3.0.2 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.

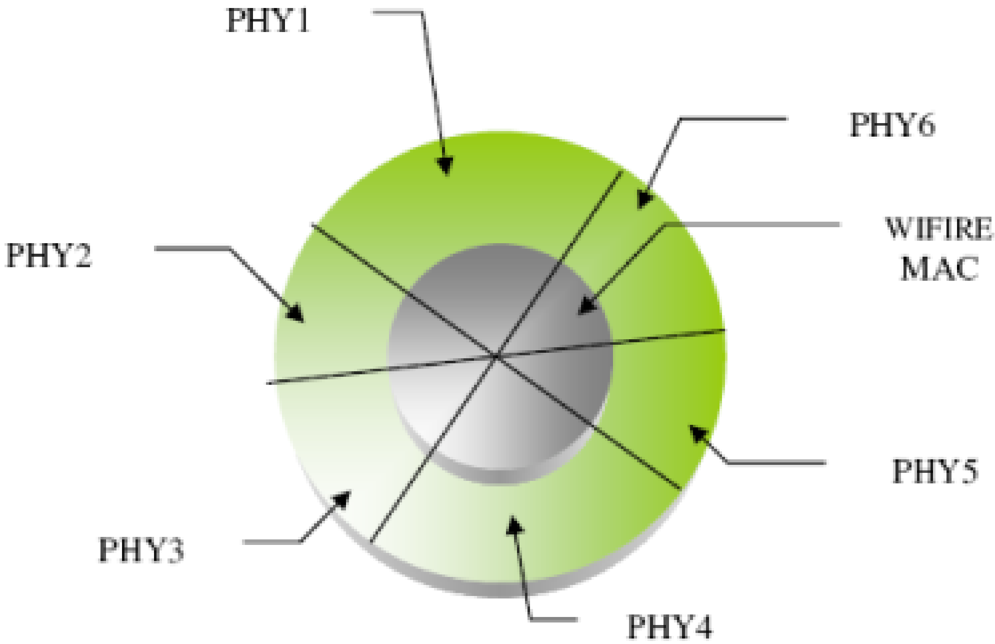

Figure 3.3: MAC Over PHY

3.0.3 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 process is to get registered to the network.

3.0.3.1 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 exchanges operational parameters and capabilities. This process enables the ST to acquire IP address to set-up provisioned connections.

3.0.4 Connection Management

After registration, the ST can request 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.

3.0.5 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 service flows that generate fixed-size data packets on a periodic basis, such as VOIP.
  - *Real-time Polling Service* (rtPS) - Designed to support real-time service flows that generate variable-sized data packets on a periodic basis, such as MPEG video.
  - *Non Real-time Polling Service* (nrtPS) - Designed to support non real-time service flows that require variable sized data grants on a regular basis, such as high bandwidth FTP.
  - *Best Effort Service* (BE) - Provides efficient service to best effort flow traffic.

- 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.

3.1 Relevant WiMAX background

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.

The QoS management of 802.16 have the following components

- Admission Control
- Buffer Management
- Scheduling

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. On Downlink, its broadcast and as only BS will transmit data 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 being passed through the UL-MAP by the BS.

The following figure shows the layers of MAC and PHY

3.1.1 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 being associated with these service flows. When a customer needs new service then new connections are being established. These connections are needed active maintenance. When everything is done the connections are being terminated.[8]

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 and request intervals defined by their respective IEs. BS uses a random back-off algorithm to resolve contention.

