

Study of WiMAX Simulation

A Thesis

Submitted to the Department of Computer Science and Engineering

of

BRAC University

By

Ahmed Al Amin

ID: 05210025

Moniruzzaman Khan

ID: 05210026

Md. Saiful Alam

ID: 05210024

Riaz Mohammad Mony

ID: 02201093

In Partial Fulfillment of the

Requirements for the Degree

of

Bachelor of Science in electronics and communication engineering

May 2008

DECLARATION

We hereby declare that this thesis is based on the results found by ourselves. Materials of work found by other researcher are mentioned by reference. This thesis, neither in whole nor in part, has been previously submitted for any degree.

Signature of
Supervisor

Signature of
Authors

ACKNOWLEDGMENTS

Special thanks to our honorable supervisor Dr. Tarik A. Chowdhury for his help and support to proceed our thesis on WiMAX technology, to our co-supervisor Amina Hasan Abedin for her co-operation, to Mr. Rajab for his technical support and assistance in hardware part of our thesis, to Mr Altaf for his assistance in the computer lab.

ABSTRACT

In modern world wireless communication systems are involved in every part of life. WiMAX is the upcoming wireless system which uses IEEE standard 802.16. By using WiMAX technology we can overcome the limitations of the existing wireless communication like short coverage area, lack of security and low data rate. In our thesis, initially we analyzed the basic concept of WiMAX. Then we tested transmission and reception of WIMAX technology by using MATLAB simulation. In this process we have transferred a data array from the transmitter, passed it through a channel, received the signal from a receiver, and recovered the main signal. We have also worked on the hardware implementation of WiMAX network with door lock and window alarm system. In the simulation part the input data that we have transmitted was recovered and there were no distortion in the recovered signal. From the graphical representation we come to know that the error rate is zero. In the hardware part when the input password matches with the set password in the lock system a sharp signal is sent otherwise a faded signal is sent. The received signal at the receiver was distorted a bit but the result was satisfactory.

TABLE OF CONTENTS

	Page
TITLE.....	1
DECLARATION.....	2
ACKNOWLEDGEMENTS.....	3
ABSTRACT.....	4
TABLE OF CONTENTS.....	5
LIST OF FIGURES.....	7
LIST OF TABLES.....	8
CHAPTER - I CONCEPT OF WiMAX	
1.1 Basic concept of WiMAX	9
1.2 Standard of WiMAX	11
1.3 Spectrum Allocation	15
1.4 Network Architecture	18
1.5 How WiMAX Works	20
1.6 WiMAX Security	22
1.7 Others important features of WiMAX	23
1.8 WiMAX versus 3G and Wi-Fi	25
CHAPTER - 2 SIMULATIONS	
2.1 Simulation plan	29
2.2 MATLAB code	29
2.3 SIMULINK implementation	30
2.3.1 Security	30
2.3.2 Transmitter	30
2.3.3 Channel	33
2.3.4 Receiver	45
2.4 Result Analysis	52

CHAPTER-3 HARDWARE IMPLEMENTATION

3.1 Security system based on WiMAX	54
3.2.1 Transmitter	56
3.2.2 Receiver	59
3.3.1 Door Security System	61
3.3.2 Window Alarm System	64
3.4 Result analysis	66

CHAPTER-4 FUTURE IMPLEMENTATION & CONCLUSION

4.1 Future implementation	67
4.2 Conclusion	68

CHAPTER-5 REFERENCES

LIST OF LIST OF FIGURES

Fig 1.1: Overview of WiMAX Technology.....	8
Fig 1.2: IP-Based WiMAX Network Architecture.....	17
Figure 1.3 Functions performed across reference points.....	18
Fig 1.4: WiMAX operation.....	19
Fig 1.5: Fixed WiMAX Using CPE.....	20
Fig 1.6: Overall WiMAX Structure.....	26
Fig 2.1: WiMAX Transmitter and Receiver with Sensor and Control Unit.....	27
Fig 2.2: Input / Source data.....	29
Fig 2.3: Eye diagram of randomizing data.....	30
Fig 2.4: Block diagram of Encoding Process [1].....	30
Fig 2.5: Convolutional Encoder of Binary rate $\frac{1}{2}$ [1].....	32
Fig 2.6: Eye diagram of the data after encoding.....	35
Fig 2.7: After modulating the signal.....	36
Fig 2.8: After take the r.m.s value of the signal.....	36
Fig 2.9: OFDM symbol.....	37
Fig 2.10: OFDM burst structure obtained after assembling [1].....	38
Fig 2.11: Eye diagram of OFDM symbol.....	38
Fig 2.12: Rearrangement performed before realizing the IFFT operation [1].....	39
Fig 2.13: Eye diagram after performing IFFT.....	40
Fig 2.14: OFDM symbol with the cyclic prefix.....	40
Fig 2.15: Data after adding cyclic prefix.....	41
Fig 2.16: Output curve for Rician Fading Channel & AWGN Channel.....	43
Fig 2.17: Eye diagram of the received signal after removing cyclic prefix.....	44
Fig 2.18: received signal after demodulation.....	45
Fig 2.19: Block diagram of decoding [1].....	46
Fig 2.20: received signal after Decoding & Reorder.....	49
Fig 2.21: Output data.....	50
Fig 2.22: Graph of input and output data.....	50
Fig 2.23: Graph of Error rate	51
Fig 3.1: The scenario of the WiMAX system [4].....	52
Fig: 3.2 Fm Transmitter [5].....	54
Fig: 3.3 Hardware implementation of Transmitter.....	55
Fig: 3.4 FM Receiver [6].....	57
Fig: 3.5 Hardware implementation of Receiver.....	58
Fig: 3.6 Hardware implementation of Door security system [7].....	59
Fig: 3.7 Hardware implementation of Door security system.....	60
Fig: 3.8 Window alarm system.....	62
Fig: 3.9 Hardware implementation of window alarm system.....	63
Fig: 3.10 Result analysis.....	64

LIST OF TABLES

1.1 Basic Data on IEEE 802.16 Standards.....	10
1.2 Fixed and Mobile WiMAX Initial Certification Profiles.....	12
1.3 Summary of Potential Spectrum Options for Broadband Wireless.....	15
1.4 Comparison of WiMAX (Fixed and Mobile) with Other Broadband Wireless Technologies.....	25
2.1 Various rate of Puncturing Process [1].....	33

Chapter # 1

1.1 Basic concept of WiMAX

WiMAX, the **Worldwide Interoperability for Microwave Access**, is a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. It is a wireless digital communications system that is intended for wireless "metropolitan area networks". This technology can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations.

WiMAX is a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to wired broadband like cable and DSL. WiMAX provides fixed, nomadic, and portable. Soon, mobile wireless broadband connectivity without the need for direct line-of-sight with a base station. In a typical cell radius deployment of three to ten kilometers, WiMAX Forum Certified systems can be expected to deliver capacity of up to 40 Mbps per channel, for fixed and portable access applications.

Many companies are closely examining WiMAX for the "last mile" connectivity at high data rates. The resulting competition may bring lower pricing for both home and business customers or bring broadband access to places where it has been economically unavailable. Prior to WiMAX, many operators have been using proprietary fixed wireless technologies for broadband services. [2] [9][10]

The bandwidth and reach of WiMAX make it suitable for the following potential applications:

- ◆ Connecting Wi-Fi hotspots with each other and to other parts of the Internet.
- ◆ Providing a wireless alternative to cable and DSL for last mile broadband access.
- ◆ Providing high-speed data and telecommunications services.
- ◆ Providing a diverse source of Internet connectivity as part of a business continuity plan. That is, if a business has a fixed and a wireless Internet connection, especially from unrelated providers, they are unlikely to be affected by the same service outage.
- ◆ Providing nomadic connectivity.

High speed data and nomadic connectivity of the WiMAX technology enables the freedom and convenience that comes from having your Internet standing by where and when we need it—staying connected on the go to the people, communities, and resources that make up our lives. Broadband on the go is your

front row seat to all the rich multimedia Internet applications you already use, and exciting future possibilities enabled by Mobile WiMAX. [2] [9][10]

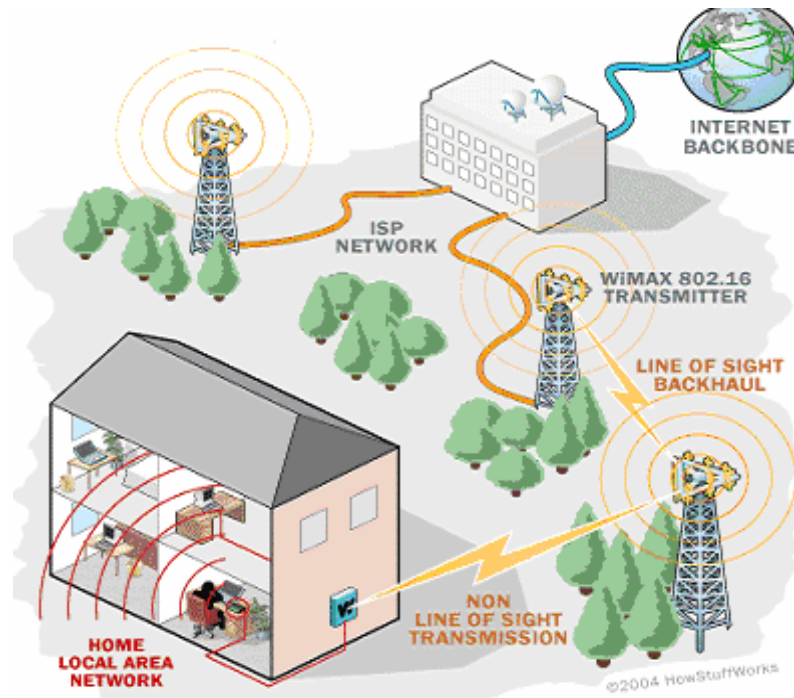


Fig 1.1: Overview of WiMAX Technology

Playing in Real-Time: Play multiplayer 3-D games, view You Tube videos, and listen to radio broadcasts— it's all there waiting to entertain us on the go.

Working Smarter: WiMAX pulls productivity out of thin air. Capture lost time by doing things in areas previously unavailable. Working on the go changes the rules of competition by allowing us to be more productive.

Staying in Touch: Broadband on the go is about keeping in touch with family, friends, and our communities using all the typical tools like e-mail and IM, but WiMAX adds face-to-face video conferencing and voice to our connections.

Locating People and Places: WiMAX enables a spontaneous lifestyle. Location-based services creates a new paradigm in accessing real-time information where and when we need it.

