SEAMLESS HANDOVER / INTEROPERABILITY BETWEEN WIMAX AND WIFI

MCS

By

Muhammad Shahid Razzaque

Submitted to the Faculty of Electrical Engineering Department
Military College of Signals, National University of Sciences & Technology,
Rawalpindi in partial fulfillment for the requirements of a M.S Degree In
Electrical Engineering

APRIL 2012

ABSTRACT

In present communication scenarios, there are multidimensional technologies working around the globe, like WiMax, GSM and WiFi. Each one of these technologies from multi vendors has different specifications and protocols. These variations make them incompatible with each other. The need of today is to evolve a system that can utilize entire available communication infrastructures for establishing a reliable communication on the day of need.

In order to bring compatibility/interoperability among these technologies, we need to establish a single platform. This will not only bring all the technologies under one umbrella but will also enable the users to choose between variety of different technologies based on their availability and Quality of Service. The need of establishing such compatibility was pronounced after 2004 Indian Ocean earthquake and tsunami which devastated the communication infrastructure in their respective areas. The partnership between the public safety communications organizations and industry manufacturers under the umbrella of Project 25, initiated a step of interoperability for government or private sector law enforcement agencies, ambulance services and crisis management centers, to communicate more effectively with each other when out of their coverage area. Interoperability provides an attractive solution to communicate with the infrastructure of different communication system at low or no signal strength of the parent system. The idea of this research is not to limit this global cause to only public safety communication systems but this is to be extended to commercial wireless communication systems.

This MS research targets at establishing seamless handover /interoperability between WiFi and WiMAX, this involves a vertical handover between the two technologies. The trigger for this handover will be the available signal strength of one or other proposed network. This implies that if the signal strength of one network goes down and signal strength of 2nd proposed network is available, the user will be handover its call to 2nd network having infrastructure / signal strength without dropping the ongoing call.

To achieve this objective, Wi-Fi and WiMax environments has been simulated in Lab view which will act as the foundation of the Interoperability process. With the successful simulation of these environments, system identifier was developed and followed by culmination into the formulation of a common modulation technique to achieve the seamless handover / interoperability.

DEDICATION

To my family, unit officers and my seniors, without whom I would not be Where I am.

ACKNOWLEDGEMENT

I am highly grateful to **ALLAH**, who provided me with not only the opportunity but also the power to acquire knowledge, skills and abilities for the successful completion of the project.

I would like to thank my advisor, **Dr. Adnan Ahmed Khan** and my co-advisor **Asst. Professor Imtiaz Khokhar** for motivating and helping me to work on interoperability between WiFi and WiMAX and providing me with the support and guidance to accomplish this task. I am highly grateful to all of my committee members, **Mr. Attiq Ahmed**, **Dr Adnan Rashdi** and **Mr. Kamran Arif Rao** who helped me throughout the project implementation and for encouraging me through all the project phases. .

It will be prudent here to thank **my unit officers, my commanding officer and my colleagues** for their help and assistance. Finally, this work would not have seen the light of the day had it not been for the humble and sincere prayers, sacrifices and good wishes of **my family and well-wishers**. May Allah bless them with prosperous and happy lives and always provide me their loving and thorough guidance.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

1.1 Introduction to the Project

There are a number of IEEE standards for wireless communication like CDMA, WiMax, GSM, WiFi etc used around the globe. Among these WiMax is one of the the most predominant technology used now a days. Another means of high speed wireless communication between end systems (PCs, video consoles, laptops, smart phones, Tablet PCs etc.) is the Wi-Fi/WLAN. The coverage of WiFi/WLAN in the course of one or more interconnected access points called a hotspot, which can illuminate an area as small as one room or as large as many miles covered by cascaded access points.

New IEEE standards of communications in present era have grown which differs to each other in a variety of their technical characteristics and are being implemented with great success. But the question arises, is there any way to bring these communication standards to a common platform so that a end user device working in a particular standard can operate in any other standard, as well. The heterogeneity of these access technologies can be overcome by the development of one platform which will provide ultimate freedom to end users. This will be implemented by equipping their handheld terminals with more than one radio interfaces and activation of only single radio interface at given instant of time. The network selection will be made on the basis of the information, about the network presently used by the mobile, accessible/available networks, and certain QoS parameters of serving and available networks [2]. This gave rise to the concept of vertical/heterogeneous handovers between different environments.

By definition, a handover means transfer of client connection from one radio channel to other [3]. Predominantly handover is used to provide the incessant connectivity to the end user when it moves from coverage area of one Base Station (BS) to other Base Station (BS) and in wireless communication it is termed as Inter-cell

handover. Another basic type of handover is intra-cell handover, where, either the physical channel or the timeslot configuration is changed. This may become unavoidable if the connection on a channel is impaired. In order to complete this, the connection quality is continuously evaluated. In case of an intra-cell handover, the Base Station (BS) informs the end user device about the new channel number and the timeslot configuration. The hand held changes directly to the new channel and is able to maintain its previous settings for timing and the BS parameters. If an end user moves from one cell to another during a call, it must be handed over to the new cell and it can be done, if the adjacent cell is time-synchronized with the current cell, therefore base station kick off a fine synchronized inter-cell handover. In this case, the user connection is transferred to the new channel in the neighboring cell.

We can also differentiate handovers on the source of technologies. If handover occurs within alike technology network, it is known as horizontal handover. In this end user moves from one cell to another, within the same system, the user connection is transferred from one radio channel to another. This procedure is called as Horizontal Handover or intra-technology handover. Horizontal Handover is employed for intra-technology mobility for same / alike environments [6].

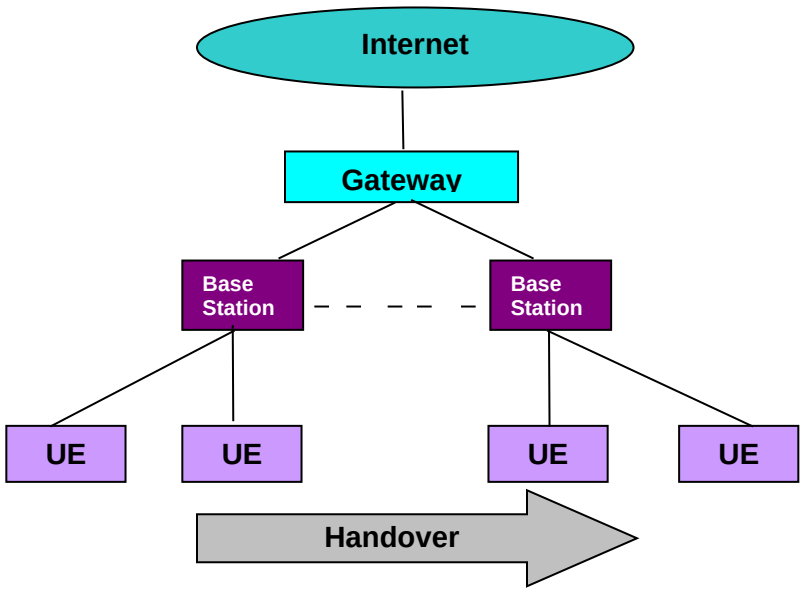

Figure 1-1 Horizontal Handover

If handover occurs between two different networks, it is known as vertical handover. Vertical Handover is the handover that occurs between two different access technologies network. It is also termed as inter-technology handover, where user connection can be shifted from one technology radio channel to a other technology radio channel. Since vertical handover occurs between different types of networks / systems with the condition of prior entering to the core network. For example, during a call, the end user may enter an area where its own network coverage finished and it might be handed over to other available network. This requires that the host maintains continuity while it is being handed over from one interface to another. To fillfill this, we need to find optimum handover solutions / Interoperability at Radio level for one interface activated at one time, without disconnecting the call.

My research investigates the mechanisms of Vertical Handover / interoperability between two systems WiMax and WiFi. The broader aspect of my thesis is to allow users from different technologies, agencies or areas, to use any base system of the network to communicate. This will allow agencies of the federal state / provincial government or private sector such as law enforcement, ambulance services and crisis management agencies to communicate more effectively with each other when out of their coverage area. Interoperability between these two systems is a step towards developing a single platform initiated by Project 25.

Project 25 is a joint venture among public safety society and industry manufacturers whose aim is the development of standards that facilitate the operation of interoperable of wireless systems that meet operation-significant needs of public safety. Project 25 was started in 1989 with head of te departments from local, state, and federal government agencies have grouped to assess highly developed technologies for private wireless systems and land mobile wireless systems particularly for public safety. With the signing of MOU in 1991 with Telecommunications Industry Association, to use the resourcefulness of the TIA to accomplish the technical requirements of the said project highlighted the importance and need of this global cause.

Project 25 will become a standard for digital wireless communication, which will be used by local public safety agencies in America and will further make possible to pass or

handover necessary information to emergencies responding team during nature calamities. Project 25 team with various disaster responding organization and public precautionary or safety association under the umbrella of Telecommunications Industry Association (TIA) will develop and agree on standard which will be uniformly followed by all agencies for handover or interoperability for effectively deployable wireless communication systems. So it will be landmark for wireless systems to use all available infrastructures for communicating with own subscribers using their counter part wireless communication systems infrastructures and particularly during natural calamities or the day of need. The systems of Project 25 are internationally operating in more than 60 countries and overall in six continents. Potentially, all the networks of entire globe will be interoperable, and this is the eventual objective of P-25.

The idea for my research came into light when it was realized that it could be possible to use commercial wireless communication systems along with Project 25 systems for achieving the overall concept of interoperability through single platform. The inspiration for this Interoperability will be helpful to achieve a concept of Global Access Network.

The objectives set for this project is to use the resources of the WiFi systems to facilitate voice communication between end users instead of the WiMax resources, when available. This would make the calls free and also free up the WiMax resources enabling the operator to increase its customer base. This will be achieved by simulating WiMax and Wi-Fi systems according to the set standards, the development and simulation of a module capable of identifying these two systems in different environments and the development of a technique for making both the systems able to communicate with each other and making a module to test the interoperability process under given channel condition.

1.2 Motivation

The partnership between the public safety communications organizations and industry manufacturers under the umbrella of Project 25, initiated a step of interoperability for government or private law enforcement agencies, ambulance services and crisis management centers, to communicate more efficiently among each other when out of

their coverage area. Interoperability provides an striking solution to communicate with the infrastructure of different communication network at low / no signal strength of the parent system.

The motivation of this research is not to limit this global cause to only public safety communication systems but this is to be extended to commercial wireless communication systems which were more distinct after Indian Ocean earthquake and later on Tsunami which devastated the communication infrastructures in their respective areas. Telecommunications for Disaster Relief (TDR) by ITU has anticipated establishing worldwide standard for interoperability which will pave a major role for availability of communication during natural calamities.

The idea of interoperability for two commercial wireless communication systems (WiMax and WiFi) is a step towards the availability of communication on the day of need as a global cause.

1.3 Problem Statement

To achieve the goal of interoperability between different public safety communication systems (P25) and commercial wireless systems, series of project has been initiated i.e. Interoperability between, Tetra & Tetrapol, Edacs & Tetrapol, Fhma & Tetra and WiMax & Lte. This combination of public safety communication systems and commercial wireless communication system for achieving a single platform of interoperability will achieve the overall concept of Global Access System. The interoperability of chosen commercial systems i.e. WiFi and WiMAX will play a major role for achieving this global cause, but at the same time it is challenging to obtain seamless handover between these two commercial wireless systems.

The focus of this thesis is to implement a scenario where interoperability / vertical handover from WiMax to WiFi and vice versa can be simulated. For the realization of the above statement, the subscriber side of WiMax and WiFi are first implemented followed by interoperable module.

1.4 Scope

This thesis is a proof of concept for the realization of a step towards global access network where all the networks can be interoperable and the user can get an “always ON” connectivity.

The scope of this thesis is limited to interoperability between radio terminal of two technologies; WiMAX and WiFi. The reason is that both the technologies are OFDM based and share number of other similarities in their specifications and frame format. Interoperability will be achieved by realizing handover on physical layer level. The trigger for the handover is state of own network signal strength and availability of other network signal strength. If the signal strength of parent network is not available or is lower to maintain the call vis-à-vis the signal strength of interoperable network is available to maintain a call, the handover becomes mandatory.

The very first step is the development of WiMAX and WiFi systems for both subscriber side followed by an identifier to checks for the signal strength of the network under use and then handover, if necessary.

1.5 Domain

This project is step towards development of a telecom standard for establishment of a global access network. The realization of this concept is done by having inter-technology handover between WiMAX and WiFi. The Simulation is done using Lab View 8.6.

1.6 Thesis Organization

Chapter 1 gives the introduction of the research area its motivation and defines it scope and highlight the problem area in the domain of achieving Interoperability / vertical handovers. **Chapter 2** gives the brief concept of vertical handover and discusses the WiMAX and WiFi technologies in detail along with basic concept of interoperability and simulator Lab View. **Chapter 3** illustrates the simulation of sub VIs used in Lab View 8.6. These includes sub VIs used for simulating WiMax, WiFi system and different handover scenarios. **Chapter 4** will illustrates the complete design of WiMax, WiFi

transceiver in physical layer and Handover/ Interoperability scenarios in the forms of complete VI. In **Chapter 5**, the results of individual simulated systems and seamless handover solution through Network Identifier and its implementation has been discussed in detail. **Chapter 6** has concluded the research work and defined the future scope/ prospectus and way forward to achieve the global cause of interoperability.

Chapter 2

2.1 Handover

Principally handover is used to provide the permanent connectivity to the last subscriber when it shifts from coverage area of one network to other network. The handover that is emphasized in this project is vertical handover, which is needed for seamless transfer of subscriber connection from WiMax to WiFi.

2.1.1 Vertical Handover

Vertical Handover is the handover that takes place between two dissimilar access technologies. It is also known as inter-technology handover. An example of such handover can be a transfer of a subscriber connection from a WiMAX radio channel to WiFi radio channel without causing the on-going call to get disengaged.

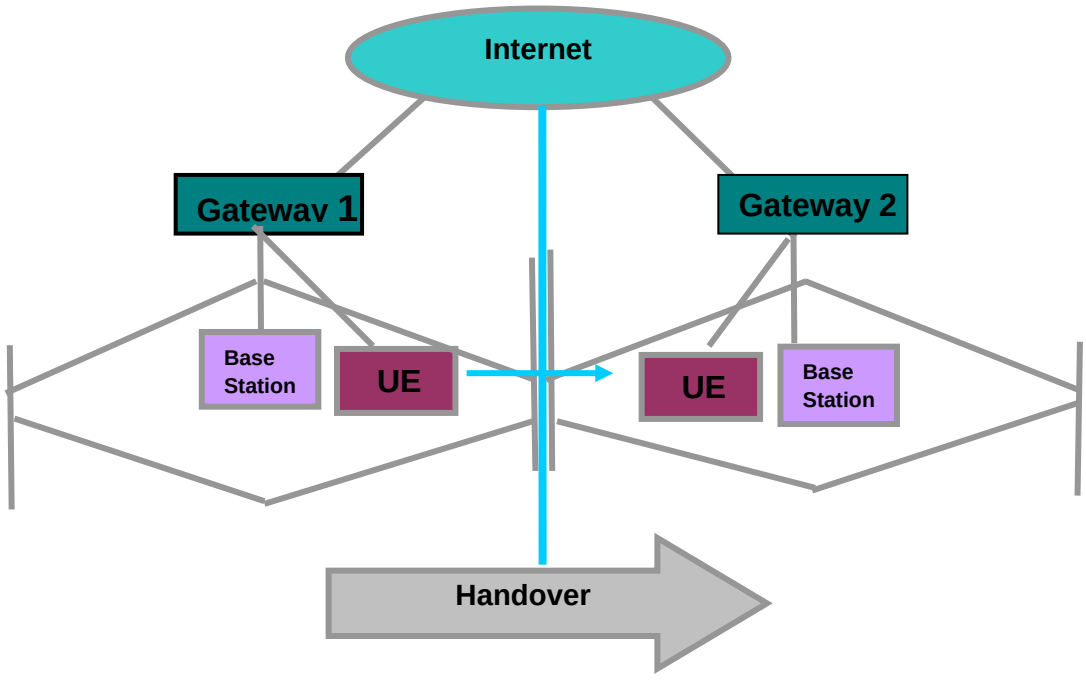

Figure 2-1 Vertical Handover

Following factors trigger the process of transition / handover from one network to another covering all global aspects:

Low signal strength of network under use.

Coverage limitations / non availability faced by network under use.

To remain always in communication or never out of communication.

Seamless transfer of network without disconnection of call.

System integrity is maintained (as it is not the case in switching).

Parent network feature not compromised /remains same regardless to system it is handed over.

Vertical handover has permitted the mobile user to pick the best available network when out of coverage zone. In other words, it can be said that mobility between various networks has now become possible due to vertical handover. There are two criterion to achieve vertical handover. They are explained below.

Hard handover is used when the communication channel is released first and then the new channel is acquired from the neighboring cell. Thus, there is a certain service interruption when the handover occurs decreasing the quality of service.

Soft handover allow multiple connections with neighboring cells. Each user maintains an active set of base stations / hotspots who's received signal strength exceeds a predefined threshold and removes them when the signal strength drops below another threshold value for a given amount of time. When presence or absence of a BS to the active set is encountered, soft handover occurs without disruption of service.

2.2 WiMAX – (Worldwide Interoperability for Microwave Access)

WiMAX is an IEEE standard defined by 802.16. The standard was first introduced in 2001 and from then it is being continually updated and improved. It is a Broadband Wireless Access (BWA) solution which is designed to provide high speed and a high quality connection over a large area. WiMAX is supported by an standardized interface that can support a multiple user types including nomadic users, mobile/high-speed users, and business users.

WiMAX is a revolutionary wireless technology that has a diverse set of technological improvements. It can support incredibly high peak data rates. Theoretically it offers 75 Mbps on downlink and 50 Mbps on uplink whereas practical data rates are 50Mbps on downlink and 20Mbps on uplink. It works with both time division duplex (TDD) and frequency division duplex (FDD) that helps in band management, transceiver design and low cost system development. TDD is favored by a greater part of implementations because of its advantages:

Flexibility in choosing uplink-to-downlink data rate ratios,

Ability to exploit channel reciprocity,

Less complex transceiver design.

The mobile WiMAX provides mobility and there are several mechanisms for handover defined for the mobile users switching from one WiMAX cell to another. In addition to intra-system handover, WiMAX also supports inter-system handovers. Extensive research is in progress to seek new ways to establish interoperability between WiMAX and other technologies.

Table 2-1 summarizes important WiMAX features[9].

FEATURES	**TECHNIQUES USED**
Frequency Range	2 – 66GHz
Bandwidth	1.25, 2.5, 5, 10, 20 MHz
Mobility	Up to 120km/hr
Transmission Technique	OFDM
Duplex Mode	TDD/FDD
Coding Schemes	Convolution Coding,
Modulation Schemes	QPSK ½, 1/3 , QAM
Antenna Techniques	Space-Time Coding, MIMO etc.
Error detection and correction	ARQ, HARQ

Table 2-1 Techniques used in WiMAX Standard

2.3 Salients of WiMax System

WiMAX offers a diverse set of features in addition with a lot of flexibility in terms of deployment options and potential service offerings. Some of the other salient features that deserve highlighting are as follows:

The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to function in NLOS conditions. OFDM is now widely acknowledged as the method of choice for mitigating multipath for broadband wireless.

WiMAX is capable of supporting extremly high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating in a 20MHz2 wide spectrum. More typically, using a 10MHz spectrum operating in TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is approximately 25Mbps and 6.7Mbps for the downlink and the uplink, respectively. These peak PHY data rates are achieved when using QAM modulation with rate 5/6 error-correction coding. Under high-quality signal conditions, even higher peak rates may be achieved using multiple antennas and spatial multiplexing.

WiMAX has a scalable physical-layer architecture that allows the data rate to scale effortlessly with available channel bandwidth. This scalability is supported in the OFDMA mode, where the FFT (fast fourier transform) size may be scaled depending on the offered channel bandwidth. For example, a WiMAX system may use 128,512 or 1,048-bit FFTs based on either the channel bandwidth is 1.25MHz, 5MHz, or 10MHz, respectively. This scaling may be done dynamically to support subscriber roaming across different networks that may have different bandwidth allocations.

MAX supports many modulation and forward error correction (FEC) coding schemes and permits the scheme to be changed on a per user and per frame basis, depending on channel conditions. AMC is an useful mechanism to maximize throughput in a time-varying channel. The adaptation algorithm typically calls for the use of the highest modulation and coding scheme that can be supported by the signal-to-noise and interference ratio at the receiver such that each subscriber is

provided with the highest achievable data rate that can be supported in their respective links.

For connections that call for enhanced reliability, WiMAX supports automatic retransmission requests (ARQ) at the link layer. ARQ-enabled connections require each transmitted packet to be acknowledged by the receiver so unacknowledged packets are considered to be lost and are then retransmitted. WiMAX furthermore optionally supports hybrid-ARQ, which is an efficient hybrid between FEC and ARQ.

Support for TDD and FDD: IEEE 802.16-2004 and IEEE 802.16e-2005 support both time division duplexing and frequency division duplexing, as well as a half-duplex FDD, which permits a low-cost system implementation. TDD is preferred by a majority of implementations because of its flexibility in selecting uplink-to-downlink data rate ratios, ability to take advantage of channel reciprocity, ability to implement in no paired spectrum and less composite transceiver design. All the initial WiMAX profiles are based on TDD, excluding two fixed WiMAX profiles in 3.5GHz.

Mobile WiMAX utilizes OFDM as a multiple-access technique, whereby different users can be allocated dissimilar subsets of the OFDM tones. OFDMA facilitates the utilization of frequency diversity and multi-user diversity to significantly improve the system capacity.

Flexible and dynamic per user resource allocation: Both uplink and downlink resource allocation are looked after by a scheduler in the base station. Capacity is shared among several users on a demand basis, by means of a burst TDM scheme. When using the OFDMA-PHY mode, multiplexing is also done in the frequency dimension, by allocating different subsets of OFDM sub carriers to different users. Resources may also be allocated in the spatial domain when using the optional advanced antenna systems (AAS). The standard allows for bandwidth resources to be allocated in time, frequency, and space and has a flexible method to transmit the resource allocation information on a frame-by-frame basis.

The WiMAX solution has a number of hooks built into the physical-layer design, which permits the use of multiple-antenna techniques, such as beam forming, space-time coding, and spatial multiplexing. These schemes can be used to

enhance the overall system capacity and spectral efficiency by deploying multiple antennas at the transmitter and/or the receiver end. The WiMAX MAC layer has a connection-oriented architecture that is designed to support a number of applications, including voice and multimedia services. The system offers support for both constant and variable bit rate, real-time and non-real-time traffic flows, in addition to best-effort data traffic. WiMAX MAC is designed to support a large number of subscribers, with multiple connections per terminal, each having its own QoS requirement. Robust security: WiMAX supports strong encryption, using Advanced Encryption Standard (AES), and has a robust privacy and key-management protocol. The system also offers an extreme flexible authentication architecture based on Extensible Authentication Protocol (EAP), which allows for a variety of user credentials, including username/password, digital certificates, and smart cards support for mobility. The mobile WiMAX variant has mechanisms to support protected seamless handovers for delay-tolerant full-mobility applications, such as VoIP. The system also has built-in support for power-saving mechanisms that increase the battery life of handheld user devices. Physical-layer improvements, such as more frequent channel estimation, uplink sub channelization, and power control, are also specified in support of mobile applications.

IP-based architecture: The WiMAX Forum has defined a reference network architecture that is based on an all-IP platform. All end-to-end services are delivered over an IP architecture depending on IP-based protocols for end-to-end transport, QoS, session management, security, and mobility. Dependence on IP allows WiMAX to ride the declining cost curves of IP processing, facilitate easy convergence with other networks and exploit the rich ecosystem for application development that exists for IP.