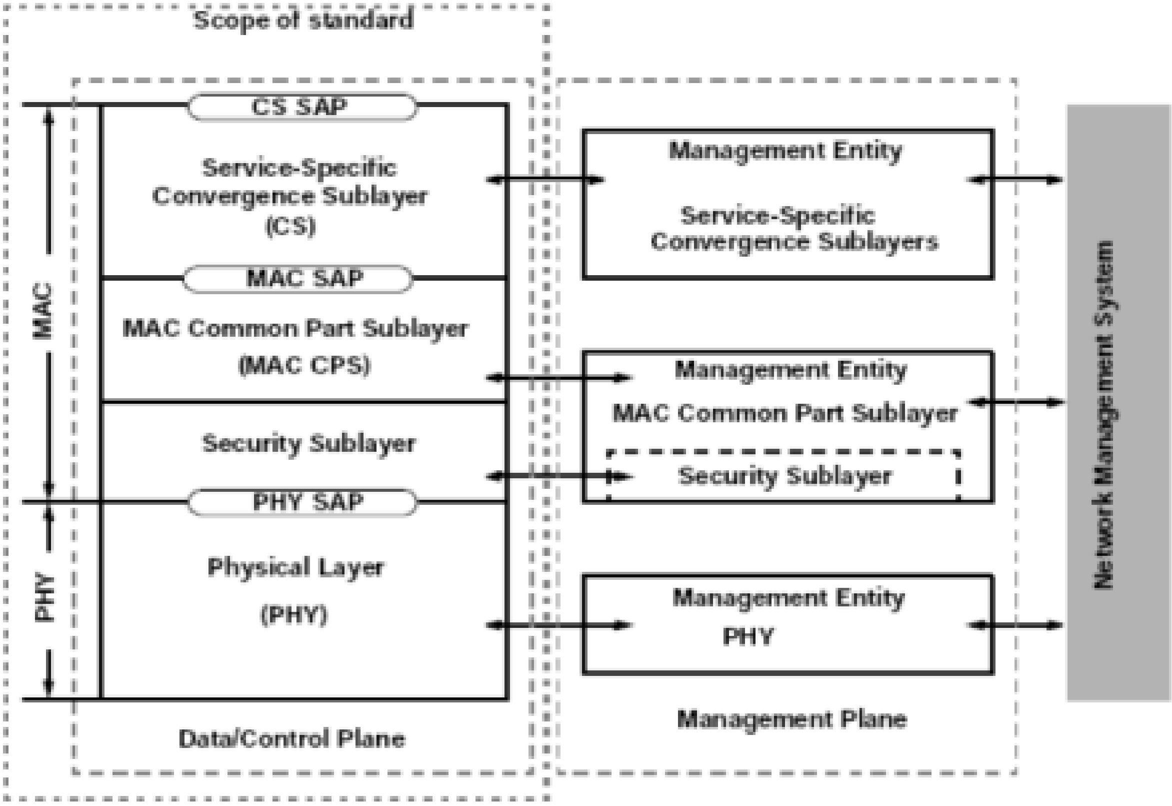

Figure 3.4: WiMAX MAC and PHY layers

Scheduling Services - Different types of service flows have been defined based on which the MAC schedule its processes. The main services that are defined are

- *Unsolicited Grant Service* (UGS) - Designed to support real-time service flows that generate fixed-size data packets on a periodic basis, such as VOIP.
- *Real-time Polling Service* (rtPS) - Designed to support real-time service flows that generate variable-sized data packets on a periodic basis, such as MPEG video.
- *Non Real-time Polling Service* (nrtPS) - Designed to support non real-time service flows that require variable sized data grants on a regular basis, such as high bandwidth FTP.
- *Best Effort* (BE) - Provides efficient service to best effort flow traffic.

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.

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 SS's 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 being allocated accordingly. An additional scheduler in SS determines in which order the service is being granted slot.

3.2 WiFi Background

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. WiFi is typically used for indoor ranges of 30 m, which can be operated at 11 Mbps and 90 m, which can be operated at 1 Mbps. With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to 8 kilometers.[9]