Receiving TV and Radio on the Go: There are just more streams of data available with WiMAX, so why not pipe broadcast television and radio into a Mobile WiMAX device? Radio stations already co-broadcast over the Internet. Mobile Internet-based TV Transmissions also set the stage for content-on-demand services like movies and sporting events. [14]

1.2 Standard of WiMAX

WiMAX technology is based on the IEEE 802.16 standard, which is also called Wireless MAN. The IEEE 802.16 group was formed in 1998 to develop an air-interface standard for wireless broadband. The group's initial focus was the development of a LOS-based point-to-multipoint wireless broadband system for operation in the 10GHz–66GHz millimeter wave band. The resulting standard—the original 802.16 standard, completed in December 2001—was based on a single-carrier physical (PHY) layer with a burst time division multiplexed (TDM) MAC layer.

The IEEE 802.16 group subsequently produced 802.16a, an amendment to the standard, to include NLOS applications in the 2GHz–11GHz band, using an orthogonal frequency division multiplexing (OFDM)-based physical layer. Additions to the MAC layer, such as support for orthogonal frequency division multiple access (OFDMA), were also included. Further revisions resulted in a new standard in 2004, called IEEE 802.16-2004, which replaced all prior versions and formed the basis for the first WiMAX solution. These early WiMAX solutions based on IEEE 802.16-2004 targeted fixed applications, and we will refer to these as fixed WiMAX. In December 2005, the IEEE group completed and approved IEEE 802.16e-2005, an amendment to the IEEE 802.16-2004 standard that added mobility support. The IEEE 802.16e-2005 forms the basis for the WiMAX solution for nomadic and mobile applications and is often referred to as mobile WiMAX

1.1 Basic Data on IEEE 802.16 Standards [8]

	802.16	802.16-2004	802.16e-2005
Status	Completed December 2001	Completed June 2004	Completed December 2005
Frequency band	10GHz–66GHz 2GHz–11GHz	2GHz–11GHz for fixed;	2GHz–6GHz for mobile applications
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS
MAC architecture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission Scheme	Single carrier only	Single carrier, 256 OFDM or 2,048 OFDM	Single carrier, 256 OFDM or scalable OFDM with 128, 512, 1,024, or 2,048 Sub carriers
Gross data rate	32Mbps–134.4Mbps	1Mbps–75Mbps	1Mbps–75Mbps
Multiplexing Duplexing	Burst TDM/TDMA	Burst TDM/TDMA/ OFDMA	Burst TDM/TDMA/ OFDMA
Channel bandwidths	TDD and FDD	TDD and FDD	TDD and FDD
Air-interface designation	WirelessMAN-SC	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMANa	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMANa
WiMAX implementatio	None	256 - OFDM as Fixed WiMAX	Scalable OFDMA as Mobile WiMAX

Currently, the WiMAX Forum has two different system profiles: one based on IEEE 802.16-2004, OFDM PHY, called the fixed system profile; the other one based on IEEE 802.16e-2005 scalable OFDMA PHY, called the mobility system profile. A certification profile is defined as a particular instantiation of a system profile where the operating frequency, channel bandwidth, and duplexing mode are also specified. WiMAX equipments are certified for interoperability against a particular certification profile.

The WiMAX Forum has thus far defined five fixed certification profiles and fourteen mobility certification profiles. To date, there are two fixed WiMAX profiles against which equipment have been certified. These are 3.5GHz systems operating over a 3.5MHz channel, using the fixed system profile based on the IEEE 802.16-2004 OFDM physical layer with a point-to-multipoint MAC. One of the profiles uses frequency division duplexing (FDD), and the other uses time division duplexing (TDD).

With the completion of the IEEE 802.16e-2005 standard, interest within the WiMAX group has shifted sharply toward developing and certifying mobile WiMAX1 system profiles based on this newer standard. All mobile WiMAX profiles use scalable OFDMA as the physical layer. At least initially, all mobility profiles will use a point-to-multipoint MAC. It should also be noted that all the current candidate mobility certification profiles are TDD based. Although TDD is often preferred, FDD profiles may be needed for in the future to comply with regulatory pairing requirements in certain bands. [8][9]

Table 1.2 Fixed and Mobile WiMAX Initial Certification Profiles [8]

Mobile WiMAX					
Band index	Frequency Band	Channel Bandwidth (MHz)	OFDM FFT size	Duplexing	Notes
Fixed WiMAX					
1	3.5 GHz	3.5	256	FDD	Product already certified
		3.5	256	TDD	
		7	256	FDD	
		7	256	TDD	
2	5.8 GHz	10	256	TDD	
1	2.3GHz–2.4GHz	5	512	TDD	Both bandwidths must be supported by mobile station (MS)
		10	1024	TDD	
		8.75	1024	TDD	
2	2.305GHz–2.320GHz, 2.345GHz–2.360GHz	3.5	512	TDD	
		5	512	TDD	
		10	1024	TDD	
3	2.496GHz–2.69GHz	5	512	TDD	
		10	1024	TDD	
4	3.3GHz–3.4GHz	5	512	TDD	
		7	1024	TDD	
		10	1024	TDD	
5	3.4GHz–3.8GHz, 3.4GHz–3.6GHz, 3.6GHz–3.8GHz	5	512	TDD	
		7	1024	TDD	
		10	1024	TDD	

1.3 Spectrum Allocation

From a global perspective, the 2.3GHz, 2.5GHz, 3.5GHz, and 5.7GHz bands are most likely to see WiMAX deployments. The WiMAX Forum has identified these bands for initial interoperability Certifications. A brief description of these bands follows.

Licensed 2.5GHz: The bands between 2.5GHz and 2.7GHz have been allocated in the United States, Canada, Mexico, Brazil, and some Southeast Asian countries. In many countries, this band is restricted to fixed applications; in some countries, two-way communication is not permitted. Among all the available bands, this one offers the most promise for broadband wireless, particularly 2.495GHz and 2.690GHz. Regulations allow a variety of services, including fixed, portable, and mobile services. Both FDD and TDD operations are allowed. Licenses were issued for eight 22.5MHz slices of this band, where a 16.5MHz block is paired with a 6MHz block, with the separation between the two blocks varying from 10MHz to 55MHz. The rules of this band also allow for license aggregation. Sprint, Nextel, and Clearwire control a majority of this spectrum in the United States. Regulatory changes may be required in many countries to make this band more available and attractive, particularly for mobile WiMAX.

Licensed 2.3GHz: This band, called the WCS band. This is available in many countries such as US, Australia, South Korea, and New Zealand. In fact, the WiBro services being deployed in South Korea uses this band. In the United States, this band includes two paired 5MHz bands and two unpaired 5MHz bands in the 2.305GHz to 2.320GHz and 2.345GHz to 2.360GHz range. A major constraint in this spectrum is the tight out-of-band emission requirements enforced by the FCC to protect the adjacent DARS (digital audio radio services) band (2.320GHz to 2.345GHz). This makes broadband services, particularly mobile Services, difficult in the sections of this band closest to the DARS band.

Licensed 3.5GHz: This is the primary band allocated for fixed wireless broadband access in several countries across the globe. In the United States, the FCC has recently allocated 50MHz of spectrum in the 3.65GHz to 3.70GHz band for high-power unlicensed use with restrictions on transmission protocols that preclude WiMAX. The available bandwidth varies from country to country, but it is generally around 200MHz. The available band is usually split into many individual licenses, varying from 2.5MHz to 2.56MHz.

Spectrum aggregation rules also vary from country to country. While some countries only allow FDD operations, others allow either FDD or TDD. In most countries, the current rules in this band do not allow for nomadic and mobile broadband applications. It is hoped that the regulations in this band will, over time, become more flexible.

License-exempt 5GHz: The license-exempt frequency band 5.25GHz to 5.85GHz is of interest to WiMAX. This band is generally available worldwide. In the United States, it is part of the unlicensed national information infrastructure (U-NII) band and has 200MHz of spectrum for outdoor use. The FCC for future unlicensed use has identified an additional 255MHz of spectrum in this band. Being free for anyone to use, this band could enable grassroots deployments of WiMAX, particularly in underserved, low-population-density rural and remote markets. The large bandwidth available may enable operators to coordinate frequencies and mitigate the interference concerns surrounding the use of license-exempt bands, particularly in underserved markets.

UHF bands: UHF band spectrum has excellent propagation characteristics compared to the other microwave bands and hence is valuable, particularly for portable and mobile services.

The larger coverage range possible in this band makes the economics of deployment particularly attractive for suburban and rural applications.

AWS band: In August 2006, the FCC auctioned 1.710GHz–1.755GHz paired with 2.110GHz–2.155GHz as spectrum for advanced wireless services (AWS) in the United States. This band offers 90MHz of attractive spectrum that could be viable for WiMAX in the longer term. [8] [9]

Table1.3 Summary of Potential Spectrum Options for Broadband Wireless[8]

Designation	Allocation Frequency	Amount of Spectrum
Fixed wireless access (FWA): 3.5GHz	3.4GHz – 3.6GHz Mostly; 3.3GHz – 3.4GHz and 3.6GHz – 3.8GHz also available in some countries	Total 200MHz mostly; varies from 2 × 5MHz to 2 × 56MHz paired across nations
Broadband radio services (BRS): 2.5GHz	2.495GHz – 2.690GHz	194MHz total; 22.5MHz licenses, where a 16.5MHz is paired with 6MHz
Wireless Communications Services (WCS) 2.3GHz	2.305GHz – 2.320GHz; 2.345GHz – 2.360GHz	Two 2 × 5MHz paired; two unpaired 5MHz
License exempt: 2.4GHz	2.405GHz – 2.4835GHz	One 80MHz block
License exempt: 5GHz	5.250GHz – 5.350GHz; 5.725GHz – 5.825GHz	200MHz available in United States; additional 255MHz to be allocated
UHF band: 700MHz	698MHz – 746MHz (lower); 747MHz – 792MHz (upper)	30MHz upper band; 48MHz lower band
Advanced wireless services (AWS)	1.710GHz – 1.755GHz 2.110GHz – 2.155GHz	2 × 45MHz paired

1.4 Network Architecture

The overall network may be logically divided into three parts:

1. Mobile stations used by the end user to access the network
2. the access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge, and
3. The connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.

The architecture framework is defined such that the multiple players can be part of the WiMAX service value chain. More specifically, the architecture allows for three separate business entities: (1) network access provider (NAP), which owns and operates the ASN; (2) network services provider (NSP), which provides IP connectivity and WiMAX services to subscribers using the ASN infrastructure provided by one or more NAPs; and (3) application service provider (ASP), which can provide value-added services such as multimedia applications using IMS (IP multimedia subsystem) and corporate VPN (virtual private networks) that run on top of IP.

The network reference model developed by the WiMAX Forum Network Working Group defines a number of functional entities and interfaces between those entities.

Base station (BS): The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micro mobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP (Dynamic Host Control Protocol) proxy, key management, session management, and multicast group management.

Access service network gateway (ASN-GW): The ASN gateway typically acts as a layer 2 traffic aggregation points within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management and admission control, caching of subscriber profiles and encryption keys, AAA client functionality, establishment and management of mobility tunnel with base stations, QoS and policy enforcement and foreign agent functionality for mobile IP, and routing to the selected CSN.