2.4 WiMAX Protocol Architecture

WiMAX Protocol Architecture comprises two OSI Layers; Physical Layer and MAC Layer. Physical Layer is responsible for encoding and decoding of signals, preamble generation and removal, and bit transmission and reception. Medium Access Control Layer accepts data from higher layers, assembles it into frames and then hands over these frames to physical layer. On receiving data from physical layer, it de- assembles the

frame, Figure 2.2 shows detailed protocol architecture of WiMAX [10]

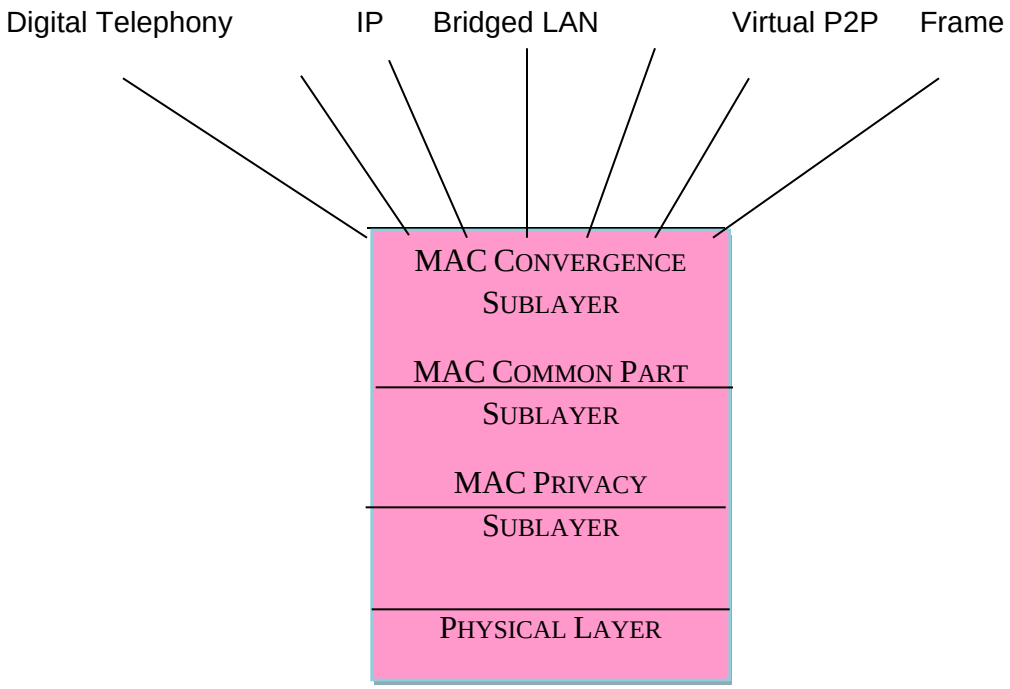

Figure 2-2 WiMAX Protocol Architecture

2.4.1 WiMAX Physical Layer

In 802.16 standard, five physical interfaces are defined which are summarized in Table 2.2.

DESIGNATION	FREQUENCY BAND	DUPLEXING	MAC OPTIONS
WirelessMAN-SC	10 – 66GHz (LOS)	TDD and FDD	-----
WirelessMAN-SCa	Below 11GHz (NLOS) Licensed	TDD and FDD	AAS, ARQ, STC, mobility
WirelessMAN-OFDM	Below 11GHz Licensed	TDD and FDD	AAS, ARQ, STC, mesh, mobility
WirelessMAN-OFDMA	Below 11 GHz Licensed	TDD and FDD	AAS, ARQ, HARQ, STC, mobility
WirelessHUMAN	Below 11 GHz License Exempt	TDD Only	AAS, ARQ, HARQ, STC, Only with mesh

Table 2-2 WiMAX PHY Interfaces

The main processes taking place at physical and LLC layer are channel coding, modulation and OFDM transmission on the transmitter side. On the receiver end, the reverse process takes place.

2.4.2 Modulation

WiMAX supports QPSK and QAM. WiMAX uses these schemes as frame basis, based on channel conditions. Flexibility in coding scheme is a useful mechanism to maximize throughput in a time-varying channel. In few flavors, it supports adaptive modulation scheme. In this algorithm a system will be helpful for using the better modulation and coding schemes with logical support of SNR and interference ratio at user end to get best data rates for the respective link.

The adaptive modulation and coding depends on the distance between the mobile subscriber and the base station. As the distance between the mobile user and it's serving base station increases, the signal strength drops due to the channel conditions and larger separation area. This low signal strength indicates that there are more chances of error. In this case, a low rate modulation schemes and codes are supported. The reason for using lower order modulation scheme such as QPSK is that the number of constellation points is lower as well as the number of information bits mapped on each constellation points is less. Hence we get clearer judgment boundary and even the erroneous data can be received correctly with low bandwidth usage. On the other hand when the distance between the mobile station and the base station decreases, the signal strength improves and a higher order modulation is preferred.

2.4.3 Orthogonal Frequency Division Multiplexing (OFDM)

The WiMAX physical layer (PHY) is based on Orthogonal Frequency Division Multiplexing (OFDM). OFDM us orthogonal sub-carriers and has inherent capabilities for error detection and correction. It offers high resistance to multipath resistance and permits WiMAX to operate in NLOS conditions.

Orthogonal Frequency Division Multiplexing (OFDM) is a multiplexing technique that further divides the bandwidth into multiple frequency sub-carriers as shown in Figure 2.3.

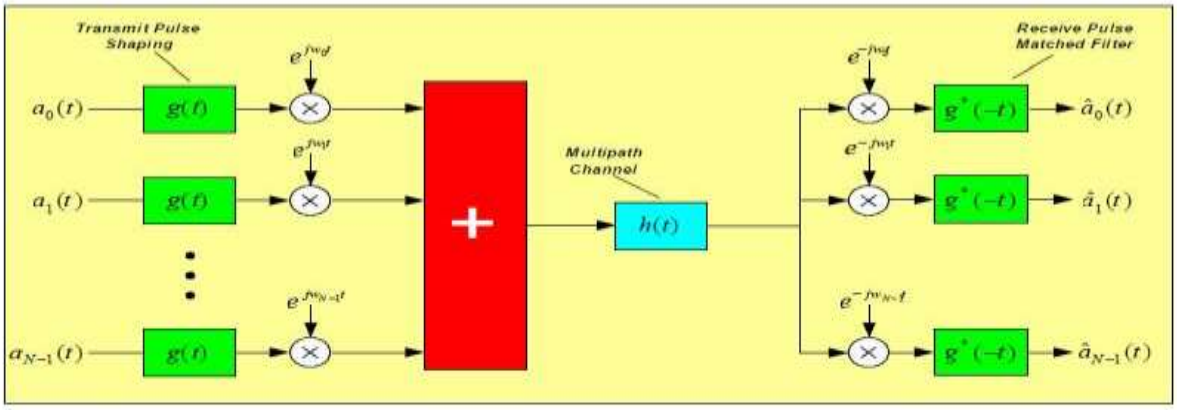

Figure 2-3 Basic Architecture of an OFDM System

In an OFDM system, the input data stream is divided into several parallel sub-streams of decreased data rate (thus increased symbol duration) and each sub-stream is modulated and sent on a separate orthogonal sub-carrier. The increased symbol duration enhances the robustness of OFDM to delay spread. Furthermore, the introduction of the cyclic prefix (CP) can completely remove Inter-Symbol Interference (ISI) as long as the CP time is longer than the channel delay spread. The CP is typically a repetition of the last samples of data portion of the block that is appended to the beginning of the data payload as shown in Figure 2.4.

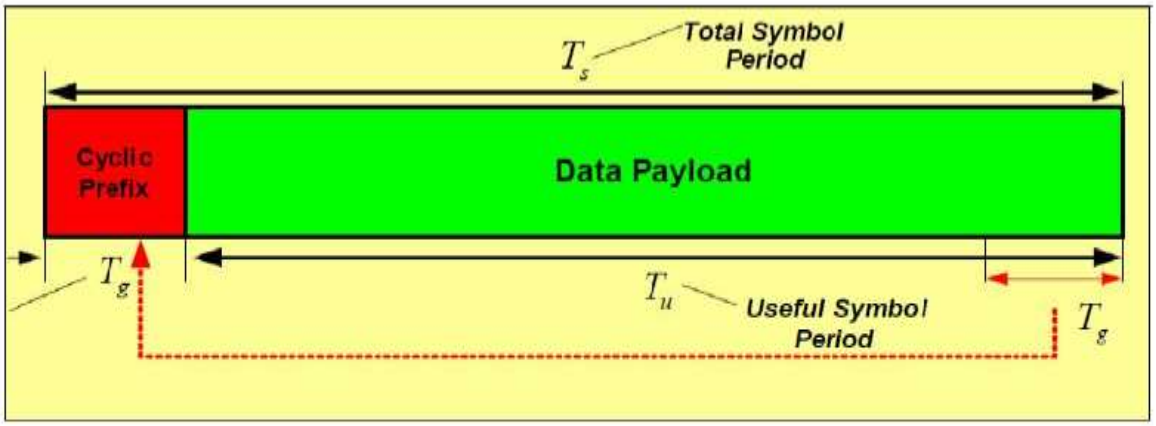

Figure 2-4 Insertion of Cyclic Prefix

The CP prevents inter-block interference and makes the channel appear circular and permits low-complexity frequency domain equalization. A perceived drawback of CP is that it introduces overhead, due to which bandwidth efficiency reduces. Since OFDM has a very sharp and like a "brick-wall" spectrum, a large fraction of the allocated channel

bandwidth may be utilized for data transmission, which helps to moderate the loss in efficiency due to the cyclic prefix.

OFDM effectively utilizes the frequency diversity of the multipath channel by coding and interleaving the information across the sub-carriers before transmission. OFDM modulation can be realized with efficient Inverse Fast Fourier Transform (IFFT), which enables a large number of sub-carriers (up to 2048) with low complexity.

In an OFDM system, resources are available in the time domain by means of OFDM symbols and in the frequency domain by means of sub-carriers. The time and frequency resources can be structured into sub-channels for allocation to individual users. Orthogonal Frequency Division Multiple Access (OFDMA) is basically a multiple-access/multiplexing scheme that allows multiplexing operation of data streams from multiple users onto the downlink sub-channels and uplink multiple accesses by means of uplink sub-channels.

2.4.3.1 OFDMA Symbol Structure and Sub-Channelization

The OFDMA symbol structure consists of following three types of sub-carriers:

Data sub-carriers for data transmission

Pilot sub-carriers for estimation and synchronization purposes

Null sub-carriers for no transmission; used for guard bands and DC carriers

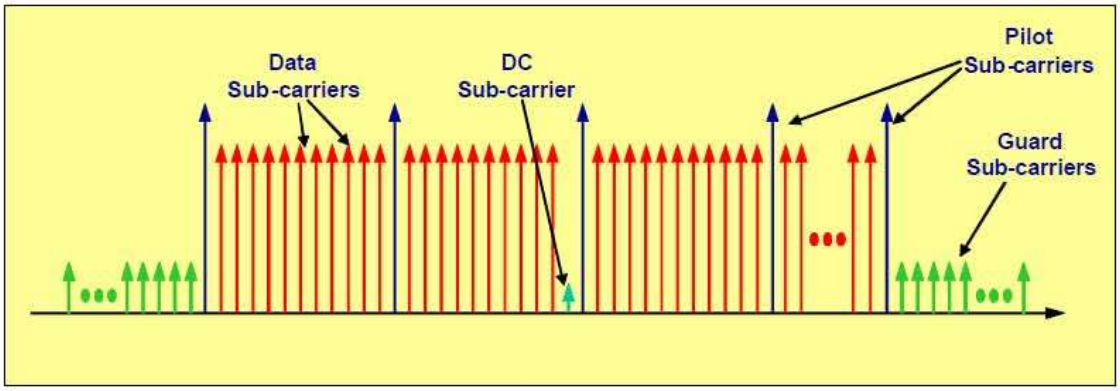

Figure 2-5 OFDMA Sub-Carrier Structure

Active (data and pilot) sub-carriers are grouped into subsets of sub-carriers. Theses groups are called sub-channels. The WiMAX OFDMA Physical layer supports sub-

channelization in both DL and UL. The smallest frequency-time resource unit of sub-channelization is one slot, which is equal to 48 sub-carriers.

2.4.3.2 Scaleable OFDMA

The IEEE 802.16e-2005 Wireless MAN OFDMA mode is based on the concept of scalable OFDMA which is also known as S-OFDMA. S-OFDMA supports a wide range of bandwidths to flexibly cater the need for various spectrum allocation and usage model requirements.

Transmission power for the uplink and downlink is not same; therefore one of the most important aspects in the uplink design is to enable highly power-efficient transmission. This improves coverage and decreases terminal cost and power consumption at the transmitter. Due to this reason, single-carrier transmission, based on discrete Fourier transform (DFT)- pre-coded OFDM, sometimes also known as Single Carrier frequency-division multiple access (SC-FDMA), is used for the WiMax uplink. Single Carrier FDMA has a smaller peak-to-average power ratio than regular OFDM, thus allowing less complex and/or higher-power terminals.

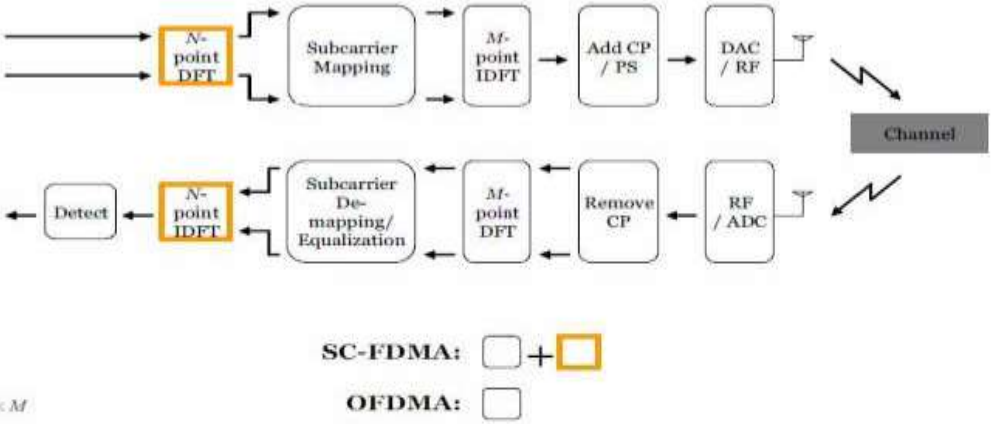

Figure 2-6 OFDMA and SC-FDMA Block Diagram

SC-FDMA may be regarded as DFT-spread orthogonal frequency division multiple access (OFDMA), where time domain data symbols are transformed to frequency domain by DFT before going through OFDMA modulation. Figure 2.6 shows a block diagram of OFDMA and SC-FDMA.

2.5 WiMAX MAC Layer

The WiMAX MAC layer provides an interface between physical layer and higher transport layers. It comprises three sub-layers.

MAC Convergence Sublayer

MAC Common Part Sublayer

MAC Privacy Sublayer

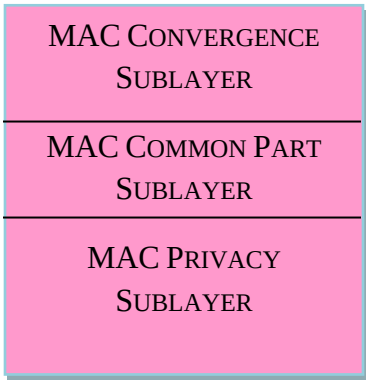

Figure 2-7 MAC Sublayers

2.5.1 MAC Convergence Sub Layer

The service-specific MAC Convergence Sub-layer (CS) is the top most sub layer in WiMAX protocol architecture. It maps external network data into MAC Service Data Units and forwards it to MAC Common Part Sub layer through the MAC Service Access Point. In addition to mapping of data, this sub layer performs another important task of Payload Header Suppression (PHS). It suppresses redundant payload header fields on transmission of data and re-establish the headers on its reception.

2.5.2 MAC Common Part Sub Layer

The MAC Common Part Sublayer exists between MAC Convergence Sublayer and MAC Privacy Sublayer. It provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. It carries out fragmentation and packing of the data and applies different Quality of Service (QoS) profiles to the transmission and scheduling of data over the physical layer.

2.5.3 MAC Privacy Sub Layer

The MAC Privacy Sublayer resides between MAC Common Part Sublayer and Physical Layer. It provides support for mutual device/user authentication, flexible key management protocol, strong traffic encryption, control and management plane message protection and security protocol optimizations for fast handovers.

2.5.4 Hybrid ARQ (HARQ)

The Hybrid Automatic Repeat-request (HARQ) process, accomplished in combination between the MAC and the Physical Layer, resends transport blocks for error recovery. The Physical layer performs the retention and re-combination (incremental redundancy) and the MAC performs the management and signaling.

Whenever there is a transport block CRC failure, the MAC indicates a NACK whereas the PHY usually indicates that failure. Resending is done by the sender on the downlink using a different type of coding. The coding is sent and retained in buffers. Eventually, after one or two attempts, there will be enough data to recreate the signal. In HARQ operation, the retransmission does not have to be fully accurate. It has to be correct to an extent where it can be combined mathematically with the previous transport block in order to produce a high-quality transport block. This is the most efficient way of providing this ARQ function. It does operate at the transport block level, there is another ARQ process mechanism operating at the RLC.

Following are the basic steps of the HARQ process:

MAC sends "NACK" message when Transport Block (TB) fails CRC

Transport blocks with errors are retained

PHY retransmits with different puncturing code

Retransmission combined with saved transport block(s)

When correct transport block is decoded, MAC signals "ACK"

Multiple HARQ processes can run in parallel to retry several outstanding TBs

Figure 2.11 shows simplified HARQ mechanism.

Figure 2-8 Simplified HARQ operation

2.6 Power-Saving Features

To support battery-operated portable devices, WiMAX has power-saving features that permit portable subscriber stations to function for longer durations without having to recharge.

Power saving is obtained by turning off parts of the MS in a controlled manner when it is not actively sending or receiving data. Mobile WiMAX defines signaling methods that permit the MS to retreat into a sleep mode or idle mode when inactive.

Sleep mode is a state in which the MS effectively turns itself off and becomes unavailable for predetermined periods. The periods of absence are negotiated with the serving BS. WiMAX describes three power-saving classes, based on the manner in which sleep mode is implemented. When in Power Save Class 1 mode, the sleep window is exponentially increased from a minimum value to a maximum value. This is typically done when the MS is doing best-effort and non-real-time traffic. Power Save Class 2 has a fixed-length sleep window and is used for UGS service. Power Save Class 3 permits for a one-time sleep window and is typically used for multicast traffic or management traffic when the MS knows when the next traffic is expected. In addition to minimizing MS power consumption, sleep mode conserves BS radio resources. To facilitate handoff while in sleep mode, the MS is permitted to scan other base stations to assemble handoff-related information.

Idle mode allows even larger power savings, and support for it is optional in WiMAX. Idle mode permits the MS to completely turn off and to not be registered with any BS and yet receive downlink broadcast traffic. When downlink traffic comes for the idle-mode MS, the MS is paged by a group of base stations that form a paging group. The MS is assigned to a paging group by the BS before going into idle mode, and the MS periodically wakes up to update its paging group. Idle mode haa the capability to save more power than sleep mode, since the MS does not even have to register or do handoffs. Idle mode is also adventitious for the network and BS by removing handover traffic from inactive MSs.

2.7 Mobility Support

With fixed broadband access, WiMAX pictures four mobility-related usage scenarios:

Nomadic. The user is permitted to take a fixed subscriber station and reconnect from a different point of attachment.

Portable. Nomadic access is given to a portable device, such as a PC card, with expectation of a best-effort handover.

Simple mobility. The user may move at speeds up to 60 kmph with short interruptions (less than 1 sec) during handoff.

Full mobility: Up to 120 kmph mobility and seamless handoff (less than 50 ms latency and <1% packet loss) is supported.

It is likely that WiMAX networks will at first be deployed for fixed and nomadic applications and then advance to support portability to full mobility over time. The IEEE 802.16e-2005 standard describes a framework for supporting mobility management. Specifically, the standard defines signaling mechanisms for tracking user stations as they move from the coverage range of one base station to another when active or as they move from one paging group to another when idle. The standard also has protocols that enables a seamless handover of ongoing connections from one base station to another. The WiMAX Forum has utilized the framework defined in IEEE 802.16e-2005 to develop more mobility management within an end-to-end network architecture framework.

The architecture also has a facility of supporting IP-layer mobility using mobile IP. Three handoff methods are supported in IEEE 802.16e-2005; in which one is mandatory and rest of the two are optional. The mandatory handoff method is known as *hard handover* (HHO) and is the only type needed to be implemented by mobile WiMAX in the start. HHO implies a quick transfer of connection from one BS to another. The handoff decisions are made by the BS, MS, or another entity, dependent on measurement results reported by the MS. The MS does a radio frequency (RF) scan on periodic basis and measures the signal quality of neighboring base stations. Scanning is performed during *scanning intervals* allocated by the BS. During these intervals, the MS is also permitted to optionally carry out initial ranging and to associate with one or more neighboring base stations. Once a handover decision is taken, the MS starts synchronization with the downlink transmission of the target BS, performs ranging if it was not done while scanning, and then finishes the connection with the previous BS. Any undelivered MPDUs at the BS are retained until a timer expires.

The two elective handoff methods supported in IEEE 802.16e-2005 are *fast base station switching* (FBSS) and *macro diversity handover* (MDHO). In these two methods, the MS retains a valid connection simultaneously with more than one BS. In the FBSS case, the MS keeps a list of the BSs involved which is called the *active set*. The MS continuously monitors the active set, does ranging, and upholds a valid connection ID with each of them. The MS, however, communicates with only one BS, called the *anchor BS*. When a change of anchor BS is needed, the connection is switched from one base station to another without having to explicitly execute handoff signaling. The MS simply reports the selected anchor BS on the CQICH. Macro diversity handover is analogous to FBSS, except that the MS communicates on the downlink and the uplink with all the base stations in the active set—called a *diversity set* here-simultaneously. In the downlink, various copies received at the MS are combined using any of the well-known diversity-combining techniques (see Chapter 5). In the uplink, where the MS transmits data to multiple base stations, selection diversity is the phenomenon which is applied performed to pick the best uplink. Both FBSS and MDHO offer greater performance to HHO, but they need that the base stations in the active or diversity set be synchronized, use the

same carrier frequency, and share network entry–related information. Support for FBHH and MDHO in WiMAX networks is not fully achieved yet and is also not part of WiMAX Forum Release 1 network specifications.

2.8 Security Functions

WiMAX systems were designed at the outset with an idea of robust security in mind. The standard includes state-of-the-art schemes for ensuring subscriber data privacy and disallowing unauthorized access, with additional protocol optimization for mobility. Security is controlled by a privacy sub layer within the WiMAX MAC. The key aspects of WiMAX security are as follow.

Support for privacy: User data is encrypted using different cryptographic schemes of proven robustness to ensur privacy. Both AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard) are supported. Most system implementations will likely use AES, as it is the recent encryption standard approved as acquiescent with Federal Information Processing Standard (FIPS) and is also easier to implement.10 The 128-bit or 256-bit key used for deriving the cipher is created during the authentication phase and is also periodically refreshed for further protection.

Device/user authentication: WiMAX provides a flexible means for authenticating subscriber stations and users for avoiding unauthorized use. The authentication framework is based on the Internet Engineering Task Force (IETF) EAP, which supports a number of credentials, such as username/password, digital certificates, and smart cards. WiMAX terminal devices come with built-in X.509 digital certificates that have their public key and MAC address. WiMAX operators have the leverage to use the certificates for device authentication and use a username/password or smart card authentication on top of it for user authentication.

Flexible key-management protocol: The Privacy and Key Management Protocol Version 2 (PKMv2) is used for securely transporting keying material from the base station to the mobile station, this protocol also periodically reauthorize and refresh the keys. PKM is basically a client-server protocol: The MS acts as the client whereas the BS, the server.