3.2.1 802.11 Reference Model

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

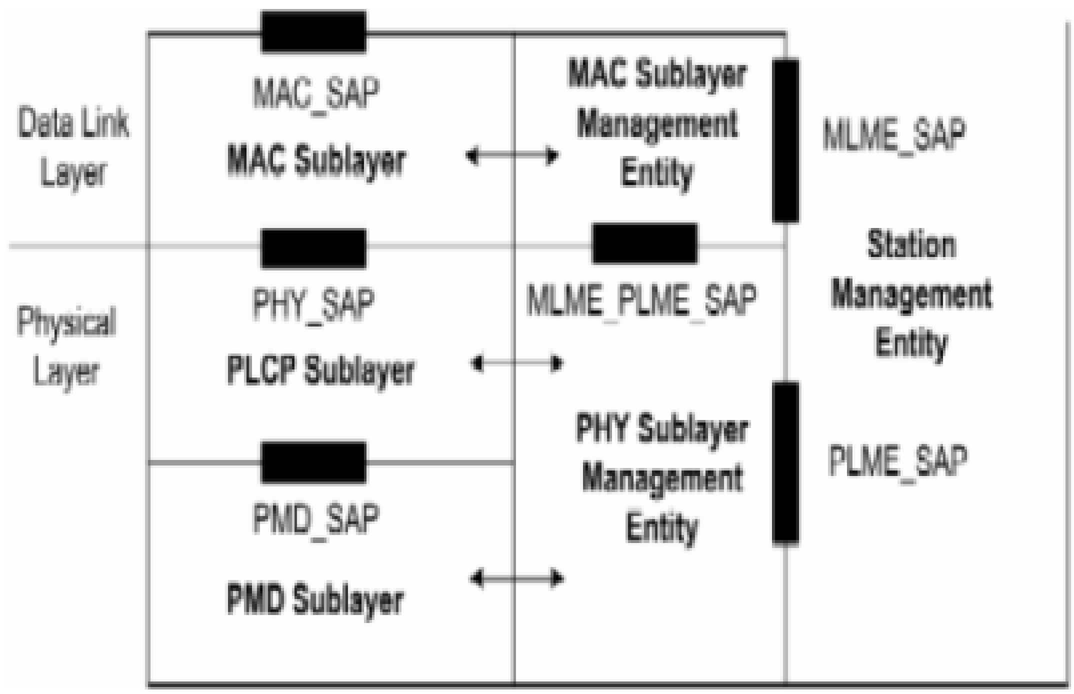

Figure 3.5: WiFi MAC and PHY Layer

3.2.2 802.11 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). There is another method also which can be used for accessing that method is Point Coordination Function (PCF), which uses polling technique to select which station to transmit.

3.2.3 802.11 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 complementary code keyring(CCK).

3.2.3.1 Types

There will be three PHY types :

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

3.2.3.2 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 (that is, RF in the air) 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.

Chapter 4

Implementation Details

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. Over LAN scenario there is no need of ranging as the propagation delay is negligible so this procedure get by passed currently. There might be need of ranging at ethernet also when the hardware is not time synchronized. We are doing ranging in order to exchange primary and basic cid's between ST and BS.

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 being exchanged.

4.2 LAN Emulation

4.2.1 What is LAN Emulation

We have emulated the WiFiRe Protocol using LAN as the basic medium of propogation between ST and BS. Here in emulation WiFiRe MAC layer will be over application layer