Connectivity service network (CSN): The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned

by the NSP and includes AAA servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs. Further, CSN can also provide gateways and interworking with other networks, such as PSTN (public switched telephone network), 3GPP, and 3GPP2.

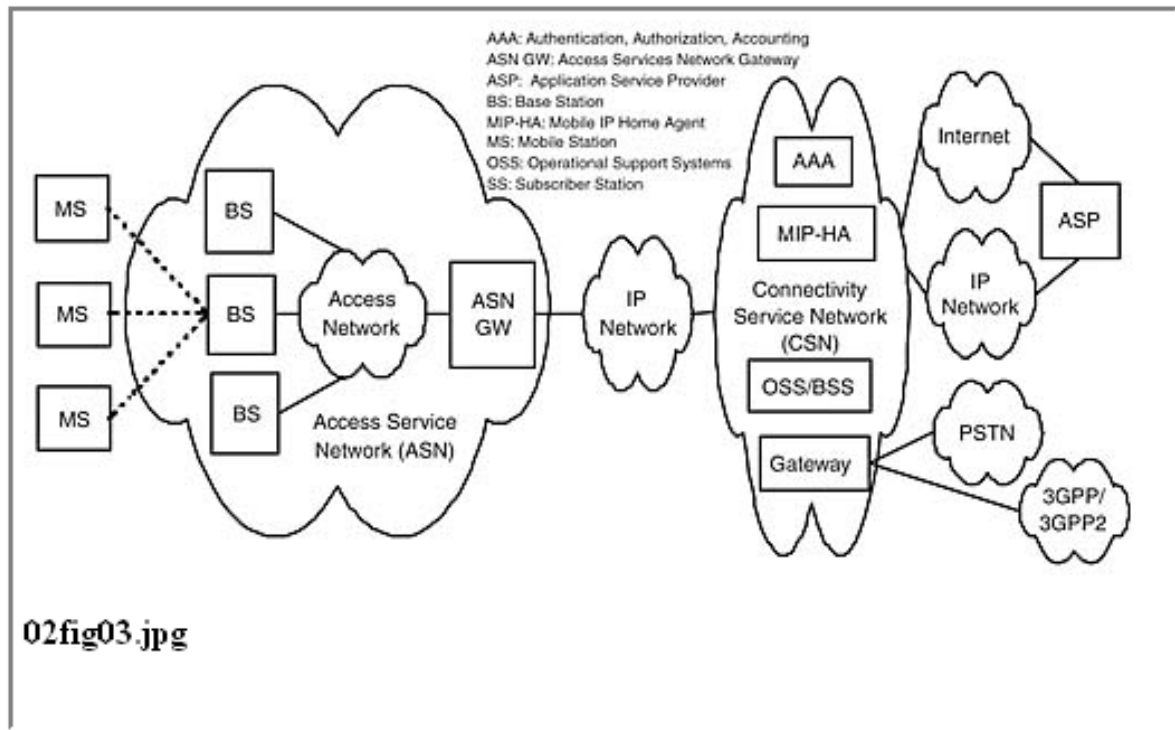


Fig 1.2: IP-Based WiMAX Network Architecture

The WiMAX network reference model defines reference points between: (1) MS and the ASN, called R1, which in addition to the air interface includes protocols in the management plane, (2) MS and CSN, called R2, which provides authentication, service authorization, IP configuration, and mobility management, (3) ASN and CSN, called R3, to support policy enforcement and mobility management, (4) ASN and ASN, called R4, to support inter-ASN mobility, (5) CSN and CSN, called R5, to support roaming across multiple NSPs, (6) BS and ASN-GW, called R6, which consists of intra-ASN bearer paths and IP tunnels for mobility events, and (7) BS to BS, called R7, to facilitate fast, seamless handover.[8] [11] [9]

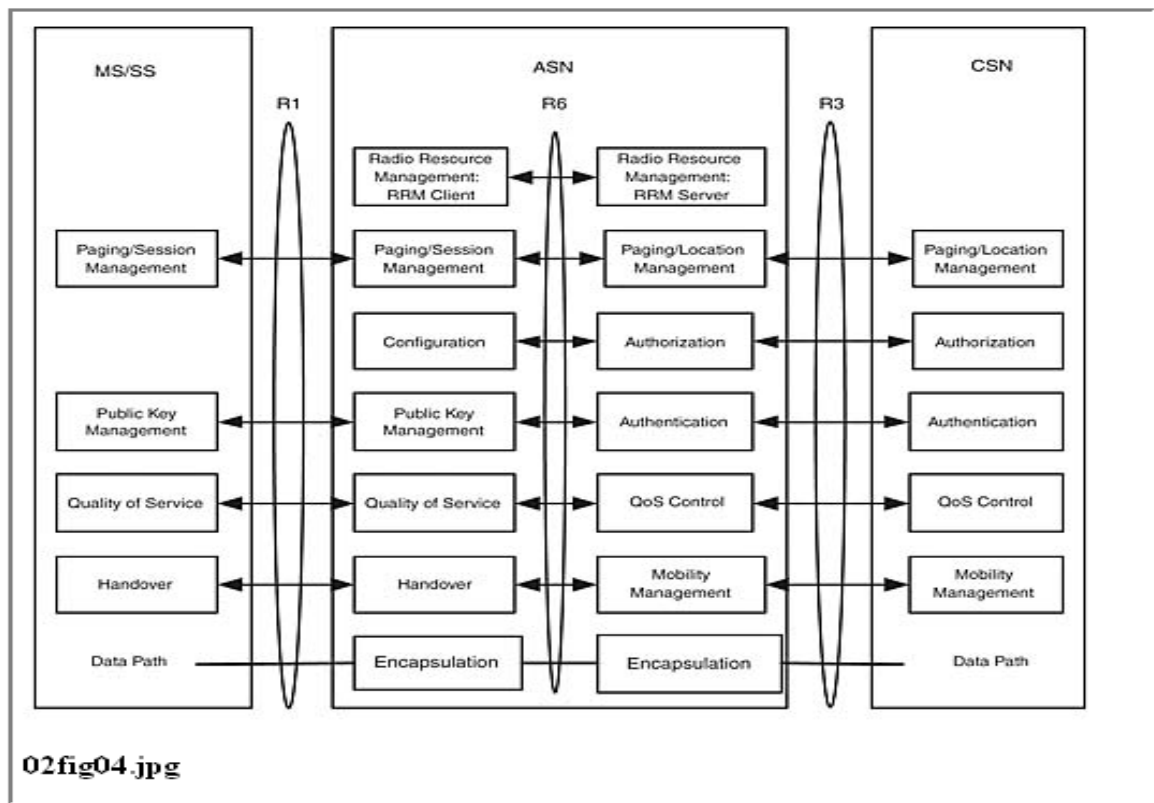


Figure 1.3 Functions performed across reference points

1.5 How WiMAX Works

The WiMAX network uses an approach that is similar to that of cell phones. Coverage for a geographical area is divided into a series of overlapping areas called cells. Each cell provides coverage for users within that immediate vicinity. When subscriber travels from one cell to another, the wireless connection is handed off from one cell to another.

A WiMAX system consists of two parts:

A Base station, similar in concept to a cell-phone tower - A single WiMAX tower can provide coverage to a very large area -- as big as 3,000 square miles

(~8,000 square km).is mounted on a tower or tall building to broadcast the wireless signal.

A WiMAX subscriber device, these could be WiMAX enabled notebook, mobile Internet device (MID), or even a WiMAX modem by using the subscriber receives the signals.

The user pays the service provider for wireless Internet access, just as they would for a normal Internet connection via a cable network. The service provider provides the end user with the software, a login and a password. Most of the laptop manufacturers today equip high-end models with a built in antenna bundled with the required software for the unit to be WiMAX compatible. The service provider beams the internet signals from the base station. The antenna at the user end catches the signals, providing uninterrupted internet as long as the signal is available. With a laptop equipped with an antenna you could be connected to the Internet wherever the signal is available from the base station. As with mobile station that catch a signal from the nearest tower of the particular service provider, so is it with new generation WiMAX services. One WiMAX base station can send signals over distances of several miles depending on the terrain. The more flat the terrain, more the coverage. If end user moves from one base station area to another, your laptop receiver will hook up to the other base station (of the same service provider) with a stronger signal.

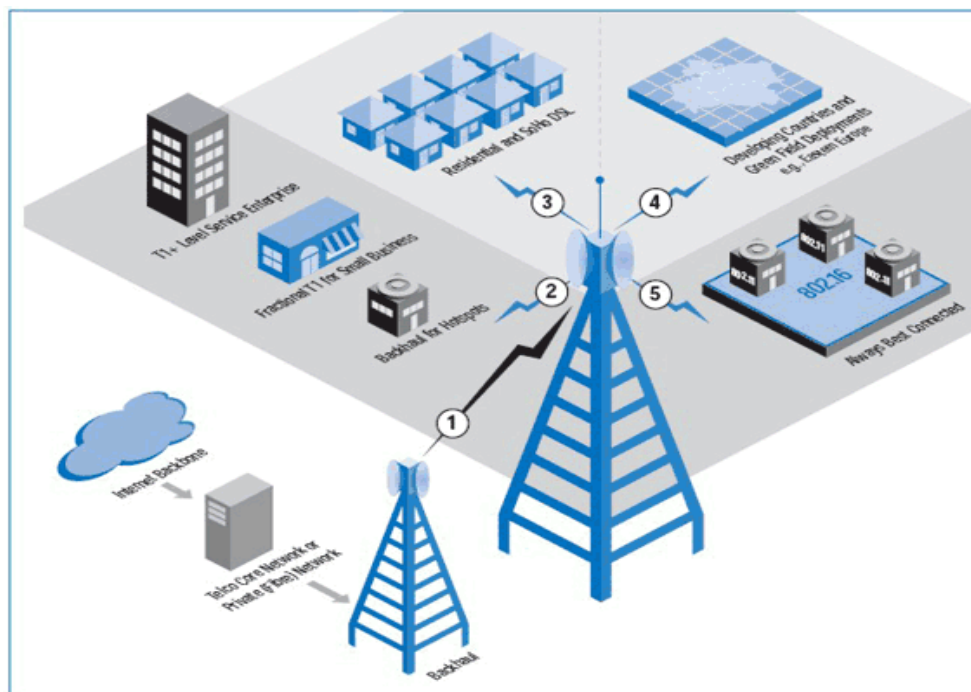


Fig 1.4: WiMAX operation

For fixed WiMAX deployments, service providers supply Customer Premises Equipment (CPE) that acts as a wireless “modem” to provide the interface to the WiMAX network for a specific location, such as a home, cafe, or office. WiMAX is also well Suited for emerging markets as a cost-effective way to deliver high-speed Internet. [12] [13]