PKM utlizes X.509 digital certificates and RSA (Rivest- Shamer-Adleman) public-key encryption algorithms to ensure secure key exchanges between the BS and the MS.

2.9 Protection of control messages:

The reliability of over-the-air control messages is protected by utlizing message digest schemes, for e.g AES-based CMAC or MD5-based HMAC.11

Support for fast handover: To support fast handovers, WiMAX permits the MS to utilize preauthentication with a specific target BS to ensure accelerated reentry. A three-way handshake scheme is supported to optimize the reauthentication procedures for aiding fast handovers and also preventing any man-in-the-middle attacks.

2.10 WI-FI SYSTEM

Every device that broadcasts a radio signal performs this task at a particular frequency, which is the oscillations, or movement from peak to trough, of the electromagnetic wave created by the transmission. The entire set of radio frequencies is termed as the radio spectrum. Contiguous portions of the radio spectrum are known as bands. Radio frequencies explain the oscillations of a radio wave. For example, if you are tuned to an FM radio station at 92.5, it shows that the radio transmission is oscillating at 92.5 megahertz per second. 92.5 megahertz (pronounced "may-ga-hurts" and abbreviated MHz) indicating that the radio transmission wave oscillates, or moves from its valley to its peak, at a rate of 92,500,000 times per second.

As a partial answer to frequency disagreements, the government has regulated the utilization of most of these frequencies. In the United States, government regulation of radio frequencies is controlled by the Federal Communications Commission (FCC)[16].

In wireless comm some frequencies are specified for particular usages, such as the military. Others, such as the AM and FM bands, are basically licensed. This shows that only the licensees can use the frequency for the function it was licensed. In addition, some areas of the spectrum have been kept aside for unlicensed uses. These set-aside areas include the 2.4GHz and 5GHz spectrums, which is what Wi-Fi utlizes. The fact that the 2.4GHz and 5GHz frequencies have been set aside for unlicensed usages does have

an enormously important implication: They are low-priced to use. This approach gives these "free" spectrums an unfair competitive advantage compared to using a spectrum that someone has paid for.

2.10.1 802.11 Standard and Its Variations

In this section, it is intended to give an insight on the basics of IEEE standards for the wireless local area network (WLAN). IEEE 802.11 is the set of standards for WLANs. When the initial version of 802.11 was ratified in 1997, the actual work was only just beginning. The initial version of the standard only had the capability of data rates up to 2 Mbps. 2 Mbps is hardly useful, especially when the transmission capacity has to be shared among all the users in an area. In 1999, the 802.11 its second extension was released by working group, to the basic 802.11 specification. In keeping with the IEEE numbering convention, the second extension was given a label of 802.11b. It increases transmission up to 11 Mbps, which is sufficient for modern networks.

IEEE standard	Speed	Frequency band
802.11	1 Mbps 2 Mbps	2.4 GHz
802.11a	up to 54 Mbps	5 GHz
802.11b	5.5 Mbps 11 Mbps	2.4 GHz
802.11g	up to 54 Mbps	2.4 GHz

Table 2-3 Comparison of various IEEE standards

“IEEE 802 has emphasized on lowest two layers i.e. PHY and Datalink layer. This is done because all the systems using 802 specifications should incorporate PHY and MAC components in their networks. The MAC layer defines the procedure and regulations to access the medium and transmit data and PHY layer defines the all reception and transmission details. Basically 802.11 analyze and define the procedure for personal computers to network using the unlicensed spectrums with various data rates or speed.

Generally, the core 802.11 standard is anticipated to specify a path for computers to network using the 2.4GHz and 5GHz free spectrums and has different flavors and speeds.

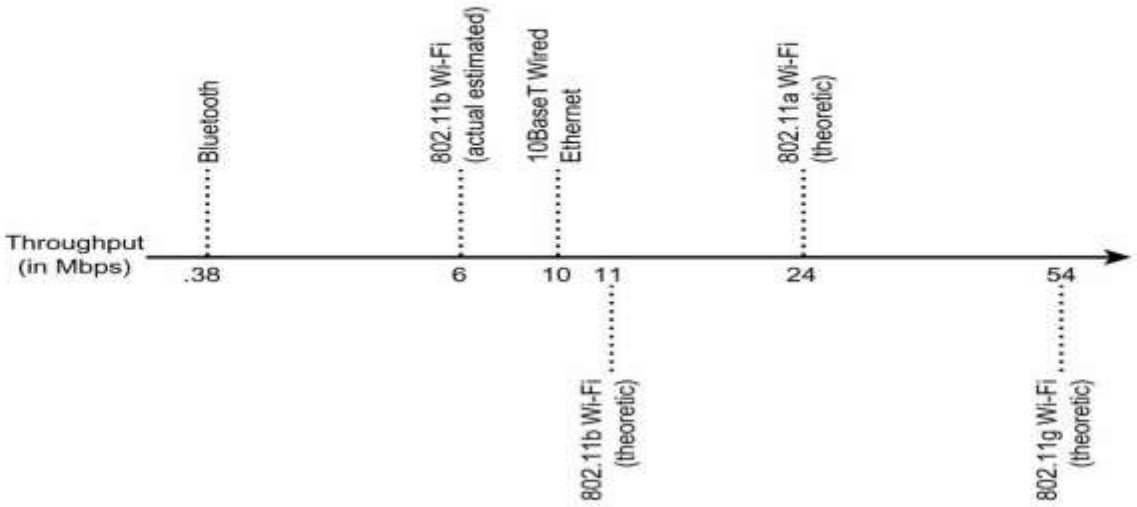

Figure 2-9 802.11 throughputs

2.10.2. The 802.11b Standard

"Wi-Fi" today, refers as 802.11b, which is basically a subset of the general 802.11 standard. Most Wi-Fi devices that are currently in use, are working on 802.11b. However, technology grows quickly, and 802.11g is gaining momentum fast. The key things to know about 802.11b:

The 802.11b standard uses the 2.4GHz spectrum.

The 802.11b standard uses a technology called Direct Sequence Spread Spectrum (DSSS) to decrease interference with other devices transmitting on the 2.4GHz spectrum.

The 802.11b standard has a theoretical throughput speed of 11 megabytes per second (Mbps).

2.10.3 802.11a and 802.11g Standards

The 802.11a and 802.11g standards are basically different variants of 802.11. The 802.11a standard utilizes the 5GHz band for transmission, which reduces the probability of interference with 2.4GHz devices and has theoretical throughput of 24Mbps. 802.11g works on the 2.4GHz spectrum and increases throughput as fast as 54Mbps. 802.11a and

802.11g highlight the promise of being considerably faster than 802.11b. The 802.11a standard poses some compatibility issues with 802.11b.

802.11a has some advantages and disadvantages, but 802.11g is a no brainier because 802.11g systems are backward-compatible with 802.11b, and faster. This backward compatibility of 802.11g devices is a necessity for Wi-Fi certification. 802.11g will be the de facto Wi-Fi standard that is the new contender whereas 802.11n is near to show its capabilities and advantages.

2.10.4 The 802.11 Standard

IEEE is in the progression of developing a new security standard for 802.11 that is called 802.11i. The Wi-Fi Alliance has introduced a subset of the 802.11i called "Wi-Fi Protected Access." Wi-Fi Protected Access gives a better level of encryption and authentication than is built into the present Wi-Fi standards. This implies that Wi-Fi networks will have stronger protection from unauthorized access and other security problems. Wi-Fi Protected Access is made to replace WEP encryption built into current Wi-Fi[18].

2.11 802.11 MAC

The key to the 802.11 specification is the MAC. It goes on all physical layers and controls the transmission of user data into the air. It provides the core framing operations and contact with a wired network backbone. Different physical layers may offer varied transmission speeds, all of which are supposed to interoperate. Fields are transmitted from left to right, and the most important bits appear in the end.

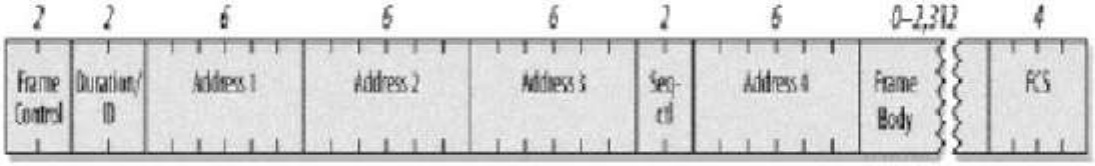

Figure 2-10 The Generic 802.11 MAC frame.

802.11 MAC frames do not contain some of the traditional Ethernet frame features, mainly the type/length field and the preamble. The preamble is an

element of the physical layer, and encapsulation information like type and length are there in the header on the data present in the 802.11 frame.

2.11.1 Frame Control

All frames begin with a two-byte Frame Control subfield. The parts of the Frame Control subfield are:

2.11.1.1 Protocol Version

Two bits specify which version of the 802.11 MAC is enclosed in the rest of the frame. Currently, only one version of the 802.11 MAC has been developed; it is allotted the protocol number 0. Further values will appear when the IEEE standardizes variations to the MAC that make it incompatible with the early specification.

2.11.1.2 Type and Subtype Fields

Type and subtype fields classify the type of frame used. To deal with noise and unreliability, several management functions are included into the 802.11 MAC. These fields indicate whether the nature of frame is data, control or management.

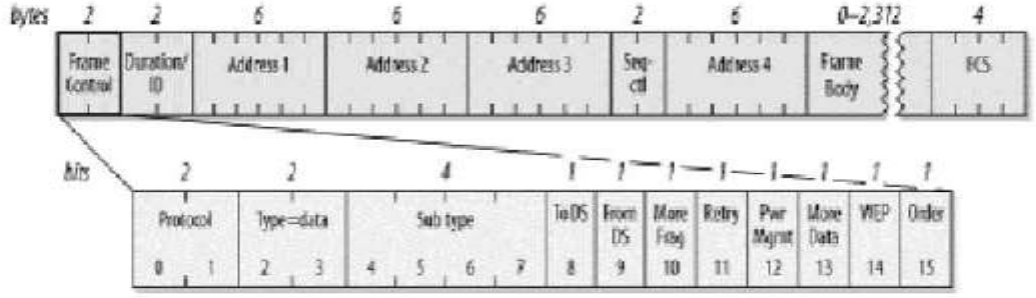

Figure 2-11 Sub-fields of frame control

2.11.1.3 To DS and From DS Bits

These bits specify whether a frame is intended for the distribution system. Every frame on infrastructure networks will contain one of the distribution systems.

	To DS=0	To DS=1
From DS=0	All management and control frames Data frames within an IBSS (never infrastructure data frames)	Data frames transmitted from a wireless station in an infrastructure network
From DS=1	Data frames received for a wireless station in an infrastructure network	Data frames on a "wireless bridge"

Table 2-4 Fragments Bit

When a higher-level packet is fragmented by the MAC, the starting fragment and any following non-final fragments set this bit to 1. Some management frames may be big enough to need fragmentation; all other frames set this bit to 0.

2.11.1.4 Retry Bit

Frames may be retransmitted frequently. Any retransmitted frame set this bit to 1 to assist the receiving station in removing duplicate frames.

2.11.1.5 Power Management Bit

Network adapters made on 802.11 are usually built to the PC Card form factor and utilized in battery-powered laptop or handheld computers. To save battery life,

numerous small devices have the capability to power down parts of the network interface. This bit specifies whether the sender will be in a power-saving mode after the finishing of the existing atomic frame exchange. One shows that the station is in power-save mode, and 0 shows that the station is active.

2.11.1.6 More Data Bit

To house stations in a power-saving mode, access points may buffer frames accepted from the distribution system. An access point sets this bit to specify that at least one frame is accessible and is sent to a dozing station.

2.11.1.7 WEP Bit

Wireless transmissions are naturally simpler to intercept than transmissions on a fixed network. 802.11 classify a set of encryption routines called Wired Equivalent Privacy (WEP) to secure and authenticate data. When WEP has processed a frame, this bit is set to 1, and the frame modified slightly.

2.11.1.8 Order Bit

Frames and fragments can be sent in order at the charge of additional processing by mutually the sending and receiving MACs. When the "strict ordering" delivery is in use, this bit is set to 1.

2.11.2 Duration/ID Field

The value symbolizes the number of microseconds that the medium is likely to stay busy for the transmission presently in progress.

2.11.3 Address Fields

An 802.11 frame may have up to four address fields. The address fields are numbered because various fields are used for various functions depending on the

frame type. Generally Address 1 is used for the receiver, Address 2 for the transmitter, with the Address 3 field utilized for filtering by the receiver.

Length of the addresses is 48 bits. If the foremost bit launched to the physical medium is a 0, the address indicates a single station (unicast). When the foremost bit is 1, the address indicates a group of physical stations and is known as a multicast address. If every bit is 1, then the frame is a broadcast and is sent to all stations connected to the wireless medium. 48-bit addresses are utilized for a number of purposes as discussed below.

2.11.3.1. Destination Address

As in Ethernet, the destination address is the 48-bit IEEE MAC identifier that communicates with the last receiver: the station that will send the frame to upper protocol layers for processing.

2.11.3.2 Source Address

This is the 48-bit IEEE MAC identifier that indicates the source of the transmission. Only single station can be the source of a frame, so the Individual/Group bit is 0 always to indentify an individual station.

2.11.3.3 Receiver Address

It is a 48-bit IEEE MAC identifier that tells which wireless station should start processing the frame. The receiver address is the destination address, if it is a wireless station. For frames sent to a node on an Ethernet linked to an access point, the receiver is the wireless interface in the access point, and the destination address may be a router connected to the Ethernet.

2.11.3.4 Transmitter Address

This is a 48-bit IEEE MAC address which specifies the wireless interface that sent the frame onto the wireless medium. The transmitter address is utilized just in wireless bridging.

2.11.4 Sequence Control Field

This is a 16-bit field utilized for both defragmentation and discarding duplicate frames. It comprises of a 4-bit fragment number field and a 12-bit sequence number field.

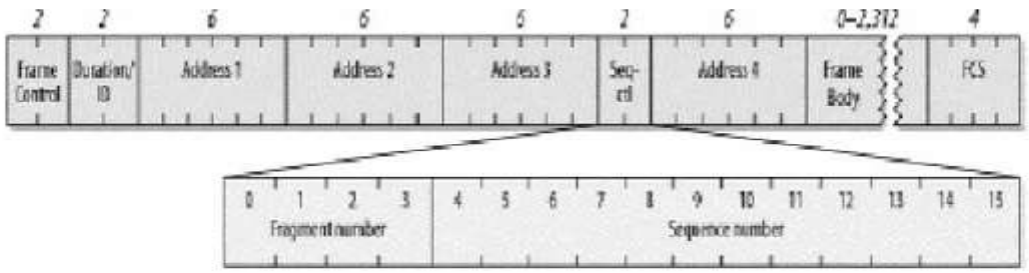

Figure 2-12 Sequence control field

Each higher-level frame is given a sequence number as they are sent to the MAC for transmission. The sequence number subfield works as a modulo-4096 counter of the frames transmitted. It starts at 0 and increments by 1 for each higher-level packet processed by the MAC. If higher-level packets are fragmented, all fragments will have the identical sequence number. When frames are retransmitted, the sequence number is not altered.

Fragment number is what varies between the fragments. The foremost fragment is specified a fragment number of 0. Each following fragment increases the fragment number by one. Retransmitted fragments maintain their original sequence numbers to aid in reassembly.

2.11.5 Frame Body

The frame body, also known as the Data field, shifts the higher-layer payload from one station to other. 802.11 can pass on frames with a highest payload of 2,304 bytes of higher-level data.

2.11.6 Frame Check Sequence

Like Ethernet, the 802.11 frame ends with a frame check sequence (FCS). The FCS is usually referred to as the cyclic redundancy check (CRC) because of the basic mathematical operations. The FCS permits stations to confirm the integrity of received frames. The entire fields in the MAC header and the body of the frame are incorporated in the FCS. The FCS must be again calculated by access points.

2.12 802.11 PHY

The 802.11 PHY is also called as the high-rate, direct-sequence PHY, abbreviated HR/DS or HR/DSSS. The utilization of radio waves as a physical layer involves a comparatively complex PHY. 802.11 divides the PHY into two major components i.e. PLCP and PMD, the first one's job is to map the frame to physical medium and later has a job to Xmitt those frame. The PLCP adds a number of fields to the frame as it is Xmitted to the air.

2.12.1 High-Rate, Direct-Sequence PLCP

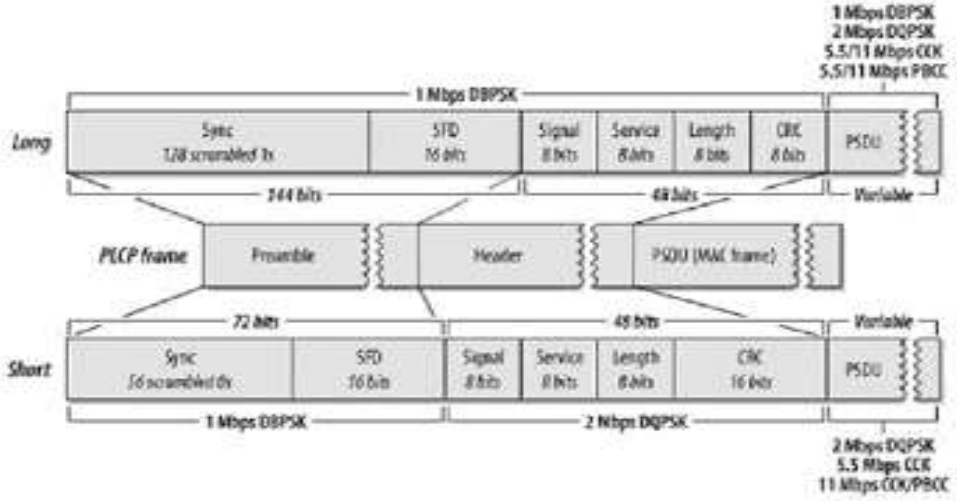

Figure 2-13 PLCP frame format

As other physical layers, the HR/DSSS PHY is divided into two parts. Like the other physical layers, the PLCP inserts additional framing information. The "long" frame format is similar to the typical DS PLCP format and must be supported. For efficient and enhanced throughput, stations must also support the optional "short" PLCP format.

2.12.2 Preamble

Frames start with the preamble, which is made of the Sync field and the SFD field. The preamble transmission rate is 1.0 Mbps using DBPSK.

2.12.3 Synchronization Fields

2.12.3.1 Long Sync

The Long Sync field comprises of 128 1 bits. Before transmission, it is processed by the scrambler, so the data content differs. A high-rate system utilizes a particular seed for the scrambling function but backward compatible with older systems that do not specify a seed.

2.12.3.2 Short Sync

The Short Sync field comprises of 56 0 bits. As the Long Sync, it is also processed by the scrambler.

2.12.4 SDF Fields

2.12.4.1 Long SFD

To specify the last part of the Sync field, the long preamble terminates with a Start of Frame Delimiter (SFD). The SFD is the sequence 1111 0011 1010 0000, in the long PLCP. Like in all IEEE specifications, the order of transmission from the physical interface is that the least significant bit comes first, so the string is transmitted right to left.

2.12.4.2 Short SFD

The Short SFD is the reverse value of the Long SFD, 0000 0101 1100 1111. The PLCP header comes after the preamble. It comprises of the Signal, Service, Length, and CRC fields. The long header’s transmission rate is 1.0 Mbps using DBPSK. On the other hand, the short header's function is to lessen the time required for overhead transmission so its transmission rate is 2.0 Mbps using DQPSK.

2.12.4.3 Long Signal

The Long Signal field specifies the speed as well as method of transmission for the enclosed MAC frame. Four values for the 8-bit code are presently specified.

Speed	Value (msb to lsb)	Hex value
1 Mbps	0000 1010	0x0A
2 Mbps	0001 0100	0x14
5.5 Mbps	0011 0111	0x37
11 Mbps	0110 1110	0x6E

Figure 2-14: Long signal values and corresponding data rates

2.12.4.4 Short Signal

The Short Signal field specifies the speed and method of transmission for the enclosed frame, but only three values are defined. Short preambles are utilized only with 2 Mbps, 5.5 Mbps, and 11 Mbps networks.

2.12.5 Service

The Service field was kept for further use by the first version of 802.11, and bits were rapidly utilized for the high-rate extensions in 802.11g. Firstly, the Length field depicts the time used for the enclosed frame in microseconds. Above 8 Mbps, the value happens to be uncertain. Thus, the eighth bit of the service field is utilized to expand the Length field to 17 bits. The third bit specifies whether the 802.11 implementation uses locked clocks; by clock locking it is meant that transmitting frequency and symbol clock use the similar oscillator. The fourth bit specifies the type of coding utilized for the packet, which is 0 for CCK and 1 for PBCC. Each and every reserved bit must be set to 0. The Service field is transmitted from left to right (b0 to b7), which is similar in both the short and long PLCP frame formats.

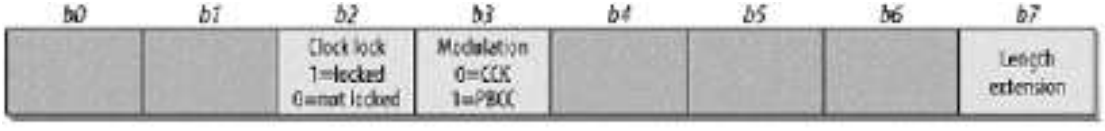

Figure 2-15 Service fields

2.12.6 Length

The Length field is identical in both the short and long PLCP frame formats and is also the number of microseconds necessary to send the enclosed MAC frame. Like for 5.5 Mbps CCK Length = number of bits/5.5, rounded up to the subsequent integer.

2.12.7 CRC

The CRC field is identical in both the short and the long PLCP frames. Senders make a calculation of CRC checksum using the Signal, Service, and Length fields. Receivers utilize the CRC value to guarantee that the header was received undamaged and was not harmed during transmission. CRC calculations are taken prior to data scrambling.

2.13 HR/DSSS PMD

The rate of 802.11 direct-sequence systems is of 11 million chips per second. The original DS PHYs split the chip stream into a series of 11-bit Barker words and then transmits 1 million Barker words per second. Every word is encoded either one bit or two bits for an equivalent data rate of 1.0 Mbps or 2.0 Mbps, respectively. To attain a higher data rate and commercial utility it is required that each code symbol allow more information than a bit or two.

Straight phase shift encoding cannot hold more than a few bits per code word. DQPSK requires that receivers distinguish quarter-cycle phase differences. If the number of bits per symbol is increased, further processing of even finer phase shifts would be necessary, such as an eighth-cycle or sixteenth-cycle shift. Detecting minor phase shifts is more complicated in the multipath interference and needs more refined (and thus expensive) electronics.

As an alternative of straight phase-shift keying, the IEEE 802.11 working group used another encoding method. Complementary code keying (CCK) splits the stream into 8-bit symbols, so that the basic transmission is based on millions of coded symbols per second. Complimentary code keying (CCK) comprises of

complicated mathematical transforms that permit the utilization of only some 8-bit sequences to encode 4 or even 8 bits per code word, for a data throughput of 5.5 Mbps or 11 Mbps. Moreover, the mathematics underlying CCK transforms permit receivers to differentiate between dissimilar codes easily, even when interference and multipath fading are present. It is quite like the chipping process utilized by the slower direct-sequence layers; the dissimilarity is that the code words are derived to some extent from the data. A static recurring code word like the Barker word is not utilized. As in the lower-rate, direct-sequence layers, Barker spreading, utilizes a static code to spread the signal over the present available frequency band. To carry information and to spread the signal, CCK utilizes the code word.

By building on the DQPSK-based phase shift keying techniques higher-rate transmission is achieved. Two bits per symbol period are transmitted by DQPSK and encoded as one of four different phase shifts. If CCK is utilized, the symbol words carry additional information. 5.5-Mbps transmitting rate encodes four data bits into a single symbol. Two bits are carried utilizing conventional DQPSK, and the remaining two are carried through the content of the code words.