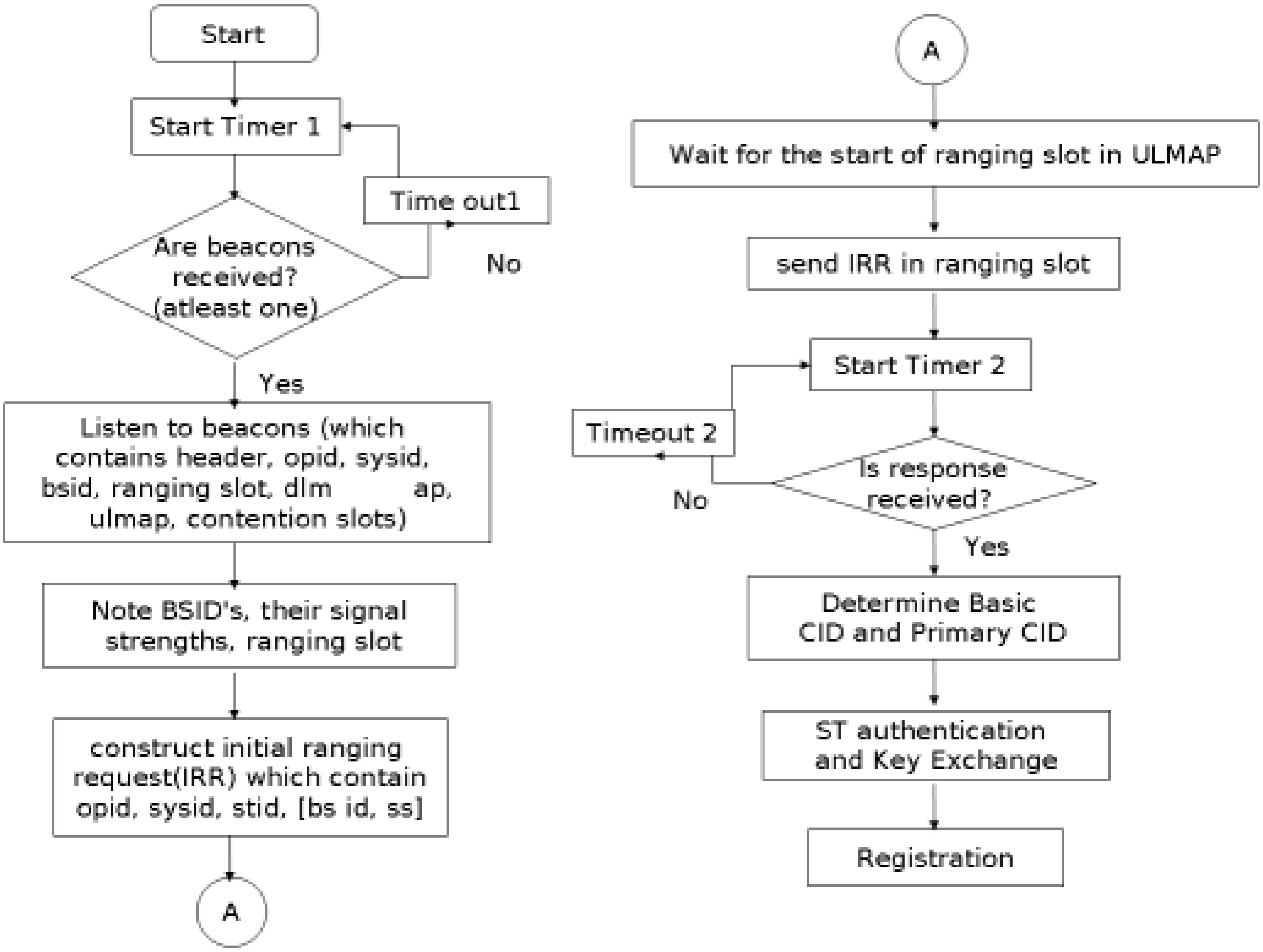

Figure 4.1: Ranging at ST

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 using C sockets by assuming that the Application Layer of the Ethernet 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 4.3 is the overview of the LAN level emulation of the protocol.

4.2.2 Why Emulating on LAN?

- To understand and ensure that steps involved in WiFiRe protocol works.