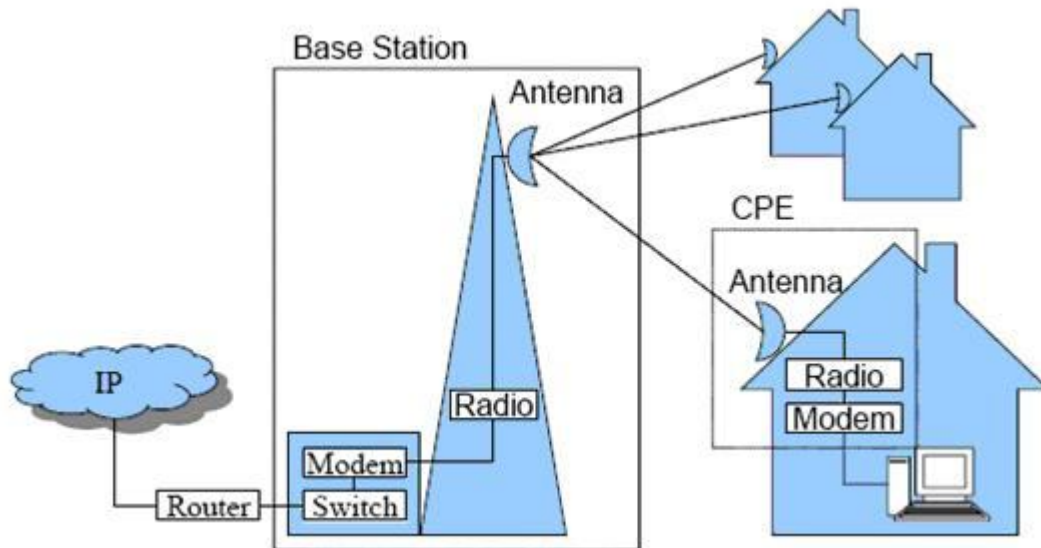


Fig 1.5: Fixed WiMAX Using CPE

1.6 WiMAX Security:

Designed by the IEEE 802.16 committee, WiMAX was developed after the security failures that plagued early IEEE 802.11 networks. Recognizing the importance of security, the 802.16 working groups designed several mechanisms to protect the service provider from theft of service, and to protect the customer from unauthorized information disclosure.

The standard includes state-of-the-art methods for ensuring user data privacy and preventing unauthorized access, with additional protocol optimization for mobility. A privacy sub layer within the WiMAX MAC handles security. The key aspects of WiMAX security are as follow.

Support for privacy: User data is encrypted using cryptographic schemes of proven robustness to provide 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 new encryption standard approved as compliant with Federal Information Processing Standard (FIPS) and is easier to implement.

Device/user authentication: WiMAX provides a flexible means for authenticating subscriber stations and users to prevent unauthorized use. The authentication framework is based on the Internet Engineering Task Force (IETF) EAP, which supports a variety of credentials, such as username/password, digital certificates, and smart cards. WiMAX terminal devices come with built-in X.509 digital certificates that contain their public key and MAC address. WiMAX operators can 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 transferring keying material from the base station to the mobile station, periodically reauthorizing and refreshing the keys. PKM is a client-server protocol: The MS acts as the client; the BS, the server. PKM uses X.509 digital certificates and RSA (Rivest-Shamir-Adleman) public-key encryption algorithms to securely perform key exchanges between the BS and the MS.

Protection of control messages: using message digest schemes, such as AES-based CMAC or MD5-based HMAC.11, protects the integrity of over-the-air control messages.

Support for fast handover: To support fast handovers, WiMAX allows the MS to use pre-authentication with a particular target BS to facilitate accelerated reentry. A three-way handshake scheme is supported to optimize the re-authentication mechanisms for supporting fast handovers, while simultaneously preventing any man-in-the-middle attacks. [8] [9] [11]

1.7 Others important features of WiMAX:

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

Scalable bandwidth and data rate support: WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth. This scalability is supported in the OFDMA mode, where the FFT (fast fourier transform) size may be scaled based on the available channel

bandwidth. For example, a WiMAX system may use 128-, 512-, or 1,048-bit FFTs based on whether the channel bandwidth is 1.25MHz, 5MHz, or 10MHz, respectively. This scaling may be done dynamically to support user roaming across different networks that may have different bandwidth allocations.

Adaptive modulation and coding (AMC): WiMAX supports a number of modulations and forward error correction (FEC) coding schemes and allows the scheme to be changed on per user and per frame basis, based on channel conditions. AMC is an effective 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 user is provided with the highest possible data rate that can be supported in their respective links

Link-layer retransmissions: For connections that require 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; unacknowledged packets are assumed to be lost and are retransmitted. WiMAX also optionally supports hybrid-ARQ, which is an effective hybrid between FEC and ARQ.

Support for TDD and FDD: IEEE 802.16-2004 and IEEE 802.16e-2005 supports both time division duplexing and frequency division duplexing, as well as a half-duplex FDD, which allows for a low-cost system implementation. TDD is favored by a majority of implementations because of its advantages: (1) flexibility in choosing uplink-to-downlink data rate ratios, (2) ability to exploit channel reciprocity, (3) ability to implement in non-paired spectrum, and (4) less complex transceiver design. All the initial WiMAX profiles are based on TDD, except for two fixed WiMAX profiles in 3.5GHz.

Orthogonal Frequency Division Multiple Accesses (OFDMA): Mobile WiMAX uses OFDM as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones. As discussed in detail in Chapter 6, OFDMA facilitates the exploitation 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 controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme. When using the OFDMA-PHY mode, multiplexing is additionally done in the frequency dimension, by allocating different subsets of OFDM sub carriers to different users. Resources may be allocated in the spatial domain as well 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 mechanism to convey the resource allocation information on a frame-by-frame basis.

Support for advanced antenna techniques: The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beam forming, space-time coding, and spatial multiplexing. These schemes can be used to improve the overall system capacity and spectral efficiency by deploying multiple antennas at the transmitter and/or the receiver. Chapter 5 presents detailed overview of the various multiple antenna techniques.

Quality-of-service support: The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services. The system offers support for constant bit rate, 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 users, with multiple connections per terminal, each with its own QoS requirement. [8] [9]

1.8 WiMAX versus 3G and Wi-Fi

WiMAX is not the only solution for delivering broadband wireless services. Several proprietary solutions are already in the market.

Third-generation cellular systems and IEEE 802.11-based Wi-Fi systems are also playing a vital role in un-tether access of Internet throughout the world.

Here we are going to discuss on WiMAX versus 3G and Wi-Fi

The throughput capabilities of WiMAX depend on the channel bandwidth used. Unlike 3G systems, which have a fixed channel bandwidth, WiMAX defines a selectable channel bandwidth from 1.25MHz to 20MHz, which allows for a very flexible deployment. When deployed using the more likely 10MHz TDD (time division duplexing) channel, assuming a 3:1 downlink-to-uplink split and 2 × 2 MIMO, WiMAX offers 46Mbps peak downlink throughput and 7Mbps uplink.

The reliance of Wi-Fi and WiMAX on OFDM modulation, as opposed to CDMA as in 3G, allows them to support very high peak rates. The need for spreading makes very high data rates more difficult in CDMA systems. More important than peak data rate offered over an individual link is the average throughput and overall system capacity when deployed in a multi-cellular environment. From a capacity standpoint, the more pertinent measure of system performance is spectral efficiency. The fact that WiMAX specifications accommodated multiple antennas right from the start gives it a boost in spectral efficiency. In 3G systems, on the other hand, multiple-antenna support is being added in the form of revisions. Further, the OFDM physical layer used by WiMAX is more amenable to

MIMO implementations than are CDMA systems from the standpoint of the required complexity for comparable gain. OFDM also makes it easier to exploit frequency diversity and multi user diversity to improve capacity. Therefore, when compared to 3G, WiMAX offers higher peak data rates, greater flexibility, and higher average throughput and system capacity. Another advantage of WiMAX is its ability to efficiently support more symmetric links—useful for fixed applications, such as T1 replacement and support for flexible and dynamic adjustment of the downlink-to-uplink data rate ratios. Typically, 3G systems have a fixed asymmetric data rate ratio between downlink and uplink. For the multiplexing WiMAX is using Time division multiplexing (TDM) and Orthogonal Frequency Division Multiplexing Access (OFDMA) where 3G is using Code Division Multiplexing access(CDMA) or TDM and Carrier Sense Multiple Access.(CSMA) is for Wi-Fi. [9] [15]

Table 1.4 Comparison of WiMAX (Fixed and Mobile) with Other Broadband Wireless Technologies[8]:

Parameter	Fixed WiMAX	Fixed WiMAX	GSM	CDMA	Wi-Fi
Standards	IEEE 802.16-2004	IEEE 802.16e-2005	3GPP Release 6	3GPP2	IEEE 802.11a/g/n
Peak down link data rate	9.4Mbps in 3.5MHz with 3:1 DL-to-UL ratio TDD; 6.1Mbps with 1:1	46Mbpsa with 3:1 DL- to-UL ratio TDD; 32Mbps with 1:	14.4Mbps using all 15 codes; 7.2Mbps with 10 codes	3.1Mbps; Rev. B will support 4.9Mbps	54 Mbpsb shared using 802.11a/g;
Peak uplink data rate	3.3Mbps in 3.5MHz using 3:1 DL-to-UL ratio; 6.5Mbps with 1:1	7Mbps in 10MHz using 3:1 DL-to-UL ratio; 4Mbps using 1:1	1.4Mbps initially; 5.8Mbps later	1.8Mbps	100Mbps peak layer 2 throughput using 802.11n
Bandwidth	3.5MHz and 7MHz in 3.5GHz band; 10MHz in 5.8GHz band	3.5MHz, 7MHz, 5MHz, 10MHz, and 8.75MHz initially	5MHz	1.25MHz	20MHz for 802.11a/g; 20/40MHz for 802.11n
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM	QPSK, 8 PSK, 16 QAM	BPSK, QPSK, 16 QAM, 64 QAM
Duplexing	TDD, FDD	TDD initially	FDD	FDD	TDD
Frequency	3.5GHz and 5.8GHz initially	2.3GHz, 2.5GHz, and 3.5GHz	800/900/1, 800/1,900/2,100MHz	800/900/1,800/1,900MHz	2.4GHz, 5GHz
Coverage	3–5 miles	< 2 miles	1–3 miles	1–3 miles	< 100 ft indoors; < 1000 ft outdoor
Mobility	Not applicable	Mid	High	High	Low

Now a days Major wireless service provider are already planning to roll out WiMAX, and is enabling mass market adoption of WiMAX in notebooks and other mobile Internet devices(MID) similar to the way it enabled Wi-Fi in notebooks. WiMAX is a global, standards-based technology that is being adopted and deployed in many countries around the world. For example, two carriers in the U.S., Sprint and Clearwire, will be deploying WiMAX services in 2008, and over 100 carriers are currently trialing Mobile WiMAX around the world