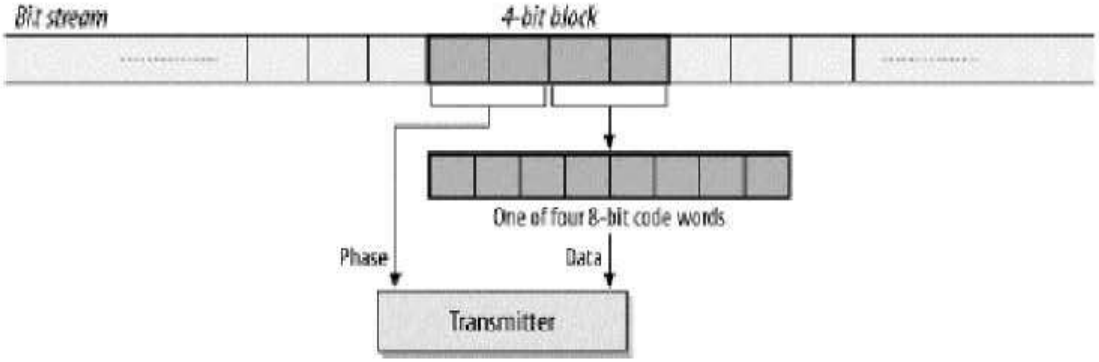

Figure 2-16 Transmission at 5.5 Mbps

The PCLP frame has the MAC frame embedded in it, which is split into a string of 4-bit blocks. Every 4-bit block is further split into two 2-bit segments.

The encoding of the first 2-bit segment is done by using DQPSK-type phase shift between the current symbol and the previous symbol. A different phase shift

is used by even and odd symbols for technical reasons. The start of symbol numbering is with 0 for the first 4-bit block.

Bit pattern	Phase angle (even symbols)	Phase angle (odd symbols)
00	0	π
01	π/2	3π/2
11	π	0
10	3π/2	π/2

Figure 2-17 Mapping of first two bits

The next 2-bit segment is utilized to choose one of four code words for the existing symbol.

Bit sequence	Code word
00	**i**,1,**i**,-1,**i**,1,-**i**,1
01	-**i**,-1,-**i**,1,1,1,-**i**,1
10	-**i**,1,-**i**,-1,-**i**,1,**i**,1
11	**i**,-1,**i**,1,-**i**,1,**i**,1

Figure 2-18 Mapping of second two bits

2.14 Interoperability

2.14.1 Concept of Interoperability

When it is preferred to build a system interoperable with another, the thought that approaches mind is that this system goes to a different environment and converts with respect to that environment. As per IEEE interoperability is the capability of a system / systems or components to transfer intelligence / information and to use the intelligence / information that has been transferred or passed.

Interoperability can be defined in more general way is:
"Interoperability is a belonging of a system, whose interfaces are understood and implement able, to work with various available products or communication wireless systems without any implementation problems or regulatory issues.

"In telecommunication the term can be defined as":
The capability of wired or wireless communication systems to offer their various system/ network features / services and to avail / accept different features and services from other interoperable wired or wireless systems and to exchange the network integration features to make the enable to operate together with better efficiency[19].
The condition attained among communications-electronics systems when information or services can be directly and satisfactorily exchanged between them and/or their users. The degree of interoperability should be specified when referring to particular cases.

The main aim of this theory is that a call commencing in WiMAX resources should be capable to transfer from its own environment to the WI-FI environment. Keeping in view the WiMax environment the entire routing and call forwarding happens at the core network. This is the responsibility of MSC. It can be concluded that some changes/additions will have to be prepared to attain interoperability between systems. Currently, MS (Mobile Station) can support different networks such as CDMA, GSM, and Wi-Fi etc. Thus the necessity at the user end is an additional module that can sense what environment is the user roaming and be competent to switch automatically to the new environment. Despite the fact that end terminal supports many systems, still they are incapable of accomplishing this. Therefore some variations are required in the MS so it becomes competent of changing automatically according to the environment. For instance fundamental block of commercial systems that utilizes a common frequency, channel estimation, error correction codes and line codes. Only the modulation block varies for the entire the different systems utilized. So, it is necessary to manipulate the modulation techniques of the systems [20].

2.14.2 Interoperability approaches

2.14.2.1 Using Multiple Antennas

In the said approach device is produced which have a separate physical antennas attached for every system i.e. one for WiMax, one for WiFi and so on. The formed device for multi systems will switch to that one specific antenna for its communication.

2.14.2.2 Drawbacks

In this device had the restriction of a very big size, multiple antennas would be installed separately on the device. Another disadvantage was that a huge amount of power was essential to energize all these antennas.

2.14.2.3 By Installing Bank of Filters

This was enhanced approach toward interoperability by seeing the limitations of previous approach, as it implies bank of filters to segregate different frequency groups instead of installing multiple antenna for every system. This allows the device to identify whether a signal from a system is reachable or not and then tune its antenna to that particular frequency.

2.14.2.4 Draw back

In this approach the shortcoming of large size of device on the origin of physical antennae was removed but still the size will stay huge enough to accommodate bank of filters. Moreover, the device would be unable to identify between the multi networks in the same frequency range. Moreover, problem of the huge power will remain their which is mandatory to energize the bank of filter.

2.14.2.5 By identification through Modulation

In the said scheme the requirement of multiple antennas or bank of filters is removed. For the purpose different systems were checked utilizing different frequency ranges but for interoperability using modulation identification we need them to utilize the same

frequency range. Though, we need maintenance of parent modulation schemes for the uniqueness of the systems.

2.14.2.6 System / Network Identifier

The end terminal/ handheld identifies the existing environment around it. Suppose the handheld is operating in the WiMax environment and is is a WiMax terminal, it can simply communicate with the core network only if there is WiFi environment, it requires interoperability for communication. Therefore, to recognize the environment where the end terminal / handheld is operating, certain identification is needed. Multiple techniques are available for the detection of the environment.

2.14.2.7 Identification of Modulation basing on EYE diagram

As different modulation schemes were used by the project 25 and commercial wireless communication systems so this approach uses a modulation identifier basing on the eye diagram. This system identifier can be utilized for identification of the modulation and therefore can detect the Network / system. Due to software processing in it so there is no power concern with this scheme

2.14.2.8 Disadvantage

Every modulation scheme has a distinct waveform and every waveform has different points of convergence which identify or isolate them from other waveforms. To calculate these convergence points, complex digital image processing is involved which induces a unreasonable time delay in the system which is impracticable and results into disconnection of an ongoing connection.

2.14.2.9 Constellation diagram identifier

The amplitude and phase of every waveform is recognized from their constellation diagram and by showing their points in each part of quadrant which helps to recognize the modulation scheme and the system in use.

2.14.2.10 Disadvantage

When filters with dissimilar parameters are used it becomes unsuccessful. This can be seen in the case of Gaussian filter which produced a QAM constellation diagram with 16 points, surrounded in close proximity of the theoretical locations. Since the pulses are interfering into each other. The one constellation point of both QPSK and 16QAM, modulation will be at same position, so after going through identification based on constellation point it will be difficult for system identifier to correctly identify the needed environment. Therefore, the said technique is impracticable, as info of correct location of the points is very difficult to identify. Another limitation is of complex algorithms and complication of scaling of the algorithm for inclusion of more than two schemes. Therefore we need to find another network identification which overcomes all problems mentioned above.

2.15 Lab VIEW

Lab VIEW is a graphical programming atmosphere used by scientists to evolve sophisticated test, and control systems using intuitive graphical icons and wires that resemble a flowchart. It suggested uncomplicated integration with various hardware devices and offers unlimited built-in libraries for advanced analysis and data visualization. It was introduced in 1989 and then onward it has rose as an industry leader [21]. This podium is scalable across various targets and OS.

Lab VIEW consist of graphical modules said as Virtual Instruments. These are put together in an perceptive flowchart-like manner and then integrated with together to develop a system design. These VIs are stand alone modules that are used by number times to build various systems.

This is an interactive GUI based comprised of two panels; and Control Panel and Front Panel. Front Panel is the for user interface with different controls and displays. It is in the form of independent icons, matrices and graphs which demonstrates the inputs fed to the system and the outputs received. Inputs are called controls and placed in the form of binary. The outputs are called as indicators. Indicators are in the shape of matrices or graphs that depicts the

output values. The Control Panel is a block diagram that shows the flow of the module. In it processing is done on the module input. It includes various functions from large area of fields along with with mathematics, physics, DSP etc. Both the above mentioned Front and control panels are shown in Figures 2.19 and 2.20 respectively.

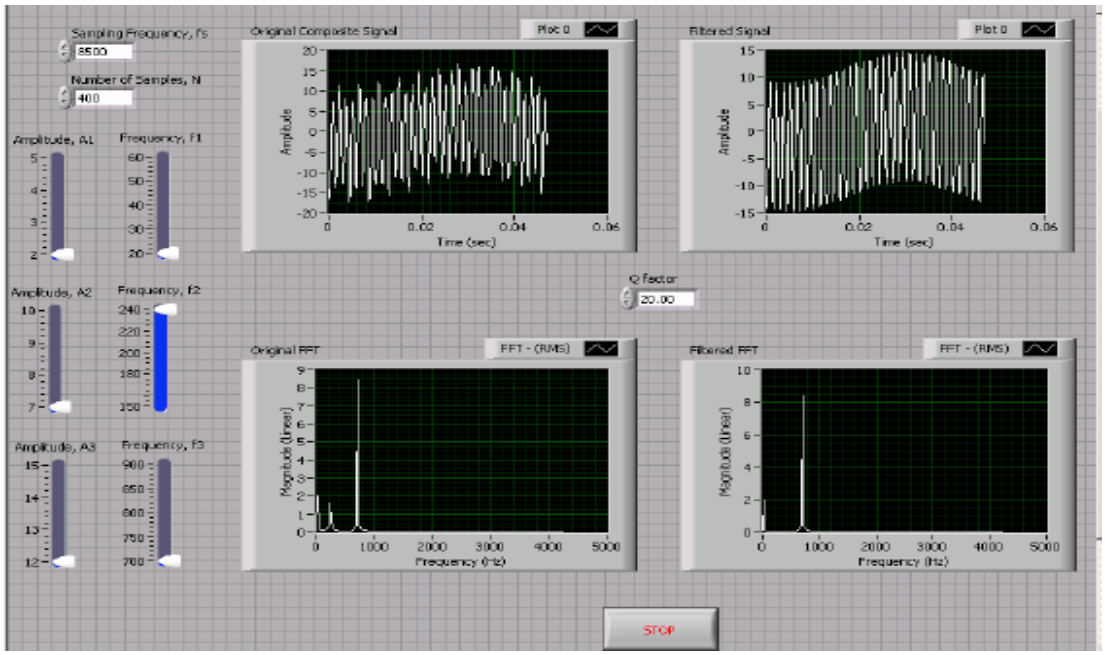

Figure 2.19 Front Panel Lab View

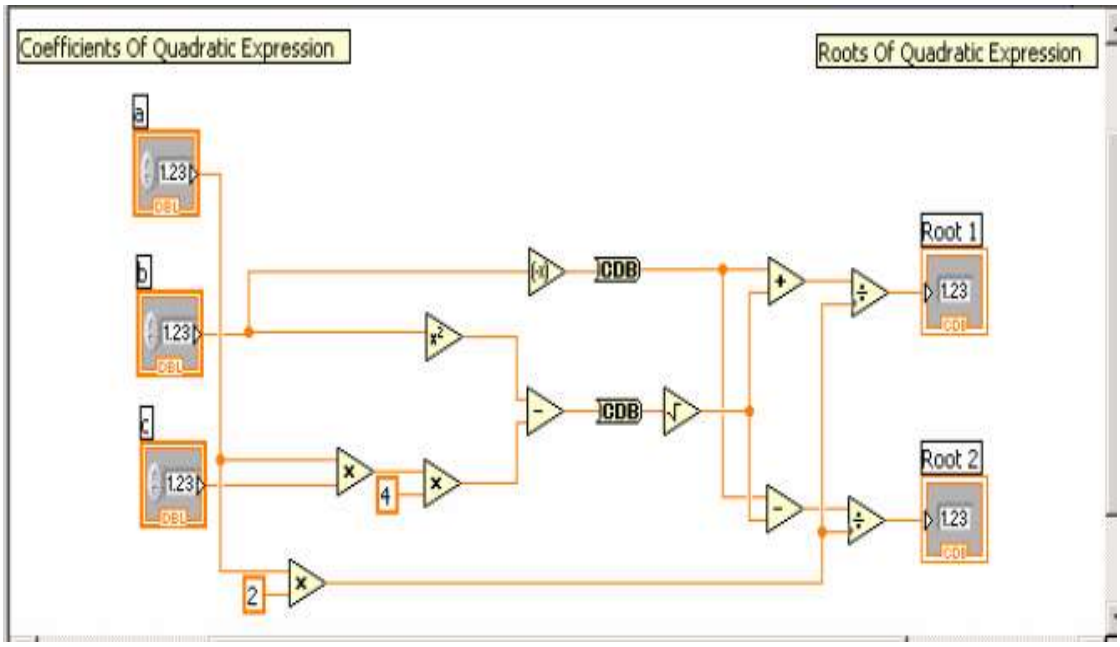

Figure 2.20 Control Panel Lab View

With this graphical and text based modules, Lab View uses hybrid programming approach. Lab View graphical feature allows programming with drop and drag function blocks as an alternative of writing of text. Beside these programming , m files and DLLs as text-based codes can be included in Lab View simulations.

Connecting of any instrument or sensor ability with the help of given libraries and drivers are also available in Lab View. It can also be integrated to USB, PCI, PXI, Wi-Fi, Ethernet, GPIB etc.

Chapter 3

SIMULATION METHODOLOGY

The research work has been systematically distributed into three sub modules.

1. Simulation of WiMax SubVIs
2. Simulation of WiFi SubVIs
3. Simulation of handover between WiMax and WiFi

Lab VIEW 8.6 is the simulation software which has been used for simulating these above mentioned Sub VIs (Virtual Instruments). The major advantage of lab View is of reusability of VIs in various designed modules and it has the capacity to run on hardware or any test equipment without any conversion to other language, it is compatible with FPGA for embedding or testing purpose. The Procedure evolved to design complete system and interoperability modules, above mentioned Sub VIs have been designed which are explained in the following sections:-

3.1 WiMAX Sub VIs Simulation

WiMAX wireless broadband solution presents a rich set of features with a lot of flexibility in terms of deployment options and potential service offerings good resistance to multipath, and allows WiMAX to function in NLOS conditions in the presence of OFDM. WiMAX support high data rates. The PHY data rate for its peak values is as high as 74Mbps when it is using a 20MHz spectrum. Because of its scalable physical-layer architecture, it allows data rates to measure easily with present channel bandwidth. WiMax also has the capability to support various types of modulation and error detection and correction coding schemes and allows them to be adaptive as per desired channel condition and required user per frame basis. WiMAX supports Hybrid automatic retransmission requests (HARQ) at the link layer. HARQ-enabled connections require each transmitted packet to be acknowledged by the receiver; unacknowledged packets are assumed to be lost and are resent. It Support for TDD and FDD: IEEE 802.16-2004 and

IEEE 802.16e-2005 supports both time division duplexing and frequency division. The WiMax standard permits bandwidth resources to be allocated in time, frequency, and space and has a flexible method to convey the resource allocation information on a frame-by-frame basis.

WiMAX physical layer has been simulated in accordance with IEEE std. 802.16-2004 in Lab View. Simulation consists of bit generation with Forward Error Correction, Convolutional interleaver and then Modulation. In LABVIEW there are number of libraries with a big number of functions for data acquisition, signal generation, mathematics, statistics, signal conditioning, analysis, etc., along with numerous graphical interface elements thus offering flexibility in programming and analysis. The block diagram depicts our methodology of simulating Wimax

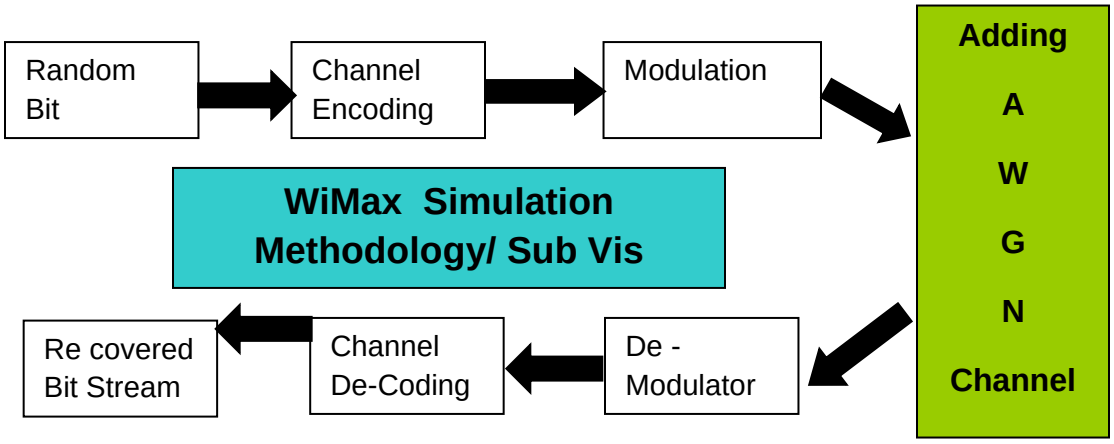

Figure 3-1 Block Diagram of WiMax Vi

Each block in the above figure represents each sub vi created for simulation of complete System.

3.1.1 Bit Generation Sub VI

At transmitter, the random binary bit stream of 500 random bit generation was simulated with PN order sequence 9 that acts as input bit stream. To give practical demonstration few information bits are chosen as reference and are shown as below which has been generated through bit generation block. In the said block, “MESSAGE” is a cluster which is used whose elements are required to be accessed. Cluster comprised of element, whch includes No of bits, Synchronization and Guard bits. So for future reference ‘Bit Gen’ Sub VIs means, message bits are generated in said sub VI. After having been generated or produced these message bits are fed to the Channel coding Sub VI. The generated bits during this process are shown as below:-

Figure 3-2 Message bits

The Sub VI uses following process to generate these message bits as shown below:

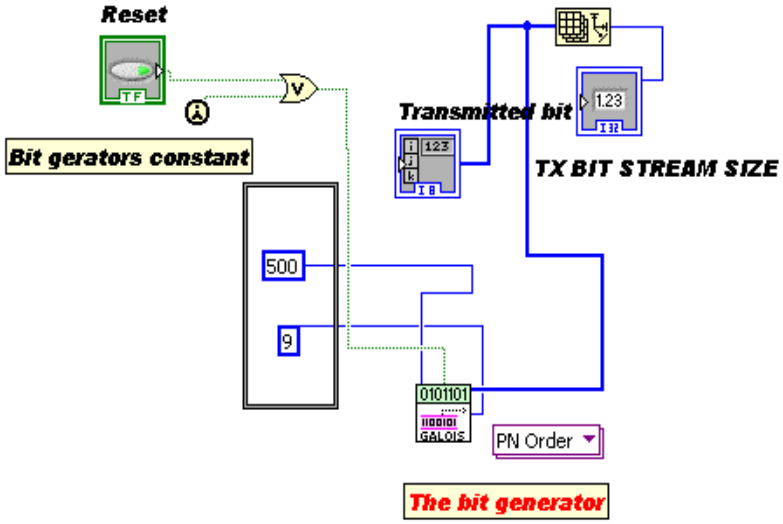

Figure 3-3 Bit Generation Sub VI with PN order

3.1.2 Channel Coding

Channel coding is a scheme which is used to secure data sent over it for storage or correct retrieval of received information even in the presence of error. It is a practical method to reduce information rate through the channel and increase reliability. WiMAX utilizes convolutional encoding as its primary channel coding technique.

3.1.2.1 Concatenated Convolutional Codes

3.1.2.2 Convolutional Codes

Convolutional codes launch redundant bits into the data stream through the use of linear shift registers as shown in figure 3.4.

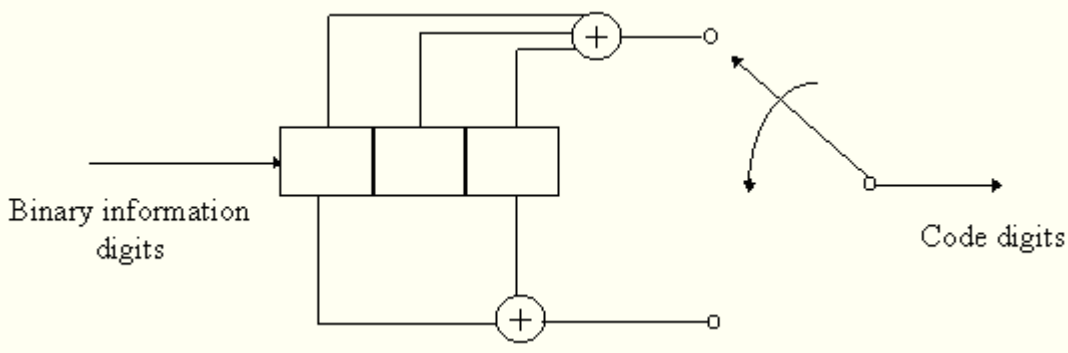

Figure 3-4 Convolutional Encoder

The bits carrying information are fed to the memory / shift registers as shown in above fig. At the output encoded bits by modulo-2 sum are received. Here for demonstration purpose ½ code rate has been used for convolutional encode which can be mathematically defined as

$$(r = k/n)$$

"k" is the no of input message / information bits and "n" is the number of output bits which are received as encoded bits for single time interval. "K" is Constraint length for a convolutional encoder and constraint length relates the number of bits upon which the output depends which can be mathematically defined as:-

$$(K = m + 1)$$

Where “m” is the memory size the shift register which stores the state information of the convolutional encoder

Coding aims at enhancing transmission quality when the signal suffers disturbances (such as significant noise when the reception level is low, interferences, multipath propagation, and Doppler shift). It results, however, in an increased number of bits that calculated with the received data.

Convolution coding adds redundant bits in such a manner that the decoder can, within limits, identify errors and correct them. In order for a code to be able to correct errors, a certain number of additional bits have to be added. The added bits are called redundancy bits. The convolutional code employed in WiMax / WiFi uses a rate of r = 1/3 and a delay of K = 5. This means that five consecutive bits are utilized to calculate the redundancy bits and that for each data bit an additional redundant bit is added. Before encoding the information bits, four bits are added. These bits are all set to zero and used to reset the convolutional code. Since five bits are always used to calculate the appropriate redundancy bits, the trailing four zeros for the last data bit are needed. The block diagram of the convolutional encoder used for speech is shown in Figure 3.5.