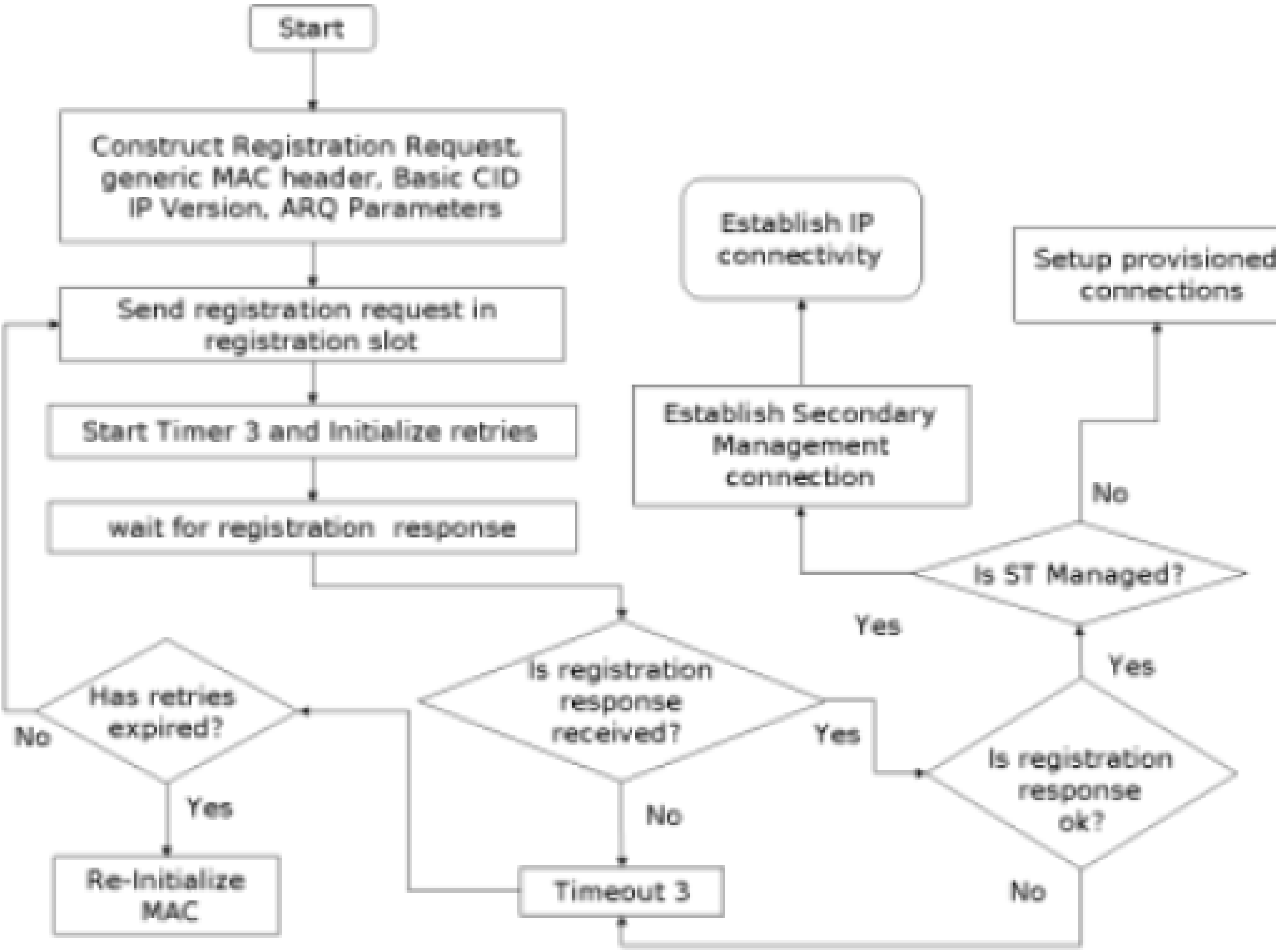

Figure 4.2: Registration at ST

- It is comparatively easy to debug and make changes on 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 (i.e. LAN in this case).
- Design and implement structures and small working modules in order to test and reuse them with minimum changes while going into kernel level.