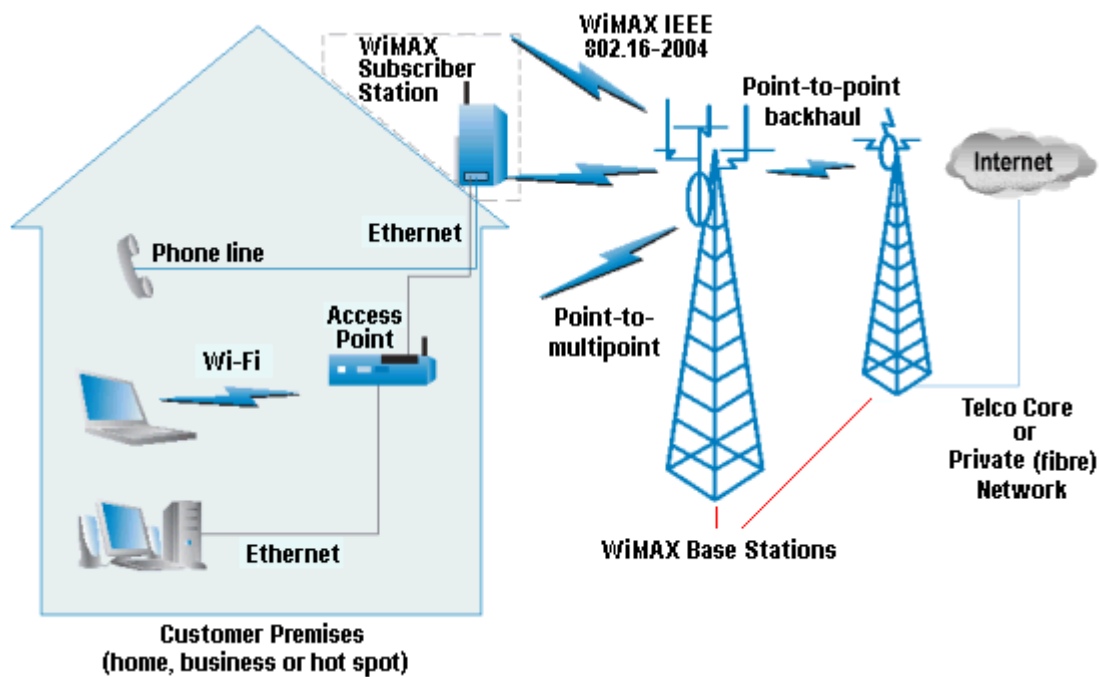


Fig 1.6: Overall WiMAX Structure

CHAPTER # 2

SIMULATION

2.1 Simulation plan:

In our thesis work we have implemented a WiMAX transmitter & receiver using MATLAB. Here we also connect a control system and a sensor to our transmitter for security purpose. Here is the whole scenario of our simulation.

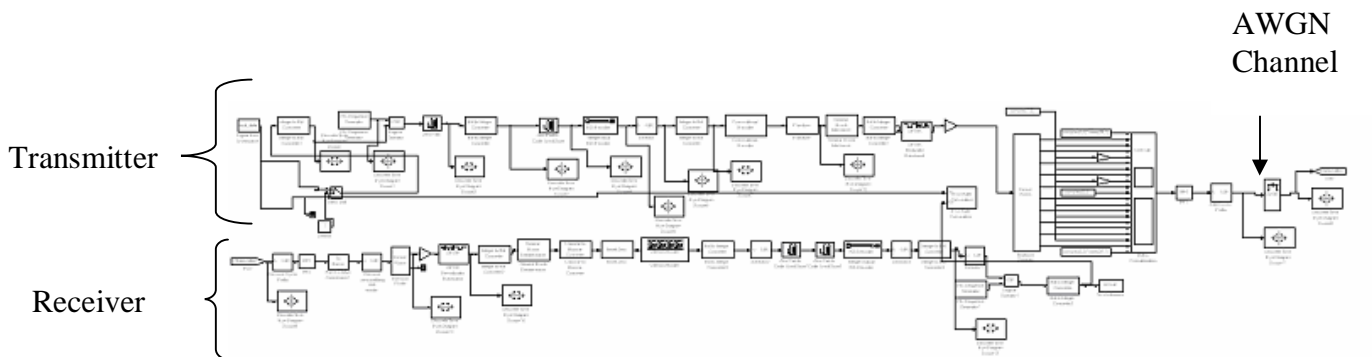


Fig 2.1: WiMAX Transmitter and Receiver with Sensor and Control Unit.

We have mainly design our Simulation by using SIMULINK in MATLAB. But a small code is needed for generate data and communication purpose.

Our Simulation has 2 major parts:

- ❑ MATLAB code
- ❑ SIMULINK implementation

2.2 MATLAB code:

Here we have write a MATAB code. The main purpose of the code is to generate a data array of 8 integers. Each of the integer represent code like area, country etc. Then the code generates “genpoly” and “primpoly” which are used in the part of PN sequence generator & Encoder for communication purpose.

2.3 SIMULINK implementation:

Our SIMULINK has 4 major parts. They are:

- Security
- Transmitter
- Channel
- Receiver

2.3.1 Security

For our home security purpose we have used here:

- Sensor
- Control Unit

Sensor

For sensor we have used here a constant block. It sends data (only 0 & 1) to the control unit. The control unit then takes decision whether it will send signal to receiver or not.

Control Unit

For control unit we have used here switch block. It decides whether the signal is send to the receiver or not. When the sensor is activate then it sends signal to the receiver. Else no signal sends to the receiver.

2.3.2 Transmitter:

The transmitter is using to transmit the data. It is use some process to transmit the data. Firstly the logical operation (XOR) between data and PN sequence is occurs. Then encode the data by using Reed Solomon encoder, convolutional encoder and the puncturing process. This are used for noise less transmission of data. Then the data is passing through the modulator. Here we have used QPSK (Quadrature Phase Shift Keying) modulator. It is very efficient and commonly used modulator for digital transmission. Then the signal is converted to the OFDM symbol. Then pass through the channel.

The WiMAX transmitter has some Major components. They are:

- Source
- Randomizer
- Encoder
- Modulation
- OFDM symbol
- IFFT
- Add cyclic prefix
- Transmitter antenna

Source:

In source block we have use a just use an input data from workspace block. It just read data from the workspace. After running the code, a set of integer is generating. Then the source read the data from the workspace. Then plot the data.

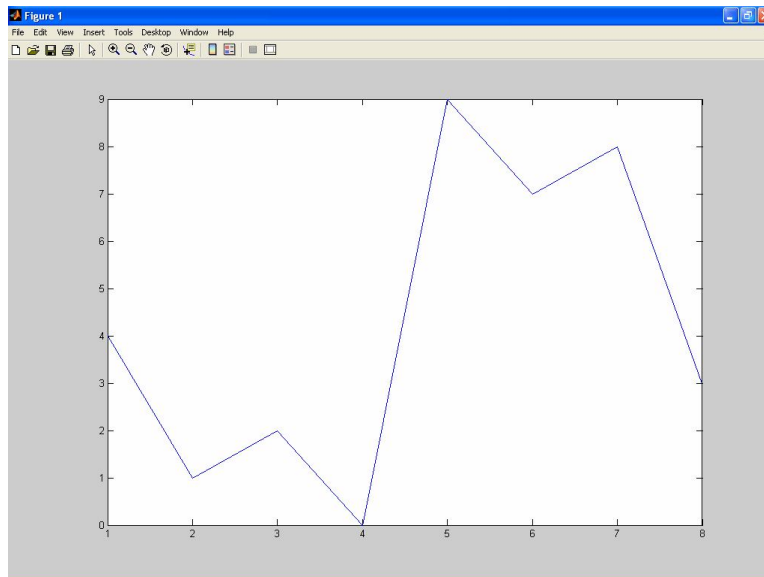


Fig 2.2: Input / Source data

Randomizer:

The randomizer is used to operate logical operation between PN sequence and the main data. It is used to identify easily for the receiver. Here we have use a PN sequence generator to generate a PN sequence. Then we have use a logical block which operates logical operation between data and PN sequence. Here we can see the eye diagram of randomizer.

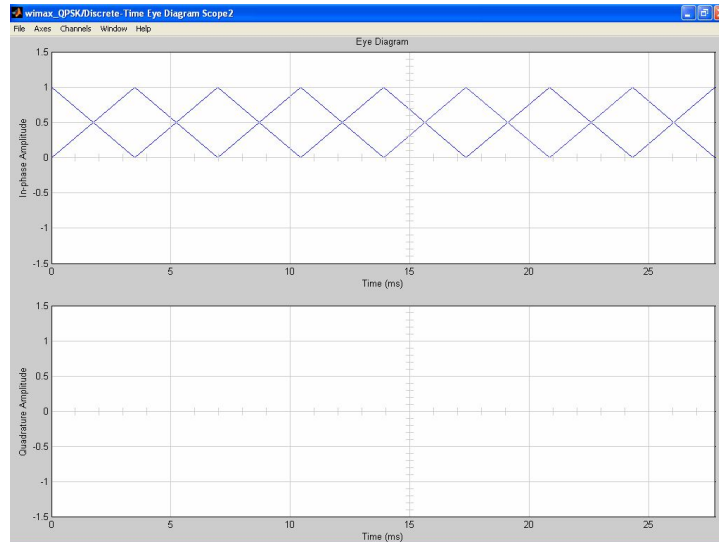


Fig 2.3: Eye diagram of randomizing data.

Encoder:

After randomizing the signal we have passed our signal through the encoding process. Encoding is used for distortion less transmission of signal. It is very important part for transmission of signal. Here we can see the how the encoding process is occur by block diagram.

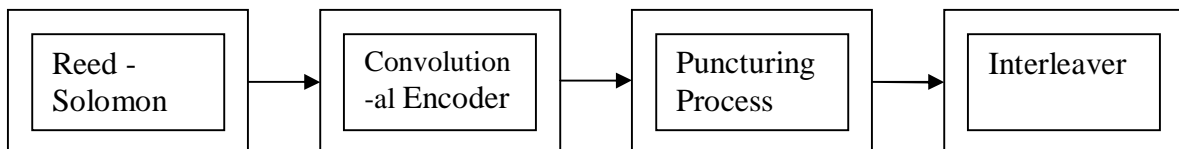


Fig 2.4: Block diagram of Encoding Process [1]

In our transmitter part we have used mainly 2 types of encoding technique. The encoding is described here.

Reed-Solomon Encoder:

The Reed-Solomon encoding is mainly used to recover the main signal if it is distorted. The properties of Reed-Solomon codes make them suitable to applications, where errors occur in bursts. Reed-Solomon error correction is a coding scheme which works by first constructing a polynomial from the data symbols to be transmitted, and then sending an over sampled version of the polynomial instead of the original symbols themselves. A Reed-Solomon code is specified as RS (n, k, t) with l-bit symbols. This means that the encoder takes k data symbols of l bits each and adds 2t parity symbols to construct an n-symbol codeword. Thus, n, k and t can be defined as:

- n: number of bytes after encoding,
- k: number of data bytes before encoding,
- t: number of data bytes that can be corrected.