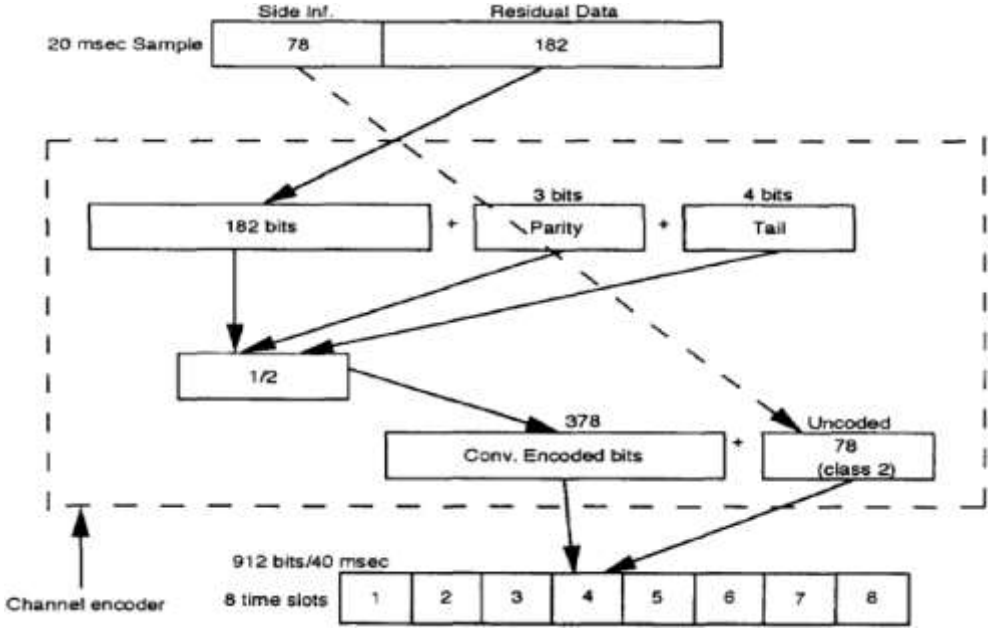

Figure 3.5: Channel EnCoder

These randomly generated bits are input to Forward Error Correction using convolutional coding scheme in Encoder Block. The encoder block outputs coded bits which are given as input to QAM Modulator. The message bits generation specifies the input bit stream which is generated by the block of the bit sequence for the data to encode. After having been generated an encoded bit stream will be of specified code rate "R". Here 1/3 code rate is for measuring the efficiency of code, the input bits and output bit stream is of the same number and i.e. 500. In my channel coding Sub VI, 1/3 code rate has been used as shown in figure 3.6. The L= k (m-1), formulae is used to defined the constraint length, with the number of memory register abbreviated by "m" which refers to the number of present bits present in the encoder for creating an effect on the bit generation of "n" at the output. The channel encoder Sub VI is given below:-

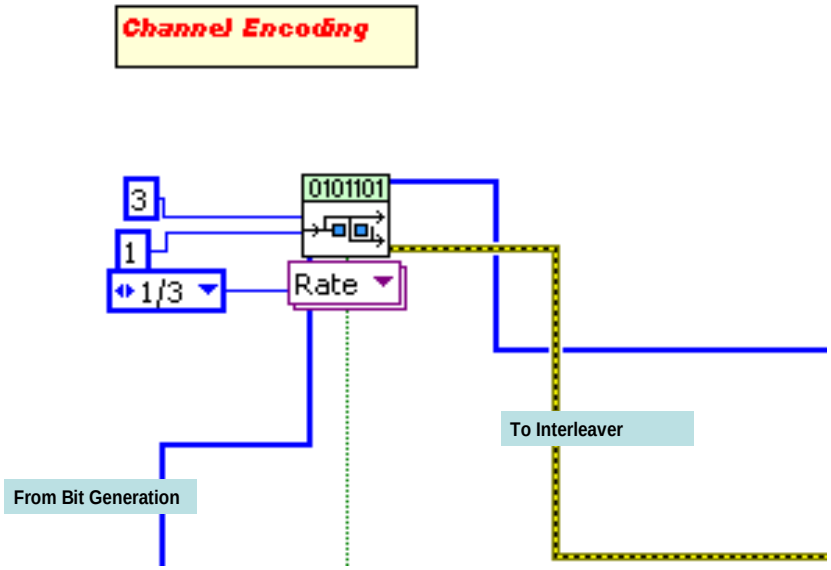

Figure 3-6 Channel Encoding Sub VI

3.1.3 Interleaving

In order to tackle the effects of error due to interference and noise, error correction techniques are used. The redundancy introduced due to error-correcting codes increases the data rate. Error-correcting codes are better at correcting arbitrarily distributed errors but do not work well when the errors

occur in bursts. For bursty errors, interleaving of data is suggested since in reality, bit errors usually occur in bursts. This is because of the reason that long fading dips affect numerous consecutive bits. To deal with this problem I have found a method of unraveling consecutive bits of a message so that these are sent in a nonconsecutive way. This is done by interleaving, which is the method of distributing data bits in a different order in which they are generated.

The interleaving method spreads the content of one block of data either across four timeslots for the most control channels as explained, eight timeslots for full rate speech, and up to nineteen timeslots. This method is important, for the reason that it protects the data against interference, noise, or physical interruption of the radio path. Under difficult environment normally 10% to 20% bursts are damaged or corrupted. Whole bursts are repeatedly lost on radio channels if the subscriber passes through a tunnel or if just about any other type of interference occurs. The intention of interleaving is during deep channel fades when burst errors then each traffic chunk should have some percentage of information. So during burst errors when information chunk is not properly received, the loss of data does not affect the complete transmission quality, and will facilitate the error-correction techniques to recover the missing data. Wireless data robustness is directly proportional to the interleaving strategy, enabling wireless communication to survive in the presence of noise and high interference and to keep the quality communication acceptable to the subscriber. Since WiMax, errors will have a tendency to come about in bursts, which may damage an entire TDMA burst. To conquer this, the bits in each message are interleaved, which lessen the average errors per block to a rate controllable by the FEC.

In my Sub Vi , I have used Convolutional interleaver due to its efficiency to tackle burst error . The convolutional interleaver efficiency is 50% better then the block interleaver. Before entering into the modulation block these bits are fed to interleaver which will organize the data in non-proximate way and is good for secrecy and to improve the performance of channel encoding in fading channel. Convolutional interleaver helps in homogeneous division of errors to keep away from burst errors, though it also increases the latency which is trade off but the latency in convolutional interleaver is ½ then block

interleaver. Convolutional interleaver is more efficient in fading and in interference channel, it passes the data at regular intervals. It selects the no of branches “N”, in which every branch has different delay “D”. The delay of branch “0” will be different from the delay of branch “1”. So each branch will have output with different delay. The interleaver block replicated for WiMax is shown in fig 3-7 below :-

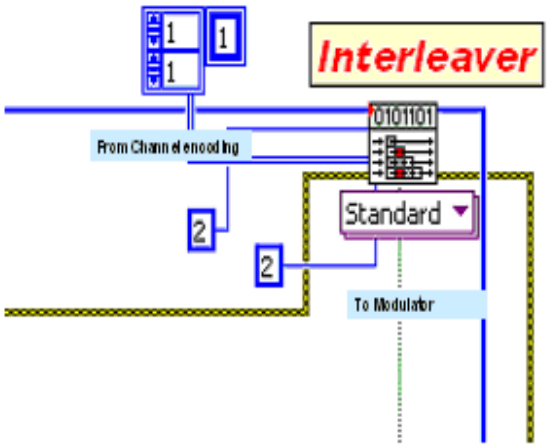

Figure 3-7 Convolutional Interleaver

3.1.4 16 QAM Modulator Sub VI

In my chosen WiMax system, constellation mapping of encoded bits is prepared using 16-QAM modulation. In Sync parameter as shown in the figure 4-5 it used to indicate the type of QAM modulation. Eye Diagram and Constellation graph indicators shows the modulated data which will be incorporated in approaching result chapter. The modulator block along with filter parameters, system parameters and synchronization parameters are shown in fig 3-8.

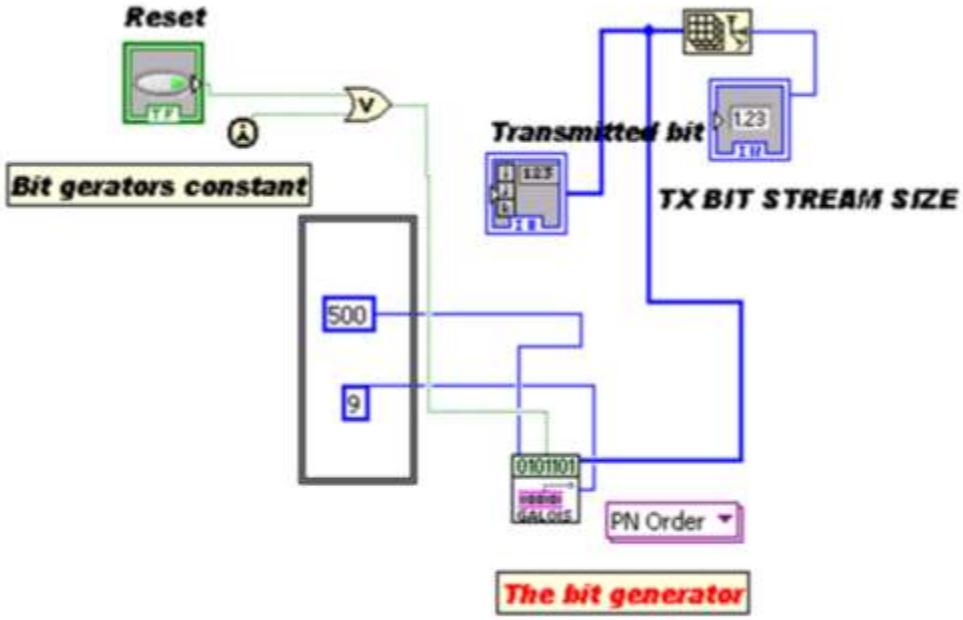

Figure 3-8 16 QAM Modulator Sub VI Block

3.1.5 Simulating AWGN Channel Sub Vi

To compose the system nearer to real time the modulated bit order passes through artificially created White Gaussian Noise (AWGN) channel. In AWGN 16 samples for each symbol are used. Samples for each symbol spell out the number of samples for each symbol in the input complex waveform. 2 Bits for each symbol are used to state the number of bits for each symbol in the modulation design underlying the input complex waveform. The signal-to-noise ratio E_b/N_0 in dbs gives the required E_b/N_0 of the output complex waveform. Figure 3-9 shows the virtual channel Sub VI blocks to produce the channel effects on the modulated symbols at the receiver side.

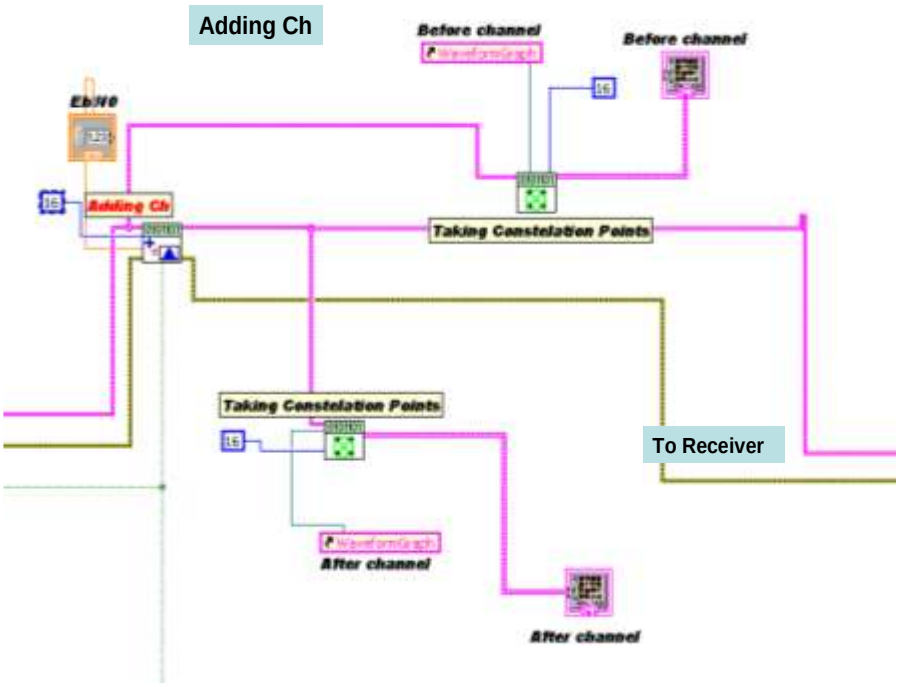

Figure 3-9 By Adding AWGN Sub VI

3.1.6 WiMax - Receiver mode

At receiver end the reverse method works and channel affected signal is fed through demodulator followed by de-interleaver and at last fed to decoder to obtain a recovered wave form.

3.1.7 16 QAM De-Modulator Sub Vi

The OFDM demodulated symbols take steps as input for QAM demodulator block. The complex base band waveform is demodulate by using 16 QAM-de-modulator and returns the complex waveform which is time aligned. The QAM system are designed or defined with the help of QAM parameters or by defining the QAM parameters**.** The ordered arrangement having the need of the filter coefficients are defined with corresponding filter coefficients. To search the array of bits, sequence order is required for which synchronization parameters are defined to unfold the synchronization order and the array of bits. This block de-maps the received constellation and recovers the bit stream which

is fed to Convolutional decoder. The block diagram showing demodulation Sub VI illustrated in fig 3-10.

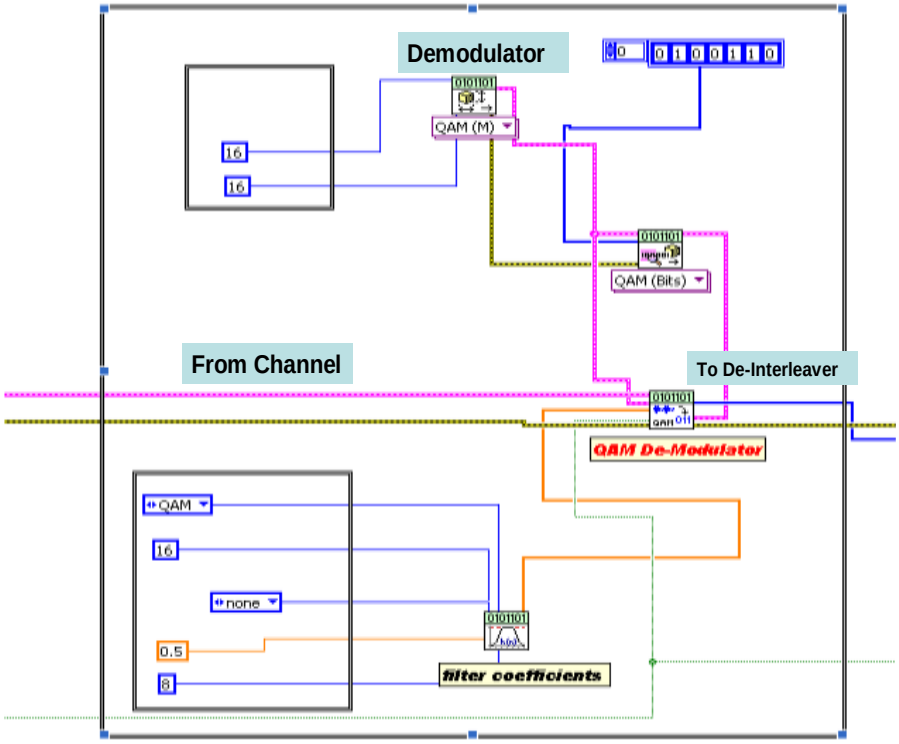

Figure 3-10 16 QAM Demodulator Sub VI

3.1.8 Channel decoder and De-interleaver Sub Vis

The reverse process will be performed by Convolutional Deinterleaver and the data will be recovered and will be fed to Convolutional decoder which has decoded the data and identifies as well as eliminates errors from the data to an extent. Simulation of WiMAX Deinterleaver and decoder sub VI is demonstrated in Figure 3-11.

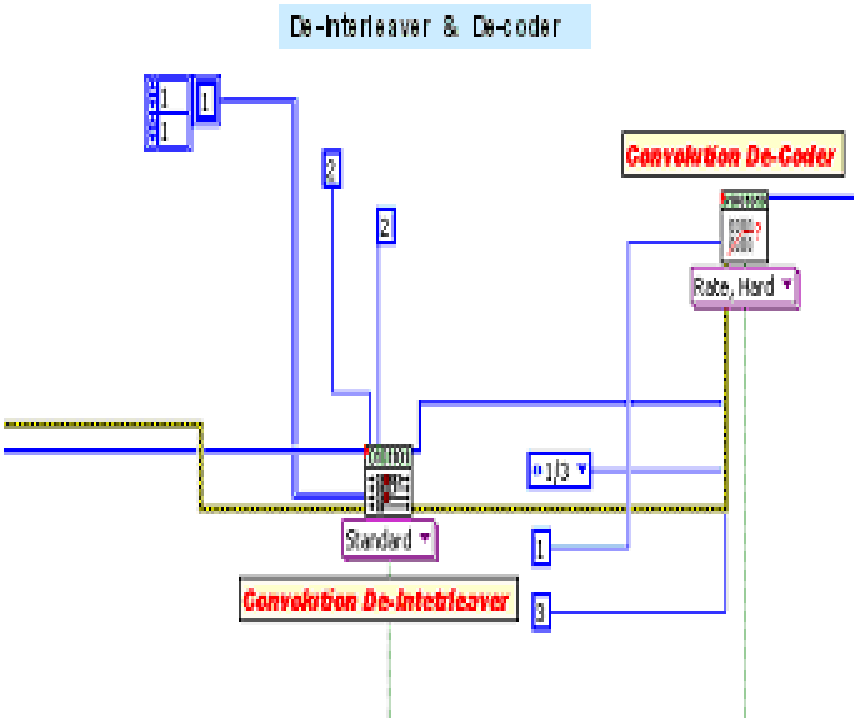

Figure 3-11 De-Interleaver and De-Coder Block

3.1.9 Bit Error Rate Sub VI

Bit error rate has been calculated at the last of receiver block to examine on the whole effectiveness of the designed system.

3.2 WiFi Simulations Sub VIs

The transmitter performs on the principle of ISO layered structure. It initiates its processing from the IP packet handed over by the layer three. Then the IP packet is processed and the length of the packet is checked and the process fragmentation is completed if it surpasses the highest allowable length specified by the 802.11 standards. These processed segments are then sent to the MAC layer module which has the responsibility of encapsulating the IP packet into the MAC frame following the 802.11 standards. It joins the frame control bits (which comprises of information such as protocol version, power management bit, more fragments bit etc), duration/ID bits, receiver address, transmitter address, source

address, sequence control bits and destination address with the IP packet. This MAC frame is then transmitted to the physical layer. Physical layer of transmitter carries out two operations on the MAC frame. Firstly it appends the PLCP header before MAC frame and secondly it modulates this information. The information in the PLCP header comprises of synchronization bits, SFD (Start Frame Delimiter), signal bits (which tells the speed of connection), service bits, length bits and CRC. The block diagram illustrates our methodology of simulating WiFi :

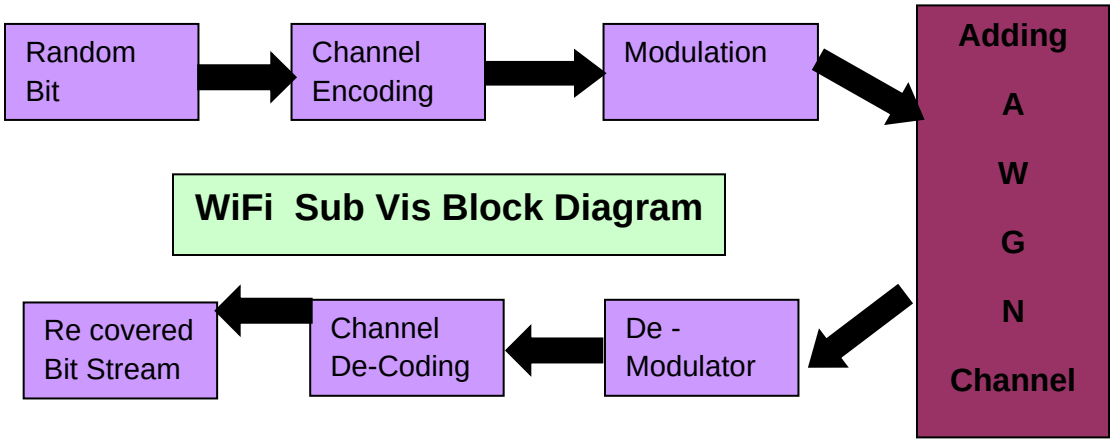

Figure 3-12 Block Diagram of WiFi SubVis

Each block in the above diagram illustrates each sub vi created for simulation of complete System. In my simulation the physical layer has been simulated and random bits are generated by the assumption that it has been applied with PLCP header. Small portion of message bits are used for reference as demonstrated below these bits go into the Channel coding block. Shown below is the process which generates these message bits.

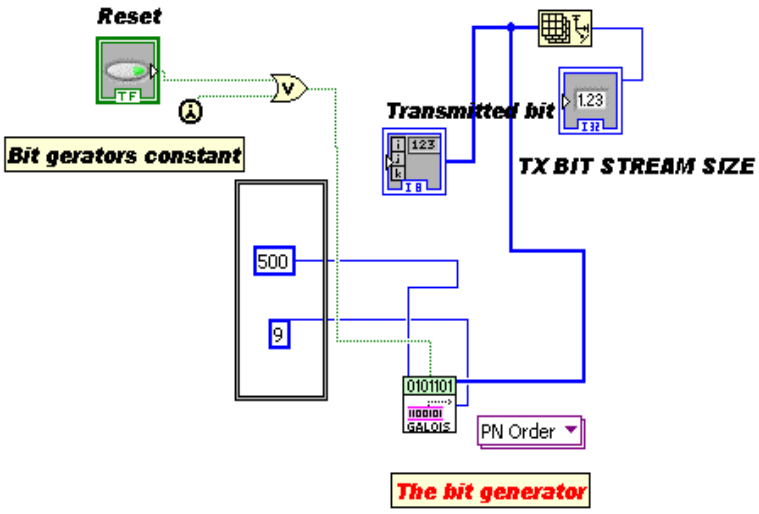

Figure 3-13 Bit Generation Sub VI with PN order

3.2.1. Forward Error Correction and Interleaver

By means of convolutional coding scheme in Encoder Block these generated bits are applied to Forward Error Correction. Output from the encoder block is in form of coded bits which are fed as input to QPSK Modulator. Channel coding is a scheme which is used to secure data sent over it for storage or correct retrieval of received information even in the presence of error. It is a practical method to reduce information rate through the channel and increase. These bits are provided to interleaver which will organize the data in non-contiguous way and is for betterment of secrecy and to improve the performance of channel encoding in fading channel. The interleaver block simulated for WiFi is demonstrated in fig 3-16 below:-

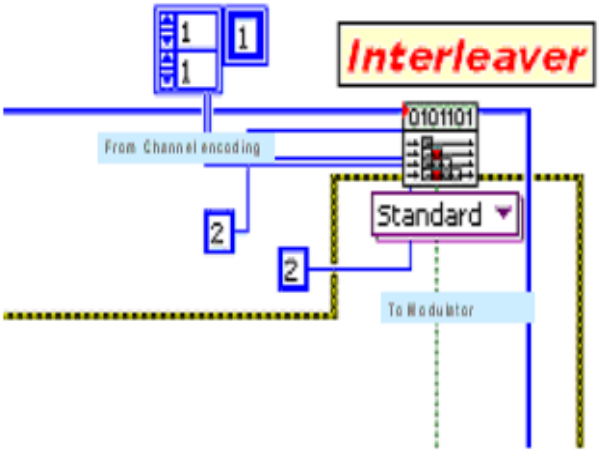

Figure 3-14 Interleaver Sub VI

3.2.2 WiFi Modulator Sub VI

For QPSK modulator some information is required to give the desired results. This information consists of PSK type, M-PSK (bits per symbol), filter characteristics, synchronization parameters (later to be used by demodulator), system parameters, sample per symbol and symbol rate. Pulse shaping filter coefficients and matched filter coefficients for the modulator and demodulator are generated by the system filter coefficient generator. The system parameter generator obtains different essential information and feeds them in the compact form to the PSK modulator and synchronization parameter generator block. The synchronization parameter for the demodulator is generated by Synchronization generator block. The modulator block obtains the system parameter, pulse shaping filter coefficients and bit stream as an input and provide the output in the form of modulated complex waveform. Fig 3-17 Sub VI clarifies the QPSK modulator for WiFi transmitter

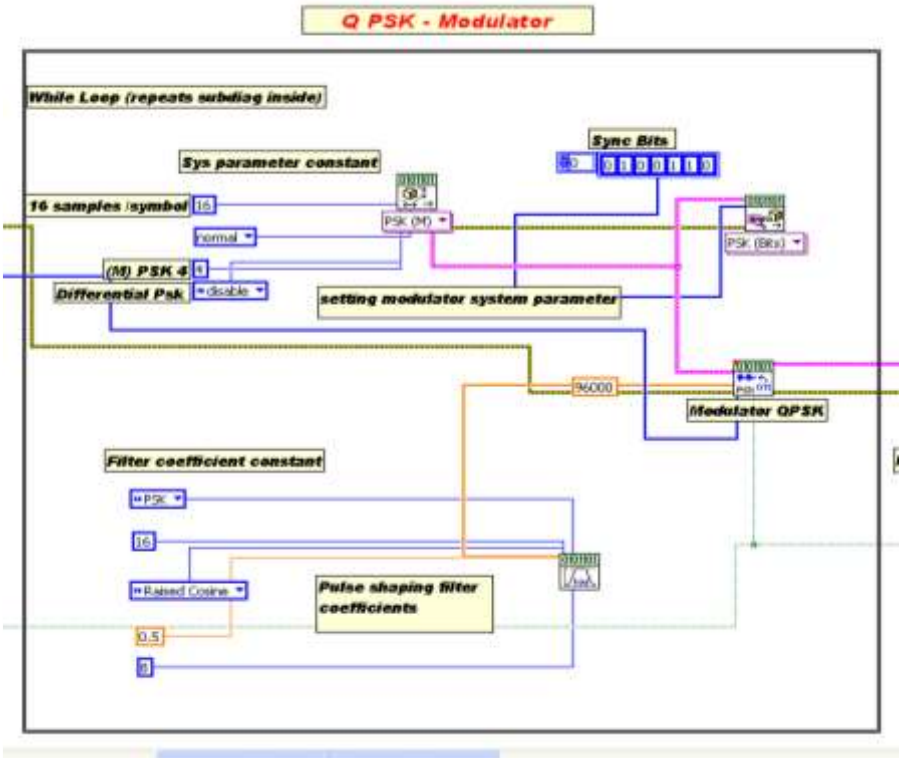

Figure 3-15 QPSK Modulator Sub VI

3.2.3 Receiver Module

The reverse process occurs at the receiving end and output complex wave form is fed to the demodulator followed by Deinterleaver and finally the bit stream is decoded by passing through Convolutional decoder. Following Sub VIs give details of the three processes after the signal is affected by Gaussian channel.