4.2.3 What we have achieved by Emulating on LAN

We have proved that the basic protocol steps of WiFiRe are correct. We have emulated Beacon broadcast, Registration, Data Service Addition, and Data Connection Termination. We have considered the following scenario while emulating. Figure 4.4 shows the

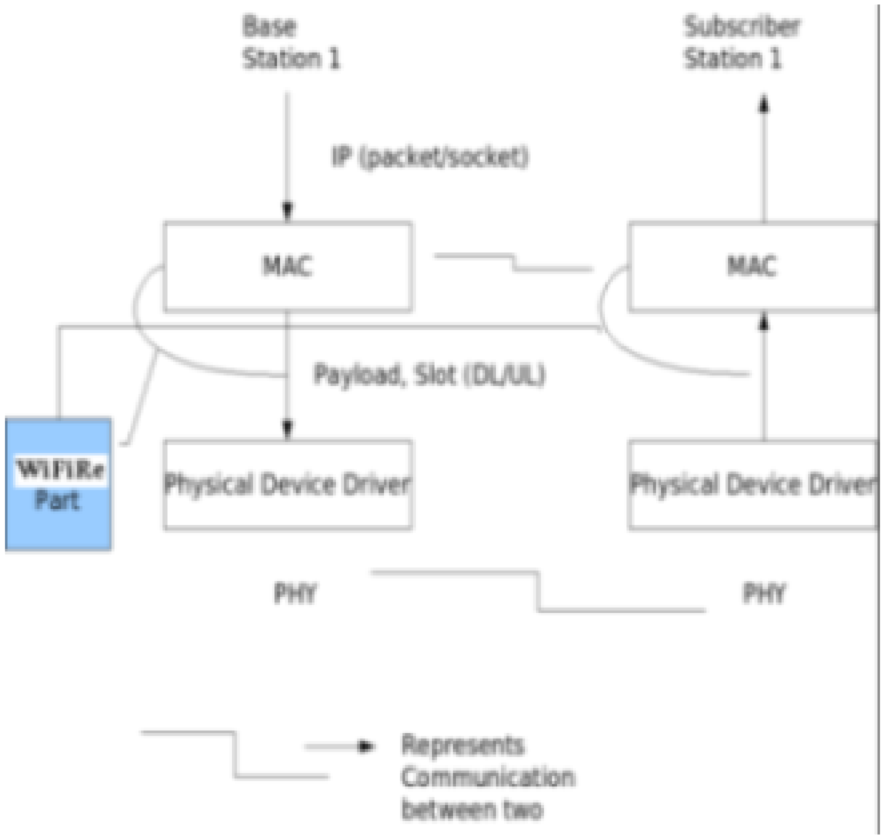

Figure 4.3: Overview of LAN emulation

basic steps that were being processed while emulating the protocol.

4.3 Construction of Beacon and Mac Management Packets

Construction of beacon requires scheduling of the ST's which are up in the DL and UL map of the beacon that is going to be transmitted. We used round robin scheduling algorithm for scheduling the ST's in the frame, this scheduling concept is explained in detail in next section. Mac Management packets are created as when required. Based on the packet that either ST or BS has to send they will create that packet. Then this packet is being transmitted through the network.