The error correction ability of any RS code is determined by (n – k), the measure of redundancy in the block. If the location of the erroneous symbols is not known in advance, then a Reed-Solomon code can correct up to t symbols, where t can be expressed as $t = (n - k)/2$. Here we have used n=255, k=239 and t=8 because this values are standard [1].

The Reed-Solomon Encoder is mainly work with integer values. So here we have first convert the bit into integer format using bit to integer converter then reorder the vector using zero padding then operate RS encoding process Then we have use a selector to select the data from our vector then convert it to the bit format again using integer to bit converter block [1].

Convolutional Encoder:

The purpose of a convolutional encoder is to take a single or multi-bit input and generate a matrix of encoded outputs. One reason why this is important is that in digital modulation communications systems (such as wireless communication systems, etc.) noise and other external factors can alter bit sequences. By adding additional bits we make bit error checking more successful and allow for more accurate transfers. By transmitting a greater number of bits than the original signal we introduce a certain redundancy that can be used to determine the original signal in the presence of an error [3].

After the RS encoding process, the data bits are further encoded by a binary convolutional encoder. It converts the single or multi bit into matrix form. It is use

to discard noise from the main signal. It is another process of error correction. It deals with bit data. It is work using poly2trellis function.

The generator polynomials used to derive its two output code bits, denoted X and Y, are specified in the following expressions:

$$G1 = 171_{\text{oct}} \text{ for } X$$

$$G2 = 133_{\text{oct}} \text{ for } Y$$

A convolutional encoder accepts messages of length k_0 bits and generates codewords of n_0 bits. Generally, it is made up of a shift register of L segments, where L denotes the constraint length. The binary convolutional encoder that implements the described code is shown in figure. A connection line from the shift register feeding into the adder means a "one" in the octal representation of the polynomials, and no connection is represented by a "zero" [1].

We have used here a convolutional encoder block for convolutional encoding.

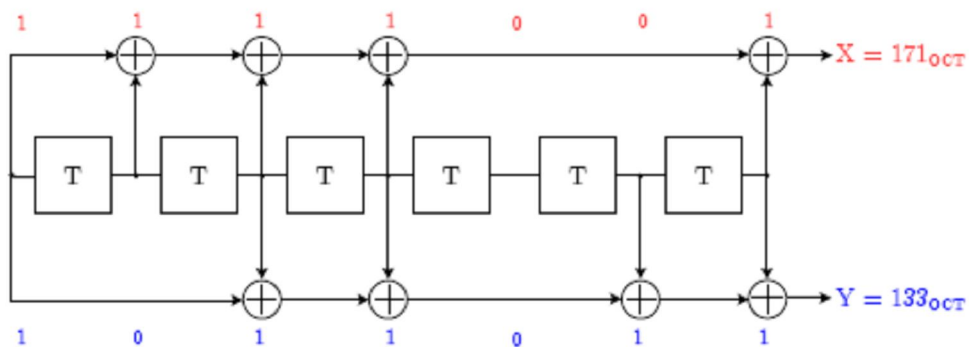


Fig 2.5: Convolutional Encoder of Binary rate $\frac{1}{2}$ [1]

Encoding consist two types of process for distortion less transmission of data. They are:

- ◆ Puncturing process
- ◆ Interleaver

Here is the description of those processes.

Puncturing Process:

Puncturing process is mainly used to convert a long bit stream data into short bit stream. It compress the long bit data. If we pass any balloon through a narrow pipe we have puncture it first then pass through then pump that again. Same process is applied here. It deals with binary bit stream.

Puncturing is the process of systematically deleting bits from the output stream of a low-rate encoder in order to reduce the amount of data to be transmitted, thus forming a high-rate code. The bits are deleted according to a perforation matrix, where a "zero" means a discarded bit. The process of puncturing is used to create the variable coding rates needed to provide various error protection levels to the users of the system. There are different types of puncturing process like as $\frac{1}{2}$ rate, $\frac{2}{3}$ rate, $\frac{3}{4}$ rate, $\frac{5}{6}$ rate. Here is the scenario of puncturing vector [1].

Table 2.1 Various rate of Puncturing Process [1]:

Rate	Puncturing Vector
$\frac{1}{2}$ rate	[1]
$\frac{2}{3}$ rate	[1 1 1 0]
$\frac{3}{4}$ rate	[1 1 0 1 1 0]
$\frac{5}{6}$ rate	[1 1 0 1 1 0 0 1 1 0]

Puncturing process and Convolutional encoding is directly support by SIMULINK in MATLAB.

Interleaver:

Interleaver is mainly used to correct burst error. After puncturing process the data is passed through the interleaver. The main purpose to use it to minimizing burst error. Interleaving is normally implemented by using a two-dimensional array buffer, such that the data enters the buffer in rows, which specify the number of interleaving levels, and then, it is read out in columns. The result is that a burst of errors in the channel after interleaving becomes in few scarcely spaced single symbol errors, which are more easily correctable [1].

WiMAX uses an interleaver that combines data using 12 interleaving levels. The effect of this process can be understood as a spreading of the bits of the different symbols, which are combined to get new symbols, with the same size but with rearranged bits [1].

The interleaver of the simulator has been implemented in two steps. First, data passes through a matrix interleaver which performs block interleaving by filling a

matrix with the input symbols row by row, and then sending this matrix content column by column. The parameters used for this block are the number of rows and columns that compose the matrix:

$$N_{\text{rows}} = 12, \quad N_{\text{columns}} = N_{\text{tcb}} / N_{\text{rows}}$$

Here the interleaving process uses a formula to do the job. That is:

$$I = \sum_{i=0}^{N_{\text{tcb}} - 1} (S * \text{floor}(i / S) + \text{mod}(i + N_{\text{tcb}} - \text{floor}(i N_{\text{rows}} / N_{\text{tcb}}), S) + 1)$$

Here:

- ◆ N_{tcb} is the total number of coded bits,

$$N_{\text{tcb}} = N_{\text{cpc}} * N_{\text{tx-data}}$$

- ◆ N_{cpc} is the number of coded bits per subcarrier, being the same as
- ◆ specified with the modulation alphabet, M_a ,
- ◆ $N_{\text{tx-data}}$ is the total number of transmitted data symbols, and
- ◆ $N_{\text{tx-data}} = N_{\text{dataNOFDM}}$
- ◆ $S = \text{ceil}(N_{\text{cpc}}/2)$

This formula is simulate by the code (data.m).It creates a variable 'int_idx' which is used in General block interleaver in SIMULINK.in this code we have use $N_{\text{cbps}} = 384$ & $N_{\text{cpc}} = 4$. Here we will see the eye diagram of the data after encoding [1].

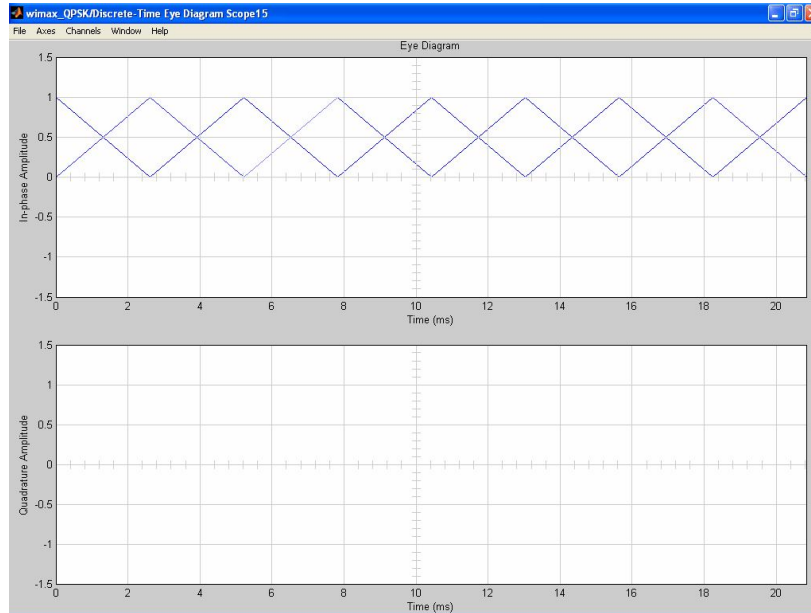


Fig 2.6: Eye diagram of the data after encoding.

The single line means there is no error in the data.

Modulation Technique:

There are several modulation technique can be implemented in WiMAX communication. Here we can use PAM, QAM, QPSK, BPSK etc. But the QPSK is very simple and easy to understand. Moreover it is the commonly used modulation technique in digital communication system. Here we have mainly used $\pi/4$ -QPSK. That's why we have used here a simple QPSK block to modulate the data. Here we have convert the bit into integer form then send it to the QPSK modulator block to modulate the signal. Here the data is modulated using the formula:

$$\exp(j\theta + j\pi m/2)$$

Where θ is the Phase offset parameter. In this case, the input can be either a scalar or a frame-based column vector [2].

The final variant of QPSK uses two identical constellations which are rotated by 45° ($\pi / 4$ radians, hence the name) with respect to one another. Usually, either the even or odd data bits are used to select points from one of the constellations or the other bits select points from the other constellation. This also reduces the phase-shifts from a maximum of 180° , but only to a maximum of 135° and so the amplitude fluctuations of $\pi / 4$ -QPSK are between OQPSK and non-offset

QPSK. Then we have use a gain block to take the r.m.s value of the signal. We have calculated it using [2]:

$$E_{r.m.s} = (1/\sqrt{2}) * E$$

Here we will see the eye diagram of the signal after modulation and then the eye diagram of r.m.s value of the signal.