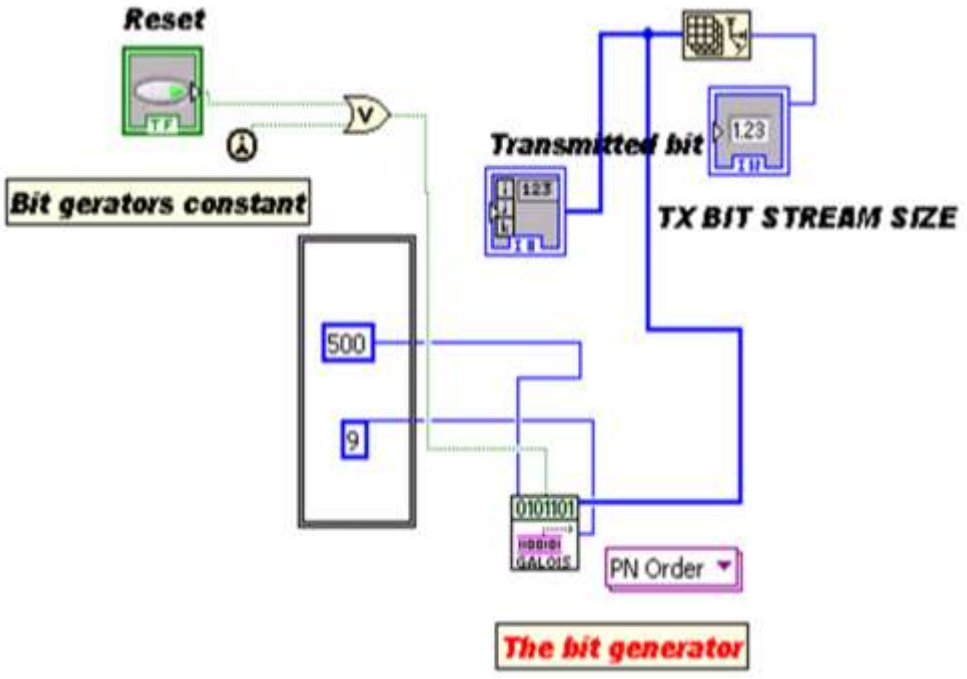

Figure 3-16 De-modulator Sub VI

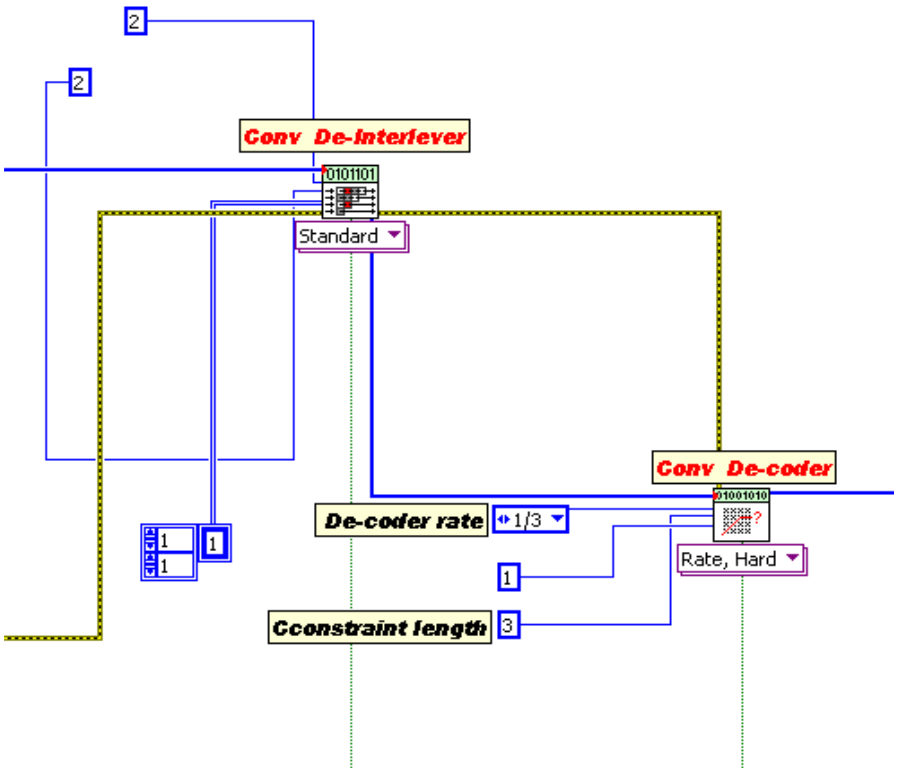

Figure 3-17 De-Interleaver and De-coder Sub VI

3.3 Handover / Interoperability Implementation

Handover judgment is taken on the base of two criteria i.e. Signal to Noise Ratio (SNR) and throughput. When any of the above mentioned criteria drops below a certain level, the vertical handover process starts. When the wireless connection between the MS (Mobile Station) and its own network lost, the alarm prompts to hook up to the any other available / interoperable network. This trigger operates on the basis of signal strength. The concept used for this purpose within its own handheld is shown in Figure 3-20.

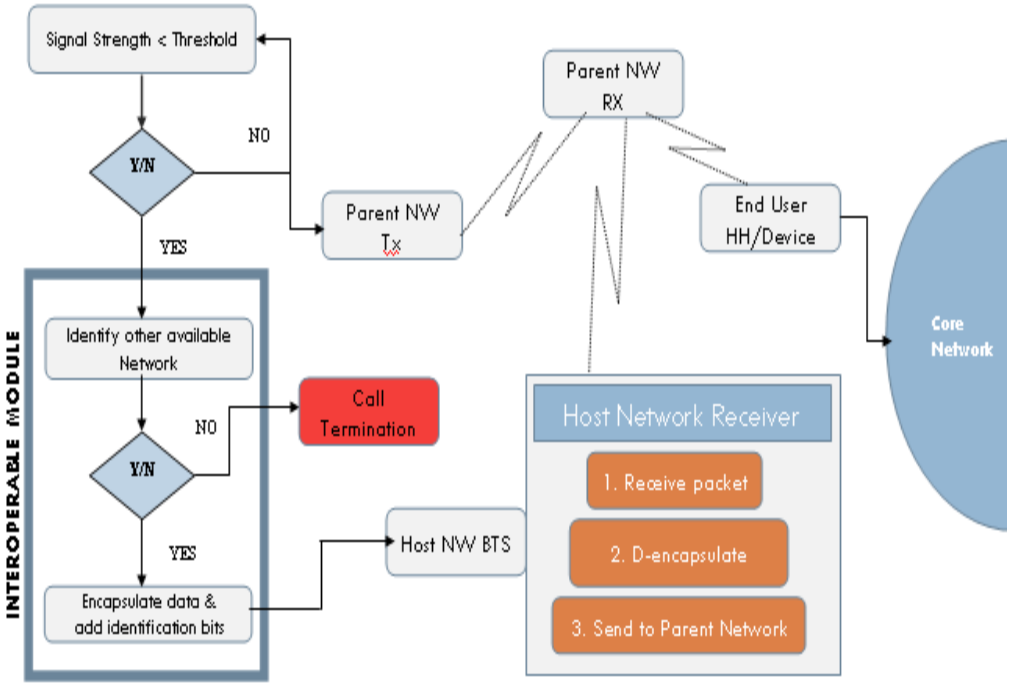

Figure 3-18 Vertical Handover concept

When the present Signal strength becomes less than the desired threshold Eb/No, a vertical handover process becomes mandatory, then search for another available interoperable network will start. If other network is available then handover will be performed. Otherwise, the user connection will be disconnected.

3.3.1 Handover process

Once the handover process begins, the next step is to execute the handover so that the end user is effectively transferred to the other network. To perform that, the mobile station encapsulates the data and sends it to the desired network. This encapsulation gives the information about the parent network. The target network, on receiving the information removes the encapsulation and learns that the hand held belonged to other wireless system / network. It then forwards the received information to its parent network without processing it. In this process, the parent network becomes aware of the host network under use.

3.3.2 Linear Prediction Coding Identification and Prediction of Future Values

Identification through LPC is highly dependable method for recognition of every modulation scheme. Every modulation scheme has its unique waveform; therefore auto regressive points are calculated to discriminate various modulation schemes. This method has proved to be the most accurate and error less method for easy discovery, scaling and efficient implementation.

3.3.3 Auto Regressive Model

It is a randomly generated process to forecast the future coefficient based on previous coefficient values. It is elaborated by the following equation,

$$x_t = \sum_{i=1}^{N} a_i \times_{t-i} + \varepsilon_t$$

Such method is known as autoregressive method of order N. In the present value x_t is based on its past values x (t-1) to x(t-N). It has the order N, which equals the number of past values of the process that are involved in its formulation. The present value of the coefficient is equal to the linear combination of the past values.

3.3.4 Lab VIEW Simulation of Network Identifier

To calculate auto regressive point, adaptive filter tool kit of lab view simulator has been used. The utmost step size for the filter has been designed. The step size affects the convergence speed, error, and stability of above mentioned adaptive filter. Smaller the step lesser will be the stability of steady state error. Moreover, a small step size also lowers the convergence speed of the adaptive filter. So this is a trade off which is to be analyzed. However, large step size might become the cause of instability of the adaptive filter. Following VI is generates the auto regressive points.

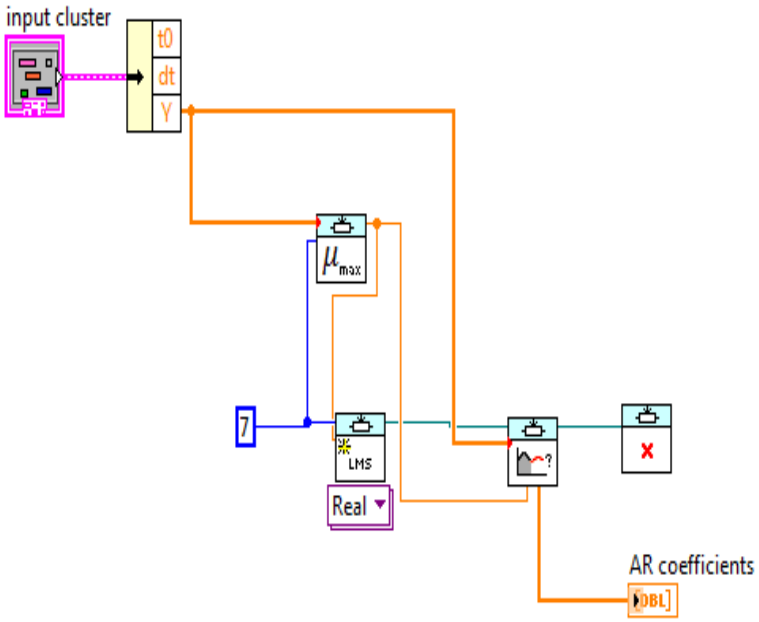

Figure 3-19 AR Coefficients Generation in LabView

A step size value was taken of length eight. Then by using this filter step size of eight, it was calculated by the 1st block, adaptive filter was created using LMS algorithm. Then Linear Prediction block was used which performed linear prediction by estimating the autoregressive model of an input signal. This evaluated and gave the AR coefficients of the signal, therefore, on the basis of these auto regressive points signal is identified.

3.3.5 System Identification

System identification is the ability of one network to recognize the other available wireless systems. It can be well thought-out as an midway step between signal interception and info recovery. When the modulation is recognized, an suitable demodulator can be easily selected to demodulate and then to recover the signal / information. This research is not only to differentiate between networks on the modulation basis but also takes into deliberation that identification of the modulation type of an unknown signal will provide priceless insight into its structure, and properties and also identify the systems.

Digital modulation maps the information to various discrete points on *I* /*Q* plane. These are called constellation points. As the signal travels from one point to another, their amplitude and phase usually changes. Then identifier decides between the two wireless systems on the basis of these constellation points which differs with each other due to their constellation diagrams.

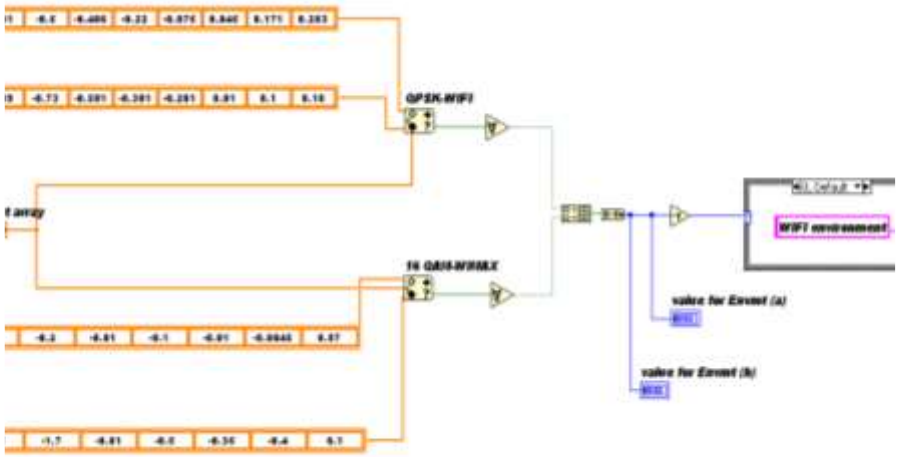

Figure 3-20 System Identifier

This network identifier takes symbols as its input. It processes these symbols through an Linear prediction block to get the Auto regressive coefficients. The property of Auto regressive coefficients is that they are unique for each exisiting modulation scheme. The auto regressive points of the incoming signal are compared with the pre-determined coefficients and if they lie within the defined limits then it is resulted that the source of the incoming signal is present in that modulation scheme.

3.3.6 Handover/Interoperability by WiMax and WiFi in each others Environment

After the prediction of environment or BTS / hotspot of other network (not parent network) the mobile station encapsulates the data and sends it to the host network. The encapsulation provides the info about the parent network. The host network, on receiving the signal / information, removes the encapsulation and sees that the handheld belongs to other network. It then forwards the received symbols / data to its parent network without decoding / processing it. In this process, the parent network becomes aware of the host network under use. The scenarios of handover are shown as below:-

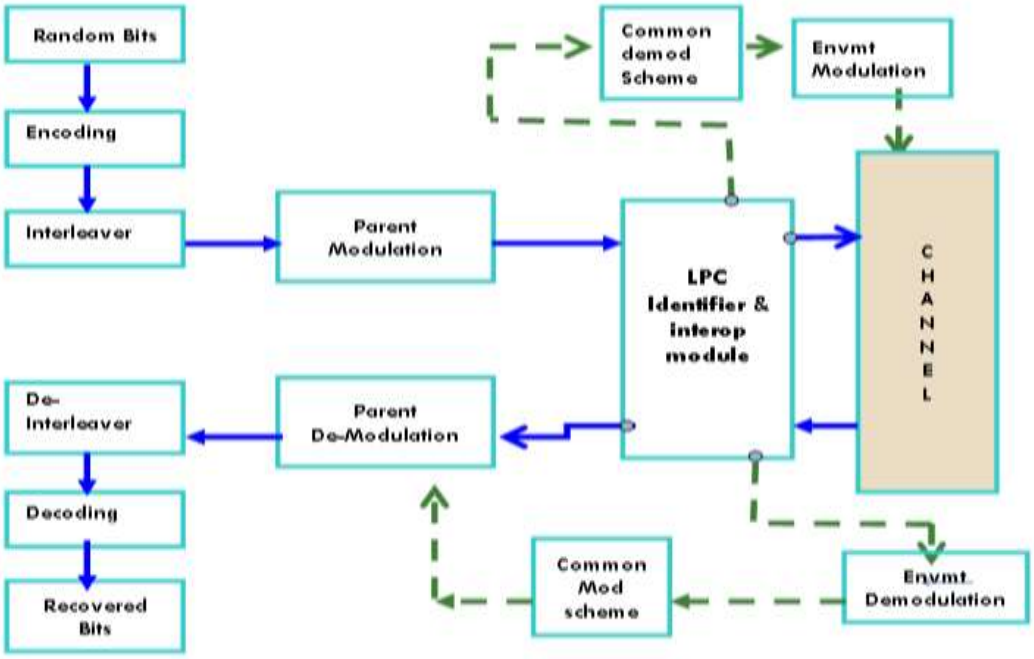

Figure 3-21 Handover/ Interoperability Scenarios

Chapter 4

SIMULATION OF MAIN VIs

This chapter comprises of three main VIs.

1. WiMax complete VI
2. WiFi complete VI
3. Handover / Interoperability complete VI

4.1 WiMax and WiFi VIs

In said WiMax and WiFi VIs, physical layer is simulated following the IEEE std. 802.16-2004 and 802.11g. These simulations have been created from bit generation followed by Forward Error Correction, Convolutional interleaver and then Modulation of respective systems. The transmitter of WiMax and WiFi included sub VIs as explained in previous chapters as discussed above are illustrated in following Fig 4-1. and 4-2 .These modules/ sub VIs have been explained in detail in previous chapter . The random bit stream generated is given as input data to both the systems. The encoding is performed through convolutional encoder in order to avoid fading and increasing secrecy to the channel. The final encoded bit stream has been convolutionally interleaved to increase the efficiency of channel encoder during burst errors and in the end data is modulated prior to passing it through amplifier, up converter and feeding to AWGN channel.

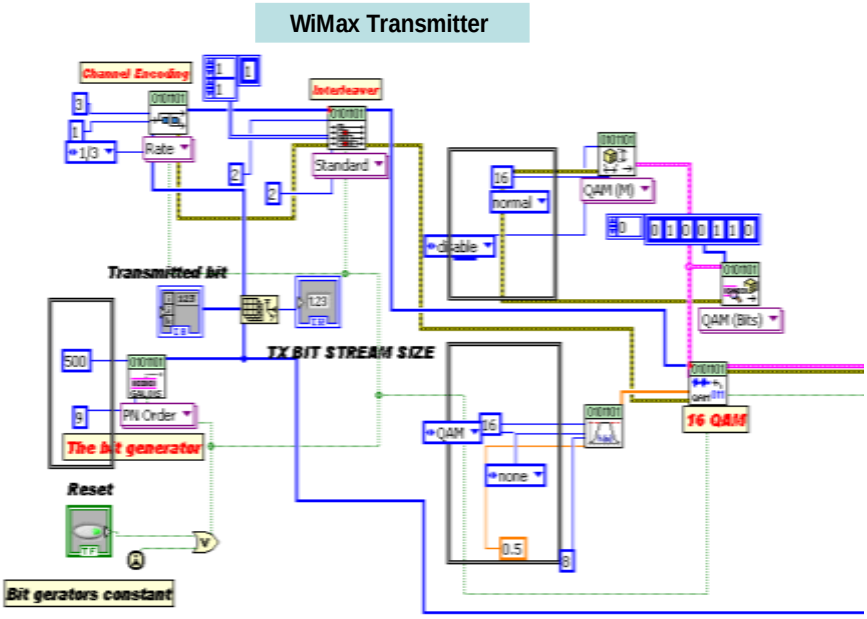

Figure 4-1 WiMax Transmitter

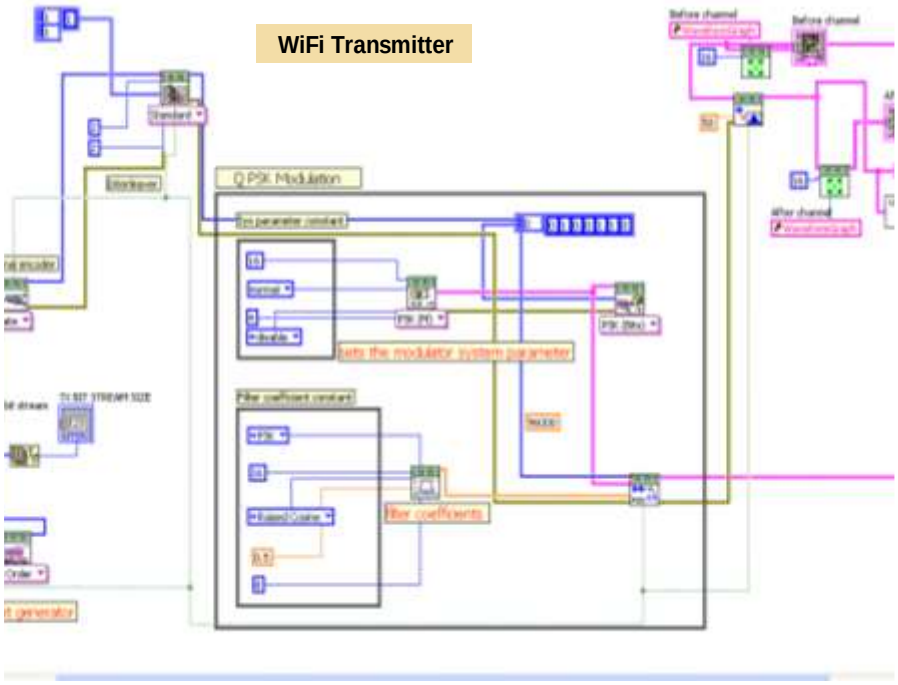

Figure 4-2 WiFi Transmitter

The reverse process occurs at Receiver end and outputs difficult wave form fed to the demodulator followed by Deinterleaver and at last bit stream is decoded by letting it

pass through Convolutional decoder. The Fig 4-3 and 4-4 demonstrate the complete VIs of WiMax and WiFi systems.