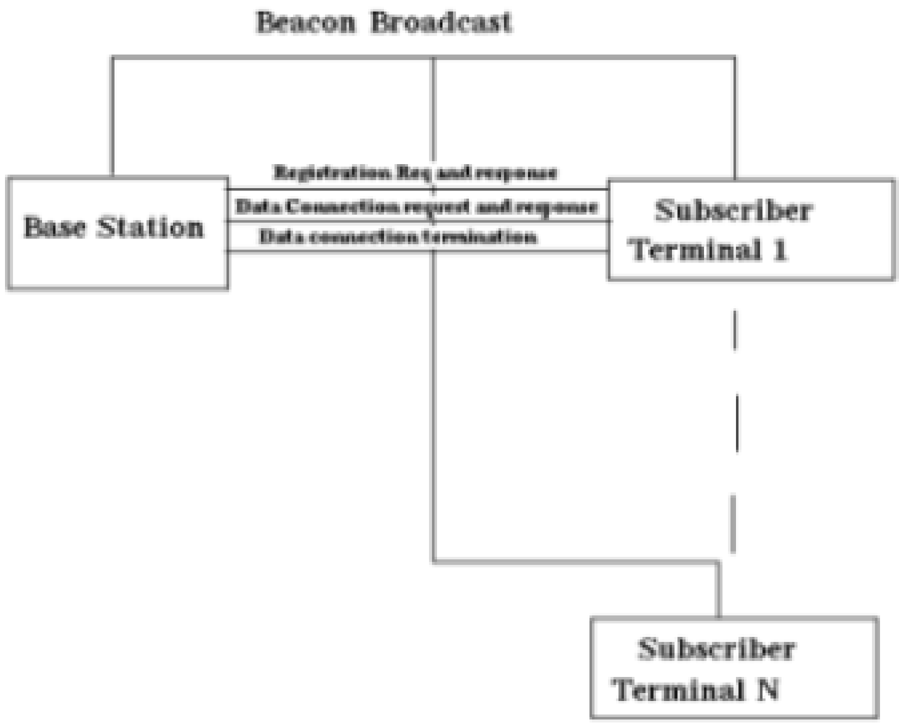

Figure 4.4: Steps that were emulated on LAN

4.4 Scheduling

Scheduling of the frame is basically defined as allocating slots to ST's which are currently on. Lets say we have to schedule a frame of size N slots, in which we have to schedule for downlink slots, uplink slots and beacon broadcast. Typically the data that comes during download is much more than the data that is being 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 contiguos slots. For making this schedule there are few scheduling algorithms.

4.4.1 Round Robin Scheduling

This is basic scheduling algorithm which is of least complexity. Uplink and downlink slots can further be divided into two contiguos parts. In our protocol as we are following Multi Sector TDM approach, opposite sectors can be transmitted in parallel. The basic approach of scheduling is that based on the number of ST's that are currently on, those are given chance one by one till all ST's are being scheduled, after that again it starts from the first ST, repeats till all slots are being scheduled with some ST. It doesn't have any priority while scheduling. It is starvation-free algorithm. It works like First Come First Schedule (FCFS) basis.

4.4.2 Greedy Approach

4.4.3 Fair Scheduling

4.4.4 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 forma 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. The followind symbols are being used in the algorithm that is going to be described.

Symbol	*Description*
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 according to bandwidth assignment granularity
$deficit_f$	A register to memorize how many bytes $flow_f$ should bring to the next round
P_{dl}	Pointer to a node of a double link
L_{max}	The upper bound of packet's length of the output link
C	Normalized bandwidth of the output link.

Algorithm There are three asynchronous actions, namely, Schedule, `|Add_flow|`,`Del_flow`. Each action is triggered by some events. Schedule is the main part of the scheduler, it is invoked when the output link enters a *busy-period*. `Add_flow` is invoked when a new flow arrives and the `Del_flow` is invoked when the flow is deleted explicitly or dead. The Schedule function is as listed below.

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}
while in busy-period **do**
  $f = P_{dl} \rightarrow fid$
  $deficit_f + = L_{max}$
  while $deficit_f > 0$ **do**
    if $L_f <= deficit_f$ **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

4.5 Memory Management

4.5.1 Fast Sockets

For high performance in the local area networks fast sockets concept is being 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 (Active Messages). Interoperability with existing programs is obtained by supporting most of the Sockets API and transparently using existing protocols for communication with non-Fast Sockets programs.

4.5.1.1 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 metadata; 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.

Figure 4.5 shows Fast Sockets' send mechanism and buffering techniques.