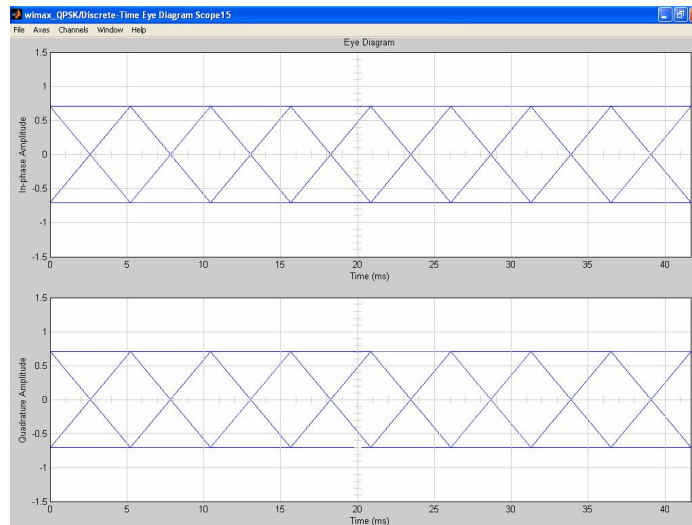


Fig 2.7: After modulating the signal

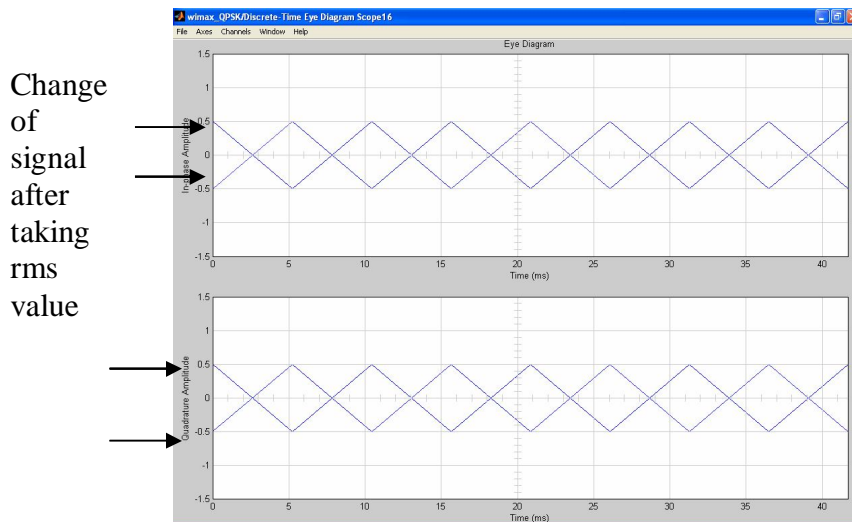


Fig 2.8: After take the r.m.s value of the signal

Here we can see that after modulation the eye diagram shows two types of amplitude because after modulation two types of amplitude is generated they are in phase & quadrature amplitude. In this eye diagram we can see that there is no error in the signal because there is single blue line in the data not multiple lines.

OFDM Symbol:

WiMAX OFDM symbol have 256 sub carriers. There are 3 types of sub carriers are used here. They are data, training, pilot and dc sub carrier. 200 of the total 256 sub carriers are used for data and pilot sub carriers, eight of which are pilots permanently spaced throughout the OFDM spectrum. The remaining 192 active carriers take up the data sub carriers. Here is a scenario of an OFDM symbol [1].

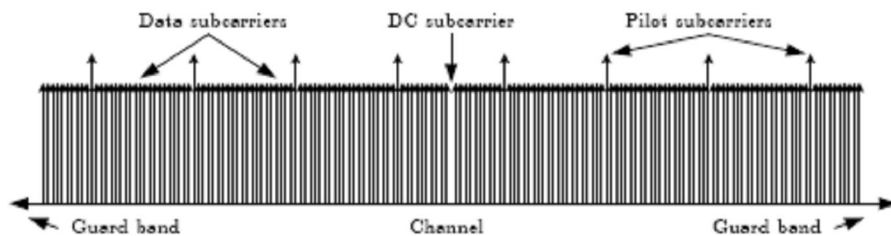


Fig 2.9: OFDM symbol

Now we have to convert our data into OFDM symbol. For this reason we have to take the data as row format then add pilot signal and training signal with our data then use a vertical concatenation to make an OFDM symbol consists of data, pilot signal and training sequence and guard band.. The major parts of the OFDM symbol are:

- ◆ Training sub carrier
- ◆ Pilot sub carrier
- ◆ Guard band

Here we have generated the Training and pilot sub carriers using constant block here we have used complex function to generate complex training and pilot signal. We have use complex function because of after modulation our data transform into complex form. The main purpose of training to generate guard band we have create a complex null vector. The main purpose to use guard band to prevent inter symbol interference (ISI). Then we have used a Matrix concatenation as an assembler. It is used to create an OFDM symbol and put the

Sub carrier into that sequentially. Here we have set the matrix concatenation into vertical catenation format as our data in OFDM symbol is in vertical form. The symbol is look like following figure after assembling [1].

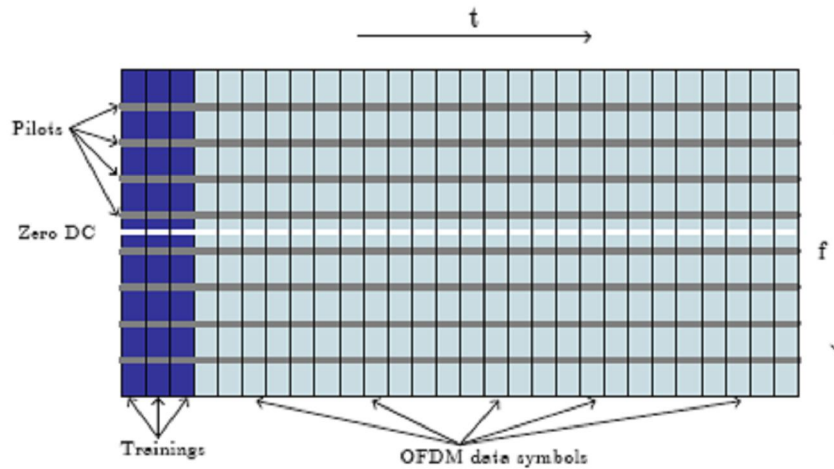


Fig 2.10: OFDM burst structure obtained after assembling [1].

Now we will see the eye diagram of our signal after converting it as OFDM symbol.

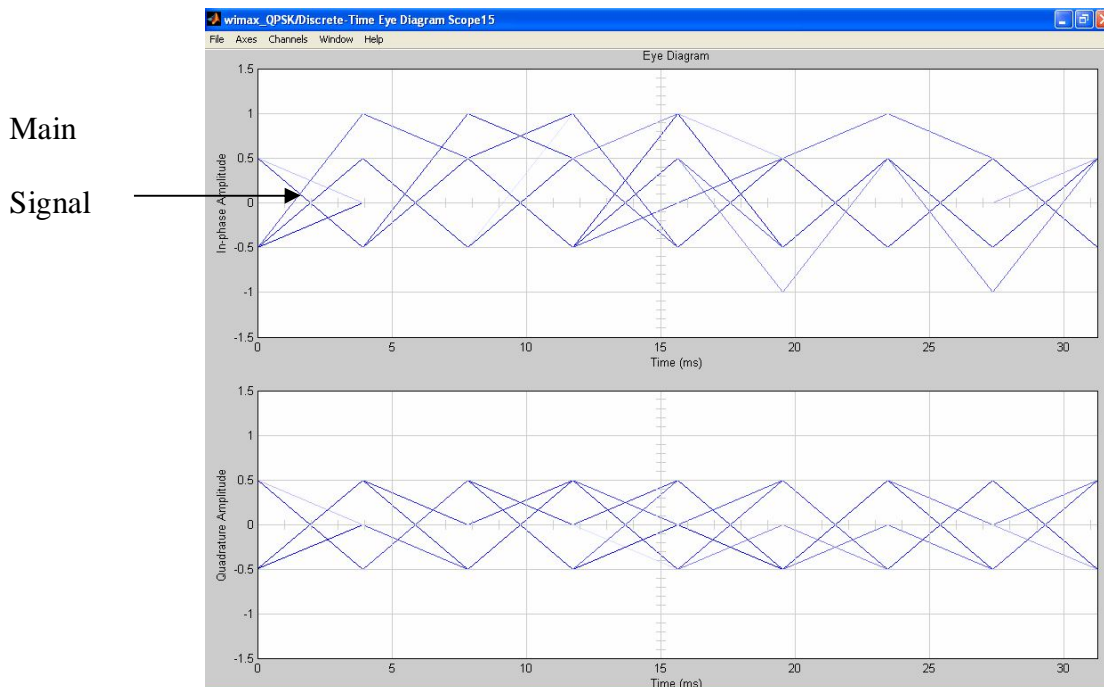


Fig 2.11: Eye diagram of OFDM symbol

Here we can see that there is no error in main signal because of single blue line.

Inverse Fast Fourier Transformation:

The IFFT is used to produce a time domain signal, as the symbols obtained after modulation can be considered the amplitudes of a certain range of sinusoids. This means that each of the discrete samples before applying the IFFT algorithm corresponds to an individual sub carrier. Besides ensuring the orthogonality of the OFDM sub carriers, the IFFT represents also a rapid way for modulating these sub carriers in parallel, and thus, the use of multiple modulators and demodulators, which spend a lot of time and resources to perform this operation, is avoided [1].

Furthermore, the FFT (or IFFT) should be of length $2r$ (where r is an integer number) to facilitate the realization of the algorithm. For this reason, the FFT length is given by

$$N_{\text{FFT}} = 2^{\lceil \log(N_{\text{data}}) \rceil}$$

Here is the scenario of OFDM block before the IFFT[1].

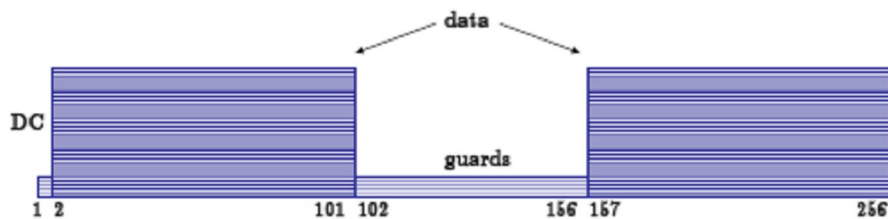


Fig 2.12: Rearrangement performed before realizing the IFFT operation [1]

Here we have used IFFT block to do the job. Here we can see the eye diagram after doing the IFFT .

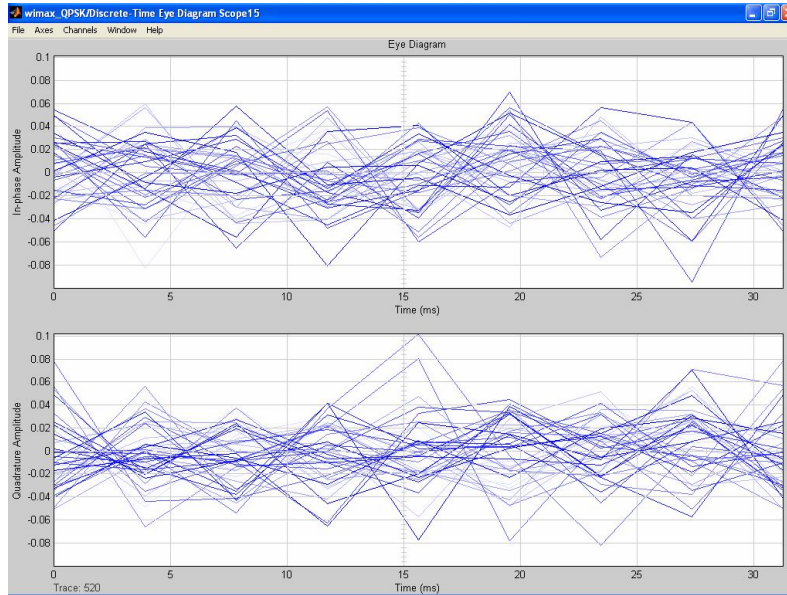


Fig 2.13: Eye diagram after performing IFFT

Add Cyclic Prefix:

The robustness of any OFDM transmission against multipath delay spread is achieved by having a long symbol period with the purpose of minimizing the inter-symbol interference. This ISI is a great drawback of digital communication system. To avoid this problem we have used cyclic prefix in our WiMAX communication. Here we have used the guard band cyclically in the long period of symbol to avoid ISI. This guard interval, that is actually a copy of the last portion of the data symbol, is known as the cyclic prefix (CP) [1].