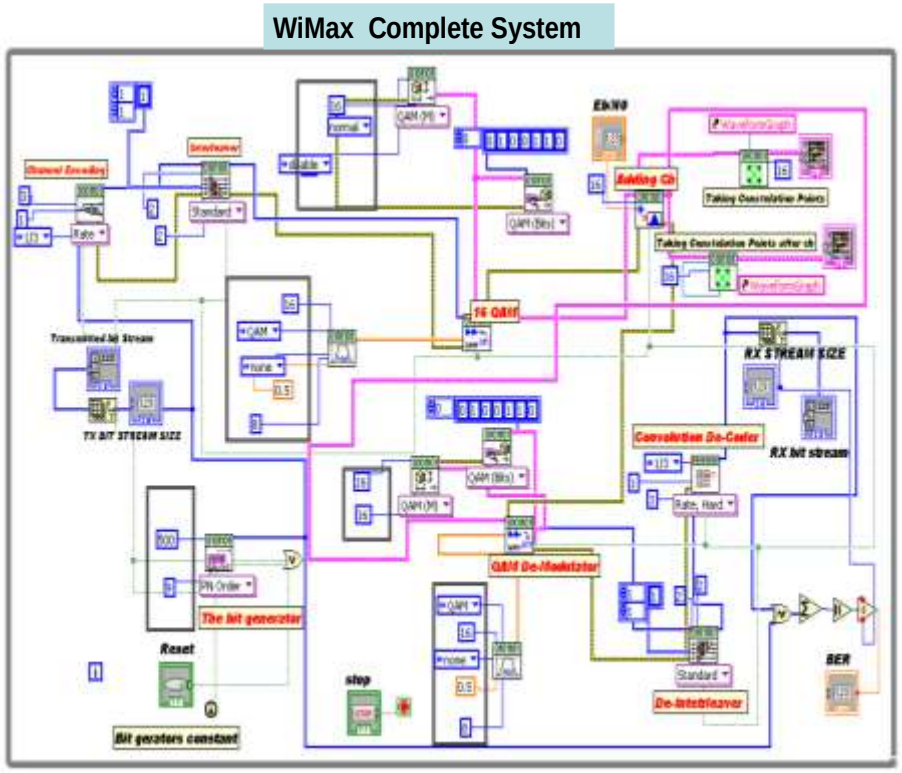

Figure 4-3 WiMax System

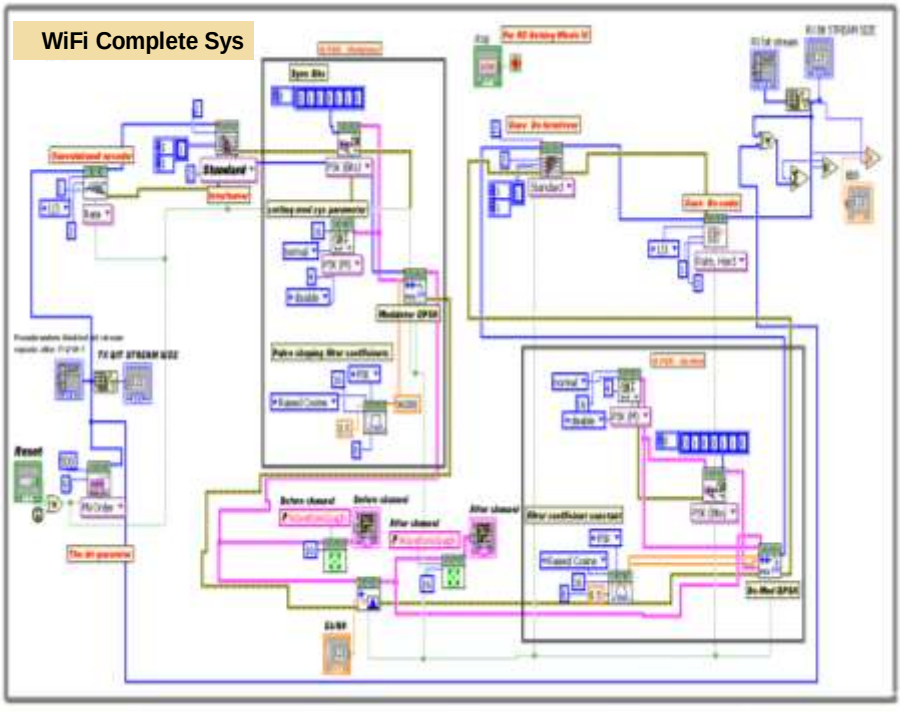

Figure 4-4 WiFi System

4.2 Handover / Interoperability

If the signal strength of parent network happens to reduce than the threshold signal strength, Eb/No a vertical handover process will begin and a look for an alternative accessible network will start. If another network is obtainable then handover will be carried out. Or else, the user connection will break.

4.2.1 Handover process

The next step after the handover process has commenced is to carry out the handover so that the Mobile user is effectively shifted to the alternative network. For performing that, the mobile station identifies the other interopeable environment and senses that its parent network signal strength is not sufficient to carry on the call, so it encapsulates the data and transmits it to the target network. The encapsulation gives the information regarding the home network. When the target network, receives the data then it removes the encapsulation and learns that the MS belonged to some other network. It then sends the received data to its parent network without decoding it. In this process, the home network becomes aware of the target network under use. There are two cases of handover:-

Terminal is WiFi and environment is WiMax

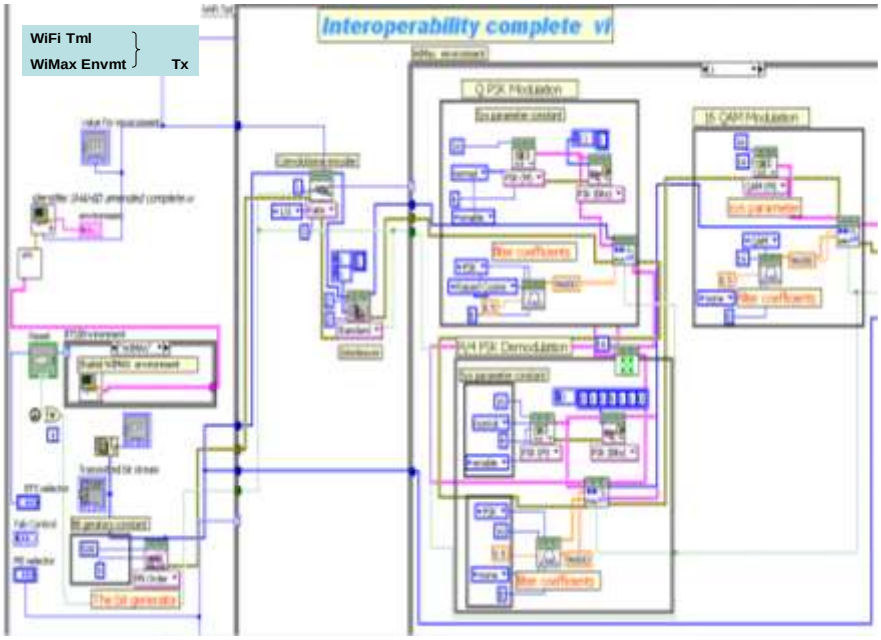

Figure 4-5 Interoperability Scenario -1(a)

In this scenario of VI when a terminal of WiFi comes in to the network of WiMax or when WiFi own network signal strength is weaker than the threshold then it decides for handover as per algorithm defined in previous chapter. The identifier then senses the environment of WiMax and passes on the info, resultantly WiFi QPSK modulated signal was demodulated with common modulated scheme Pi/4 PSK and followed by modulating into environment modulation scheme i.e. 16 QAM and the signal will be transmitted to Gaussian channel. On receiver side as explained in fig 4-5 (b).

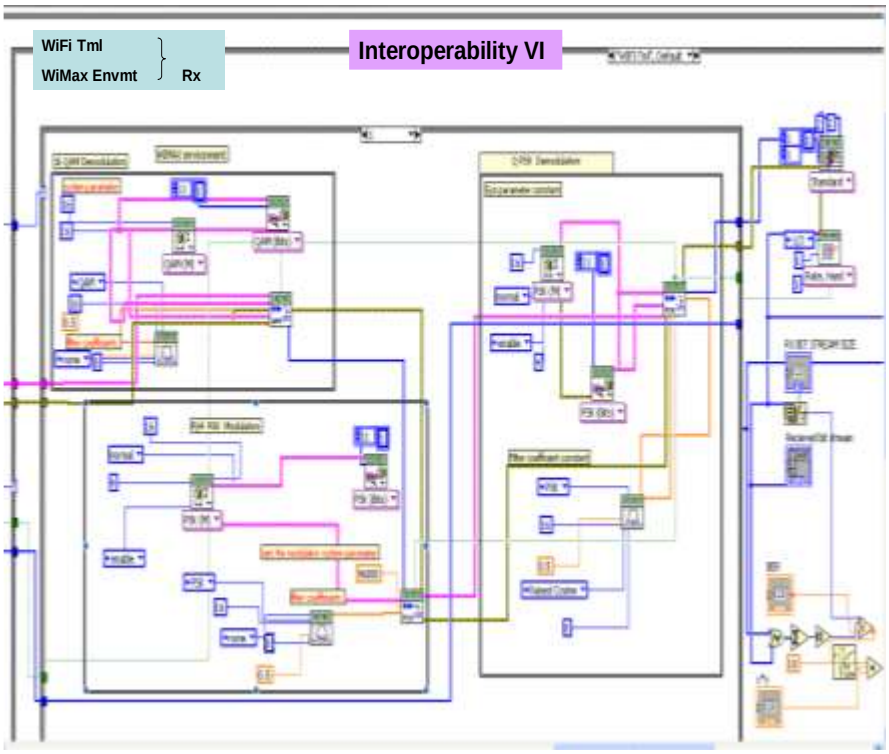

Figure 4-6 Interoperability Scenario -1(b)

When it is received, the affected AWGN signal was demodulated with environment modulation scheme 16 QAM, then modulated with common modulated scheme and finally demodulated with parent demodulator. After the said demodulation the signal was transmitted to interleaver and finally to channel decoder for recovery of transmitted signal. In the end we estimate the BER to verify the correctness and efficiency of our simulated interoperability environment.

4.2.1.1 Terminal is WiMax and environment is WiFi

In this scenario VI when a terminal of WiMax comes in to the network of WiFi or when WiMax own network signal strength is reduced from the threshold then it decides for handover as per algorithm defined in precious chapter. The identifier senses the environment of WiFi and conveys the info, resultantly WiMax 16 QAM modulated signal was demodulated with common modulated scheme 16 PSk and followed by modulated by environment modulation scheme i.e. QPSK and the signal transmitted to Gaussian channel. The transmitter part of this case where WiMax comes into WiFi loaded environment having its parent signal strength weaker then required threshold to continue the connection is explained in fig 4-6 as below:-

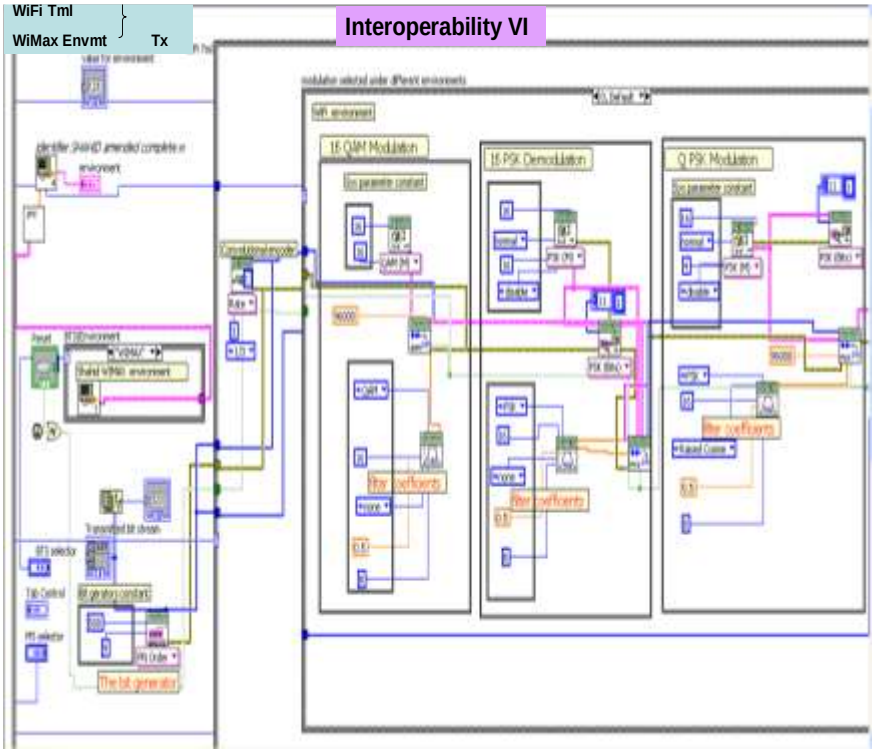

Figure 4-7 Interoperability Scenario-2 (a)

On receiver side as explained in fig 4-6 (b), the affected AWGN signal was demodulated with environment modulation scheme QPSK, then modulated with common modulated scheme and at last demodulated with parent demodulator. After the said demodulation the signal was fed to interleaver and finally to channel decoder for

recovery of transmitted signal. In the end we estimate the BER to verify the efficiency of our handover / interoperability environment.

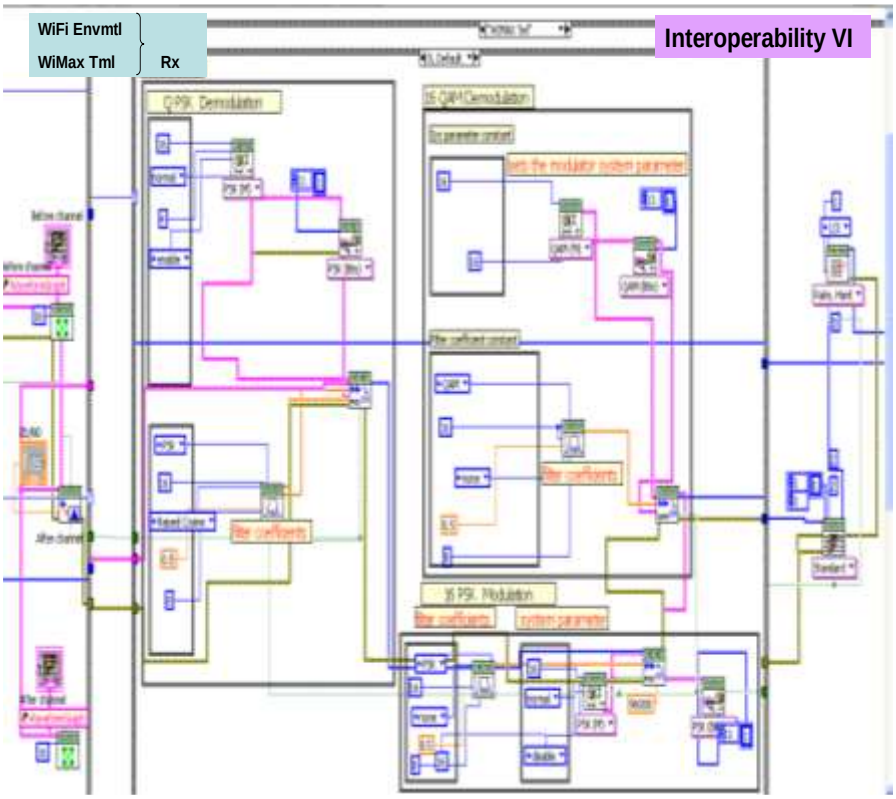

Figure 4-8 Interoperability Scenario -2(b)

Chapter 5

RESULTS AND DISCUSSIONS

5.1 WiMax Results

In this project, WiMax system is divided into transmitter and receiver portion. Therefore, it was thought appropriate to discuss the results of WiMax system in following two divisions.

5.1.1 Transmitter

The transmitter part is responsible for accepting the speech packets and transforming it into the WiMax burst form. Speech packets are composed of random bits instead of actual sampled speech coded packet. These bits are generated through random generator of PN sequence 9, the reader can refer back to chapter 3 for explanation of pseudo random bit generator. These bits are coded through channel encoder i.e. convolutional encoder of rate 1/3, after the signal has been encoded it is passed through convolutional interleaver. The efficacy of convolutional interleaver instead of block interleaver is also amply covered in previous chapter. The end result of a transmitter is the 16 QAM modulated signal as per WiMax interoperable international standards. The transmitted bits pattern, constellation diagram is shown in fig 5-1

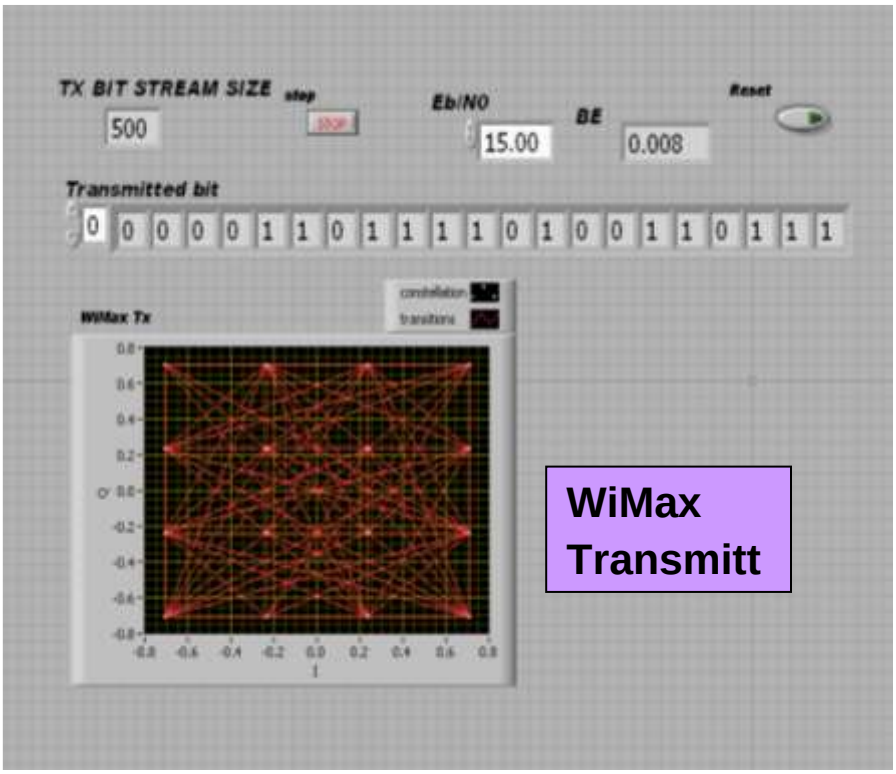

Figure 5-1 Constellation diagram of WiMax Transmitter

5.1.2 Receiver

The receiver is designed to accept the 16 QAM modulated signal after been faded by Gaussian channel and transform back it into the speech coded packets which were originally fed to the transmitter as an input. Receiver in this project has been successful in transforming the message in to its original form. It can be seen from the fig -.- that same no of bits have been received at receiver without loss and this result has been achieved at Eb/No of 15 db. It is worthy to mention here software crashes were excessively experienced for data of lengths of the order 500 or more. Therefore, in many computations the overall best performance of the system was observed at BER of about 10^{-4}. However, more practical results can be Obtained through powerful workstations which can perform simulations using as huge amount of data. The constellation diagrams in figure -.- shows mapping of data on the constellation points received at the receiver end. The dots show the constellation points and lines show the transitions between these constellation points. It is evident from the figure that the received constellation points are

fairly within their boundaries, hence making the de-mapping decision easy for the receiver. This leads to correct interpretation of the data bits. , The receive bit pattern and constellation diag is shown in figure 5-2. This data is recorded at the $_{Eb/No}$ of 15 dB.

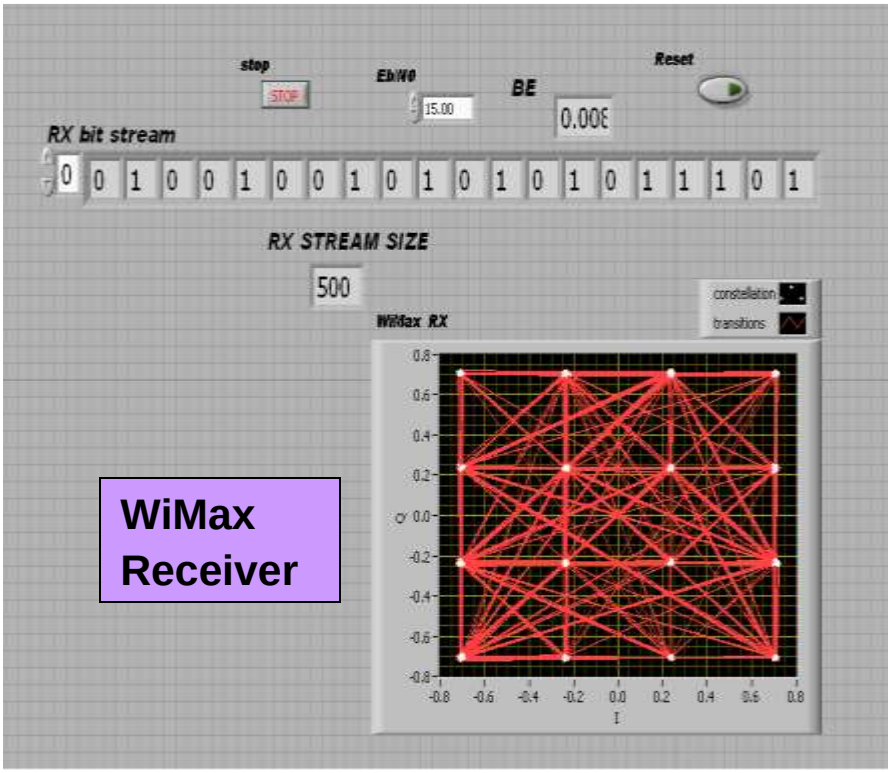

Figure 5-2 Constellation diagram of WiMax Receiver

The performance of the entire WiMax block can be visually seen from the eye diagram and BER vs $_{Eb/No}$ graph which is shown in figure 5-3 & 5-4. The eye diagram is used to analyze the performance of a communication system. It interprets the amount of noise in the signal, signal excursion, amount of distortion at sampling instant and timing jitter. Figure 5.3 shows the eye diagrams of WiMAX receiver. The wide and clear opening of the eye shows that the sampling time has been fully utilized by both the systems. The excursions in top and bottom lines in the eye diagram show the utilization of signal power. It can be noted that signal power is retained to acceptable levels which ensures the reliability of received data. Whereas, BER touches the barrier of 10^{-4} at the Eb/No of 15 dB which is best result achieved out of many computations, which is found to be satisfactory simulation result.