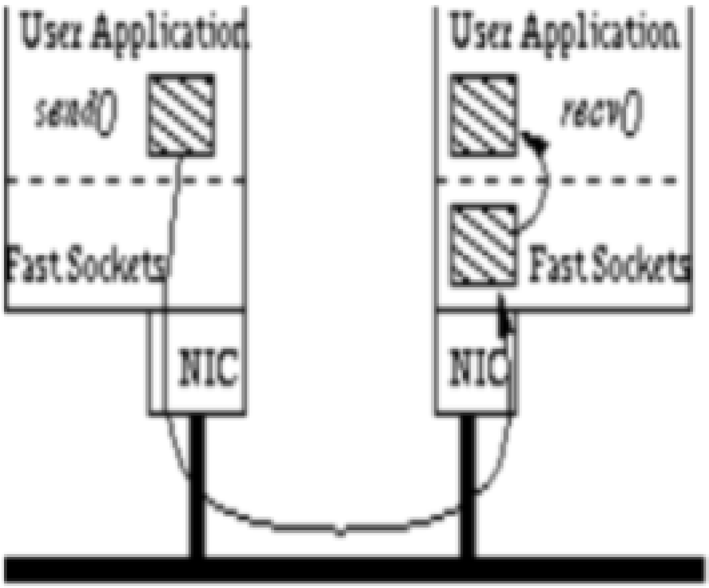

Figure 4.5: Data transfer in Fast Sockets

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.

4.5.1.2 Problems With Fast Sockets

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

- It may consume more memory than the global mbuf pool, which is used in kernel implementations.
- Sharing the socket buffer creates a problem when a fork() call is being initiated.

4.6 Malloc replacement

We used malloc for dynamically creating packets for showing demo in the second stage but as malloc() function will consume more cycles and it also creates problems when there is a pointer in a structure while sending through the network, we replaced malloc with static buffers and copied data of the structure into those static buffers.

The following code snippet shows how a structure is being copied into a buffer. It uses the concept of 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;
};
unsigned char sbuff[MAX_PKT_LEN]; /* Buffer which is going to be sent through socket */
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 is being used to copy the structure contents into a buffer and send that buffer through the network. The reverse procedure is being followed after receiving at the other end i.e. the contents of the buffer are again being transferred into the normal structure.

Chapter 5

Conclusion and Future Work

5.1 Conclusion

From the discussion in the previous chapters, we have seen that p-AODV performs better in terms of overhead on networks and average consumption of memory per node. We can also say that it is equally good as compared to flooding approach in terms of message delivery.

There is a trade off between "Load on Network" and "Message Delivery Efficiency". If we impose less restrictions on proxy selection, then the probability of message delivery increases. But, at the same time load on network and nodes is increases. If we impose strict restrictions on proxy selection criteria, then message delivery probability decreases.

To perform better in terms of message delivery percentage and at the same time maintain low load on network and nodes, we propose some extensions in the future work section.

5.2 Future Work

This project can be enhanced in two different directions:

- Improve the proxy selection function in terms of parameters and their values to improve efficiency.
- Add more features to protocols, like acknowledgement for data.

A combination of both the above extensions will provide a self tuning system. For example, a acknowledgement from destination to source can be used as carrier to distribute value of duplication and percentage of message delivered. This will help other nodes to regulate their parameters and their values while choosing the proxy, according to their requirement of message delivery. And to stop flooding of this feedback a node is allow to drop acknowledgement on the basis of its TTL field and last information flooding time. On the other hand, node can free messages from buffers of respective sequence number.

We can also apply "proxy" and "store and forward" concept with other routing protocol of ad hoc network like DSDV, DSR. This will give us a opportunity to compare two popular protocol.

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] Wikipedia. Global system for mobile communications — wikipedia, the free encyclopedia, 2007. [Online; accessed 30-June-2007].

[3] Wikipedia. Gprs — wikipedia, the free encyclopedia, 2004. [Online; accessed 30-June-2007].

[4] Wikipedia. Cdma — wikipedia, the free encyclopedia, 2002. [Online; accessed 30-June-2007].

[5] Wikipedia. Ieee 802.11 — wikipedia, the free encyclopedia, 2007. [Online; accessed 30-June-2007].

[6] Wikipedia. Ieee 802.16 — wikipedia, the free encyclopedia, 2007. [Online; accessed 30-June-2007].

[7] Bhaskaran Raman and Kameswari Chebrolu. Revisiting mac design for an 802.11-based mesh network. In *San Diego, CA, USA: HotNets-III*, November 2004.

[8] 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.

[9] LAN/MAN standards Committee. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. In *IEEE-SA Standards Board*, June 2003.