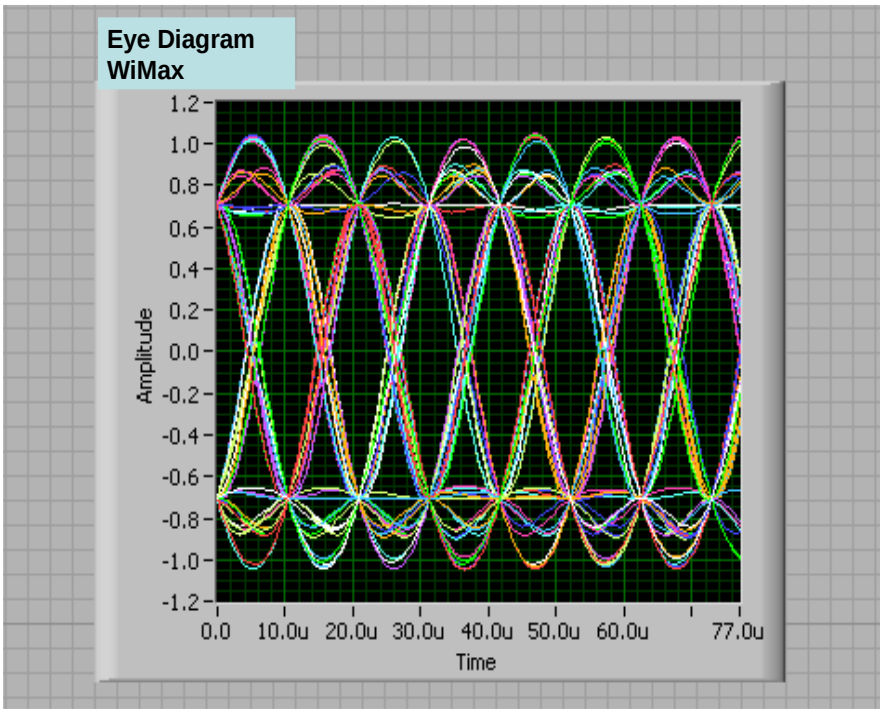

Figure 5-3 WiMax Eye Diag

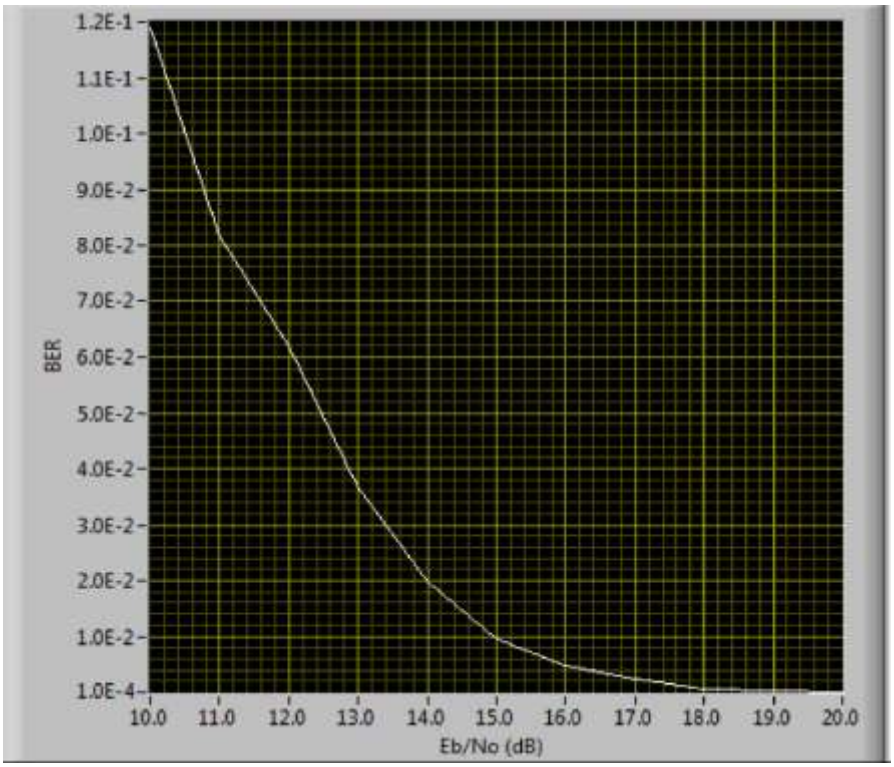

Figure 5-4 BER Vs Eb /No graph WiMax

5.2 WiFi Results

5.2.1 Transmitter / Receiver

Wi-Fi system is also designed in the similar way as of WiMax system, it will also be discussed in two portions and results / discussion will be carried out in transmitter and receiver portion. Transmitter of Wi-Fi system is designed to accept the bits through random bit generator which has been explained in chapter 3, as its input and it transforms it into the QPSK modulated signal after being coded through convolutional encoder of rate 1/3 and passing it through convolutional interleaver. The receiver of the Wi-Fi system is designed to accept the QPSK modulated signal as the input and convert it back to the received bits which was originally given to the transmitter. The Wi-Fi receiver in this project has successfully been able to recover the exact information at Eb/No of 13 db , which found to be acceptable in simulations. The constellation diagram, eye diag transmitted bit stream, Receive bit stream , BER vs $_{Eb/No}$ graph of the Wi-Fi system is shown in figure 5.5 to 5.7.

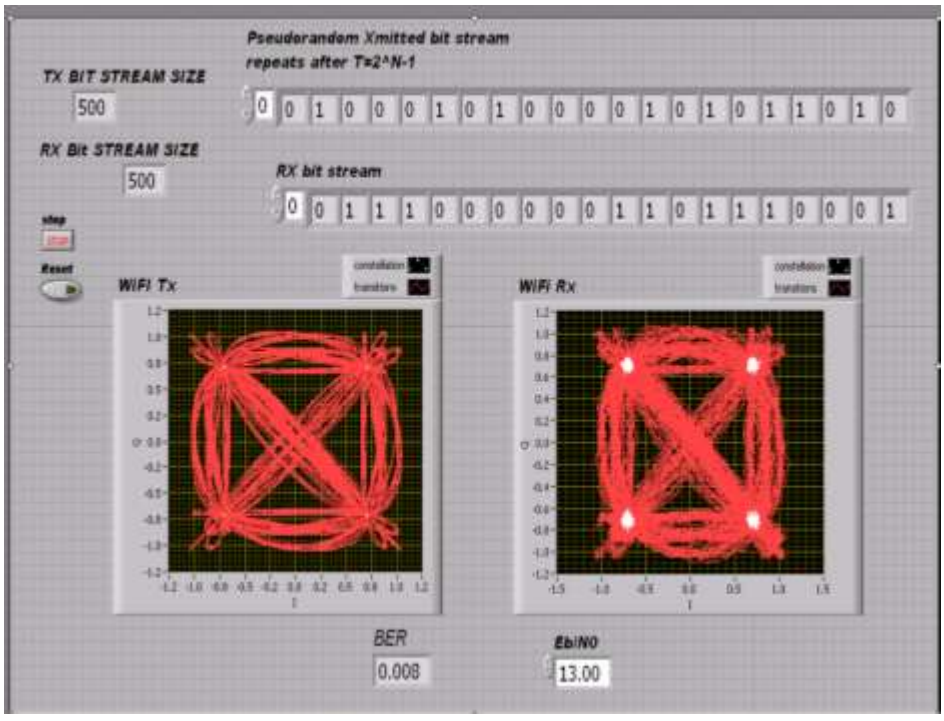

Figure 5-5 Constellation diagram of WiFi Transmitter

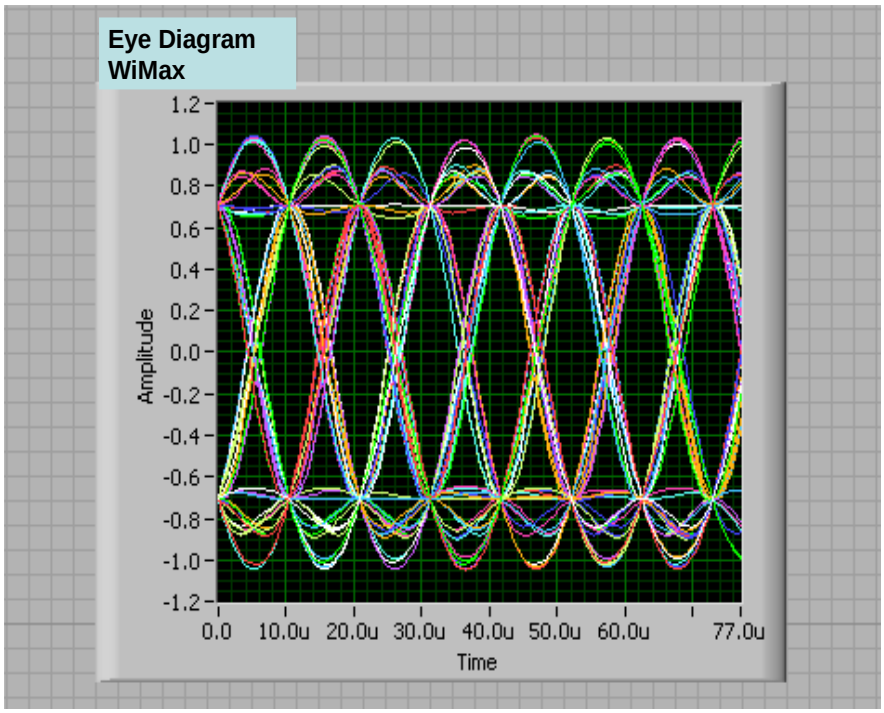

Figure 5-6 Constellation diagram of WiFi Reciever

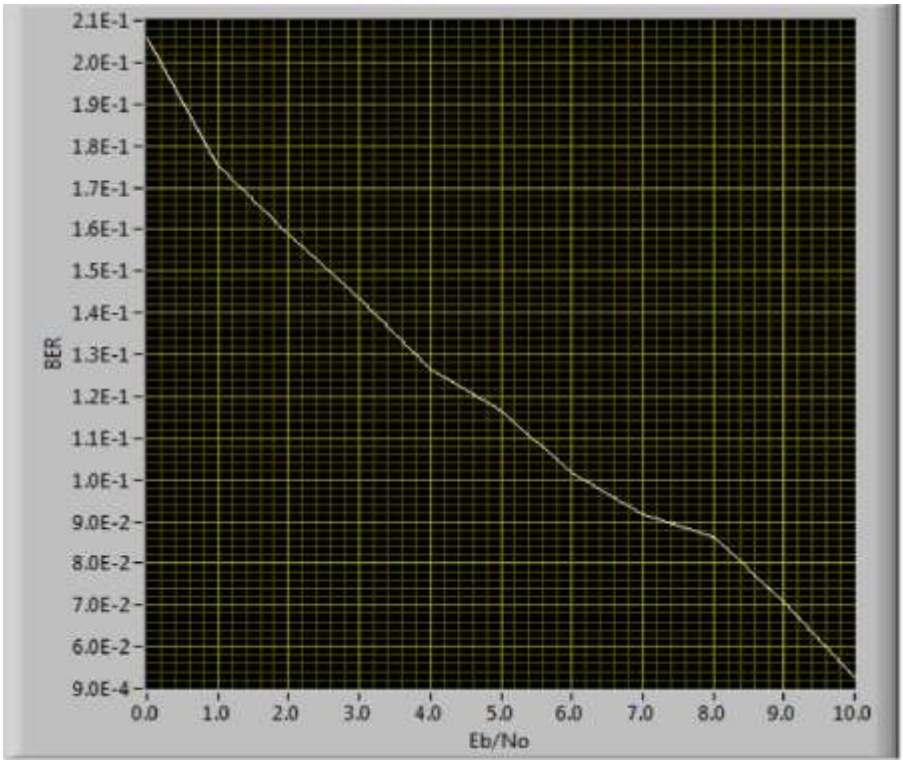

Figure 5-7 Eb/No Vs BER graph of WiMax

The Wi-Fi system simulation is even more satisfactory than WiMax as the 10^{-4} Barrier is crossed at the $_{Eb/No}$ of about 10 dB.

5.3 Results Handover / Interoperability

This section discusses the results achieved for vertical handover between WiMAX and WiFi. The results have been shown in the form of Eye diagrams, Constellation Diagrams and BER graphs. The handover / interoperability process can be tested for different scenarios, in our case there will be four scenarios, which are:

WiMax terminal transmits in WiMax environment

WiFi Terminal transmits in Wi-Fi environment

Wi-Fi terminal transmits in WiMax environment

Wi-Fi terminal transmits in Wi-Fi Environment

Two of the above i.e. first and 2nd are the Normal situations which do not Require the interoperability module. Therefore, this module has been tested for the rest of the two scenarios which are discussed separately.

5.3.1. WiMax Terminal in WiFi environment

BTS Function generates the environment of WiMax, for which the AR coefficient) ends are Calculated by the LPC sub-vi, in the MS function. These coefficients are sent to the identifier sub-vi which then identifies the environment. Then, based on the environment, the MS selects the appropriate circuitry for transmission of data. Bits generator generates the bits, convolution channel coding is applied before the bits are modulated with 16 QAO, then 16 QAM waveform is then demodulated with 16 PSK and then modulated with QPSK. Since the systems are differentiated on the basis of their respective modulation schemes, so 16 QAM applied, which is the scheme for WiMax, 16 PSK has been applied to maintain the secrecy and integrity of the user's data, as the bits are completely randomized or in other words scrambled, and finally QPSK is applied so that the WiFi system may detect the signals, thereby enabling communication to be established. The constellation diagram of fig 5.8 depicts the various stages of interoperability

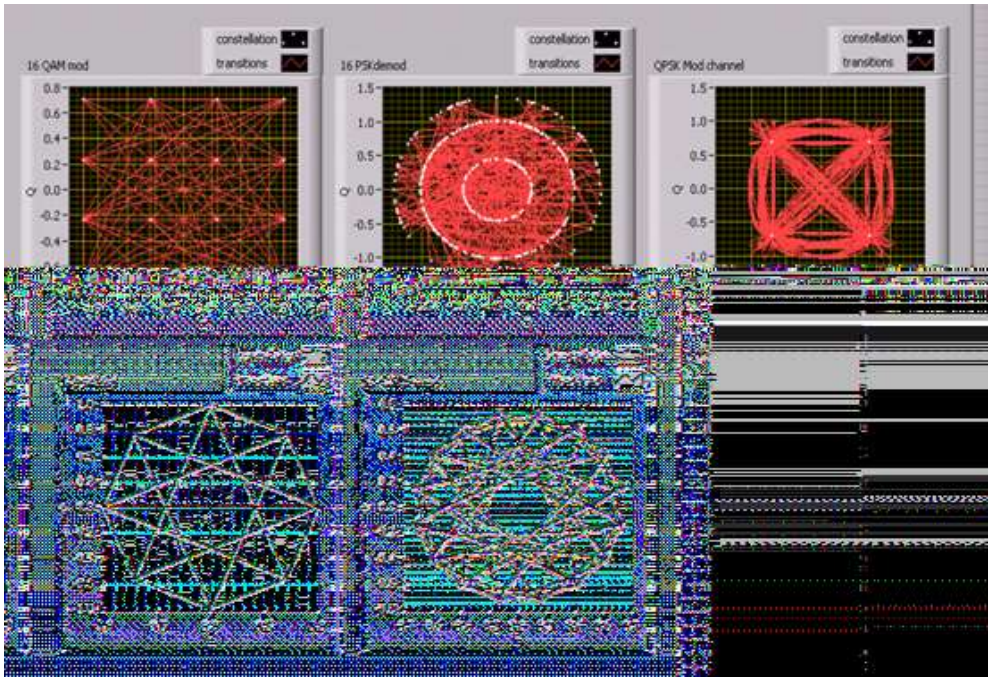

Figure 5-8 Constellation diagram of various stages of handover of WiMax to WiFi

Figure 5-9 shown as below depicts the eye diagrams of Handover scenarios between WiMAX and WiFi. It is obvious from the figures that there is uniformity in eye openings and signals are sampled ideally. Some loss of signal power is observed from excursions in top and bottom lines of the eye openings.

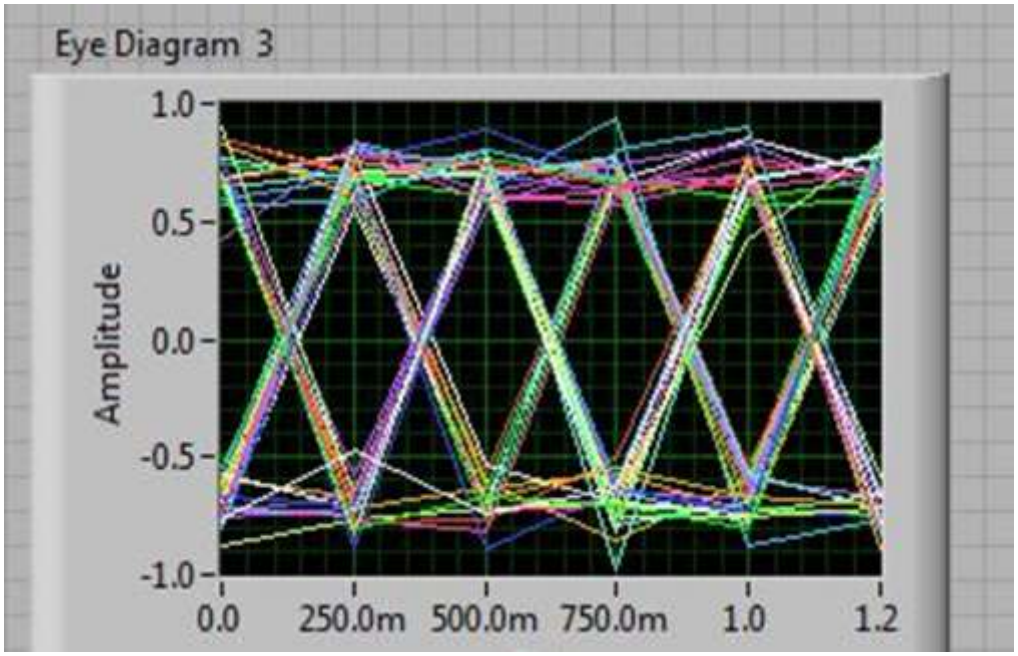

Figure 5-9 Eye Diagram – Results of vertical handover from WiMAX to WiFi

5.3.2 WiFi Terminal in WiMax environment

In this scenario when selection of BTS functions in simulator generates the environment of WiFi after calculation of the AR coefficients by the LPC sub-vi, in the MS function. These coefficients are sent to the identifier sub-vi which identifies the environment. Based on the environment, the MS comes to know that handover has come mandatory then it switches to appropriate circuitry of interoperability for transmission of data. Bits generator generates the bits, convolution channel coding and convolutional interleaving is applied before the bits are modulated with QPSK, then QPSK waveform is then demodulated with 4SPSK and then modulated with 16 QAM and the channel is fed to AWGN. Since the systems are differentiated on the basis of their respective modulation schemes, so QPSK applied, which is the scheme for WiFi, 4SPSK has been applied to maintain the secrecy and integrity of the user's data, as the bits are completely randomized or in other words scrambled, and finally 16 QAM which is environment scheme is applied so that the WiMax system may detect the signals, thereby enabling communication to be established. Constellation diagram in fig 5-10 depicts the various stages of interoperability of this scenario and fig 5-11 shows the result of handover in eye diagram.

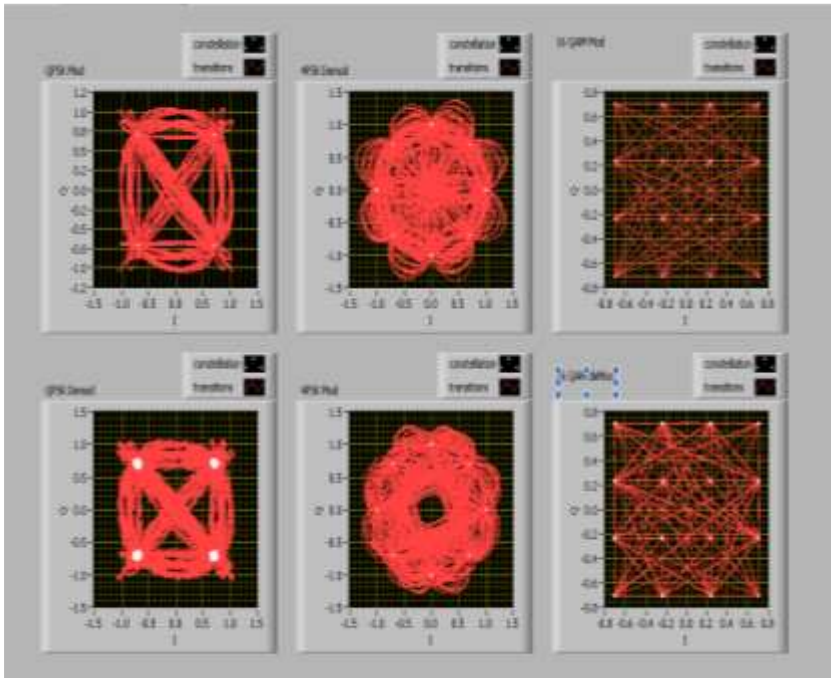

Figure 5-10 Constellation diagram of various stages of handover of WiFi to WiMax

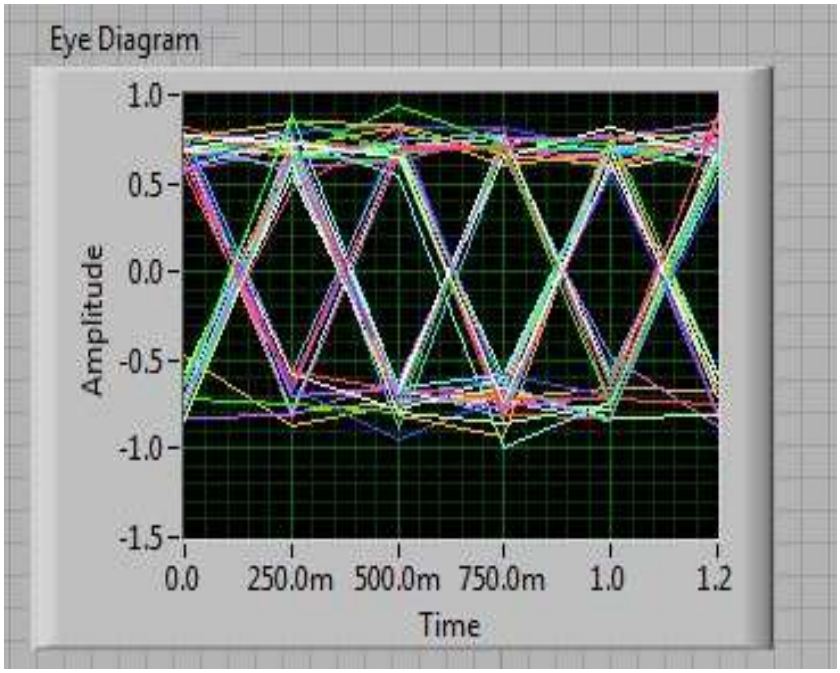

Figure 5-11 Eye Diagram – Results of vertical handover from WiFi to WiMAX

Chapter 6

CONCLUSION

The handover between WiMAX and WiFi is a practical implementation of initial step towards a great cause of a global access network where all the wireless technologies can enhance the services and coverage by interoperability, where, the end user will get connectivity at all time and even during catastrophes like Tsunami and Earth Quake. This research work has targeted on designing a vertical handover solution for WiMAX and WiFi at physical layer level on RF side without going or any change of hardware in the core network of wireless communication systems.

A way forward towards accomplishment of research work was study of WiMax and WiFi in detail and understands the differences between both technologies. Physical layers of WiMAX and WiFi have been simulated using Lab VIEW. A network identification module has been designed that determines the network of origin of data and performs handover process.

The results of handover between WiMax and WiFi, as shown by constellation diagrams, eye diagrams and BER vs. Eb/No ratio graphs, which interprets successful handover between both technologies and hence, are the proof of call connectivity in deep channel fades.

This idea of connectivity can be further improved and optimized by minimizing latency, Bit Error Rate, and inclusion of real time environment by removing channel impairment. Conclusively, the endeavor of establishing the interoperability between WiMax and Wi-Fi systems has successfully been completed.

FURURE WORK

Research is an on-going process and this work is by no means is concluded. Rather it is hoped that it will serve as a foundation for future endeavours in this global cause.

Since the series of these project has been conducted and in progress to find the optimum level of interoperability between different wireless systems. One of such effort has been initiated with name of Project-25 and simultaneously WiMax international forum of interoperability has also invited different wireless systems to join hands for achieving Global Access Network.

The effort made in College of Signals (NUST) Pakistan in series of research is to find the optimum way to make different wireless systems including few systems of P-25 interoperable at Radio lvl. These systems are made interoperable with network identifier / translator. Different methods have been adopted to identify two networks and make them interoperable which will be resultantly developed as statistical identifier and followed by handovers of multi wireless communication systems.

Furthermore, to improve the performance of researched identifier there is a need to improve LPC and AR coefficient. To eliminate the error of transition from one system to another system during handover scenarios can be removed by increasing the number of AR coefficient points which are taken as reference for selection of constellation point/ modulation. After removing these errors and development of statistical identifier, there is a dire need to select a SNR level which should be taken as reference to initiate the handover process. The SNR level should be such, where the parent system should not drop the call and should have the margin in term of time before dropping a call or vertical handover. The tested system can then be implemented on hardware like FPGA or using the SDR technique. The implemented hardware can then be deployed by the commercial networks and made available for the use by general public. On the other side, it can also be used as the backup technology for the communication systems where due to failure of one system, the communication can be continued through the other system. In short, this work can be used to bring a major change in communication perspective.