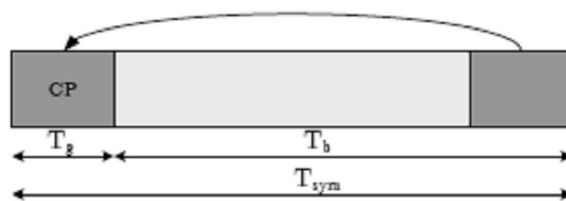


Fig 2.14: OFDM symbol with the cyclic prefix

Copying the end of a symbol and appending it to the start results in a longer symbol time. Thus, the total length of the symbol is

$$T_{sym} = T_b + T_g$$

Where:

- T_{sym} is the OFDM symbol time
- T_b is the useful symbol time, and
- T_g represents the CP time.

Here we have used a selector to add cyclic prefix with the data. Here we have use vector as input and define one based index to initialize the vector from one. We also the select the input port width as 256 as it deal with 256 bit and select the elements to use cyclic prefix into the data. Here is the eye diagram of transmitted data after adding cyclic prefix [1].

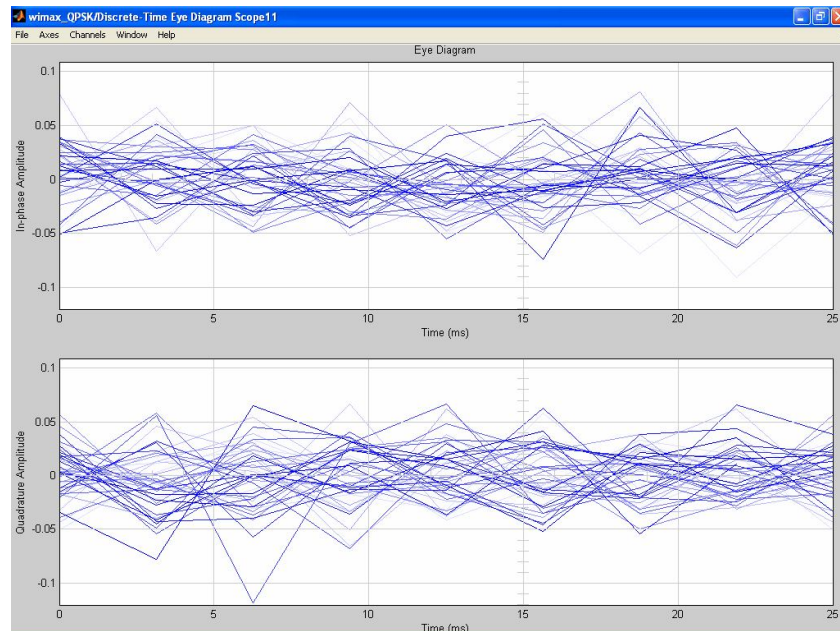


Fig 2.15: Data after adding cyclic prefix

Here we can see that there is no difference between the eye diagram of IFFT and adding cp. The eye diagram is so congested and the difference is not understood clearly in eye diagram.

Transmitter Antenna:

Here we have used a go to block to transmit the antenna to the receiver. Here the signal is same as the signal after adding cyclic prefix.

2.3.3 Channel:

Here we have passed our transmitted signal through a channel. Here we have mainly used additive white Gaussian noise channel. In communications, the additive white Gaussian noise (AWGN) channel model is one in which the only impairment is the linear addition of wideband or white noise with a constant spectral density (expressed as watts per hertz of bandwidth) and a Gaussian distribution of amplitude. The model does not account for the phenomena of fading, frequency selectivity, interference, nonlinearity or dispersion. However, it produces simple, tractable mathematical models which are useful for gaining insight into the underlying behavior of a system before these other phenomena are considered [2].

Wideband Gaussian noise comes from many natural sources, such as the thermal vibrations of atoms in antennas (referred to as thermal noise or Johnson-Nyquist noise), shot noise, black body radiation from the earth and other warm objects, and from celestial sources such as the sun [2].

The AWGN channel is a good model for many satellite and deep space communication links. It is not a good model for most terrestrial links because of multipath, terrain blocking, interference, etc. However for terrestrial path modeling, AWGN is commonly used to simulate background noise of the channel under study, in addition to multipath, terrain blocking, interference, ground clutter and self interference that modern radio systems encounter in terrestrial operation.

This is the commonly used channel in communication.

Why AWGN channel instead of Rician Fading Channel?

Our WiMAX network is based on line of sight (LOS) propagation. So simulation supports 2 types of channel. They are -

- ◆ AWGN channel
- ◆ Rician Fading channel

But here we have used AWGN channel because it is the commonly used channel in wireless communication. On the other hand in Rician Fading channel the signal is distorted. And when no signal is transmitted a huge garbage value is received by the receiver as a result the signal is totally changed. Here we can see the output curve of two different channels for no input.

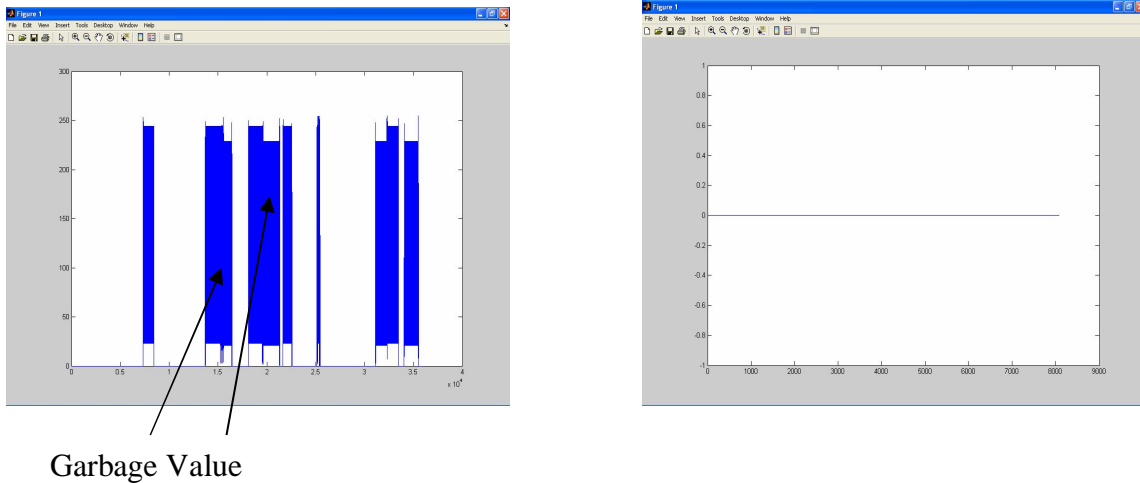


Fig 2.16: Output curve for Rician Fading Channel & AWGN Channel

For AWGN channel the error rate is almost 0 but in case of Rician Fading channel it is almost 0.8 which is so high for digital communication. For this reasons AWGN is used here.

2.3.4 Receiver:

Receiver is grabbing the transmitted signal which is come through the channel. The receiver is mainly reverse of transmitter. It consists of some important part. They are -

- Receiver antenna
- Remove cyclic prefix
- FFT
- OFDM data
- Demodulator
- Decoding
- Derandomizer
- Output

These parts are used for processing the transmitted signal and then recover the main signal from that. Now we will see how they work.

Receiver Antenna:

Receiver antenna is used to receive the transmitted data from the channel. Here we have used a “From” block which grab data from the transmitter. Hence it is an ideal case so the received signal is same as transmitted signal.

Remove Cyclic Prefix:

Remove cyclic prefix is the same as Add cyclic prefix. Here we have used a selector to add cyclic prefix with the data. Here we have use vector as input and define one based index to initialize the vector from one. It works same as Add cyclic prefix. Here is the eye diagram of the received signal after removing cyclic prefix [1].

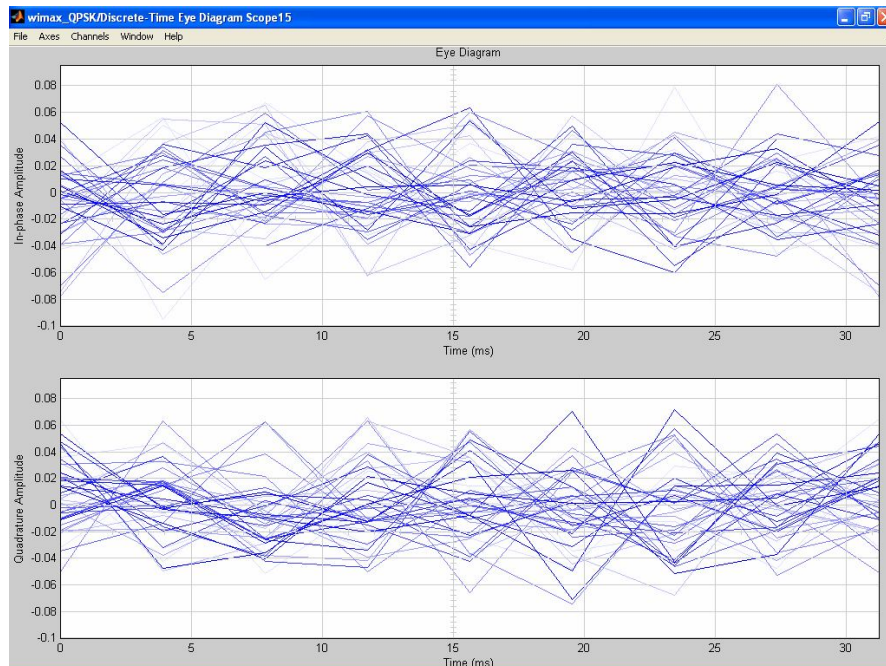


Fig 2.17: Eye diagram of the received signal after removing cyclic prefix.

Fast Fourier Transform:

The IFFT algorithm represents a rapid way for modulating a group of sub carriers in parallel. Either the FFT or the IFFT are a linear pair of processes, therefore the FFT is necessary to convert the signal again to the frequency domain. It's needed because the decoding processes are work on frequency domain based signal. It is same as IFFT. The details of FFT are discussed in IFFT part [1].

Demodulator:

Demodulator is the same as modulator. Here we have used QPSK modulation technique. So in receiver part to demodulate the data we have used QPSK demodulator to demodulate the data. It is the same as modulator but it's the reverse process of modulation. Here is the eye diagram of the signal after demodulation.

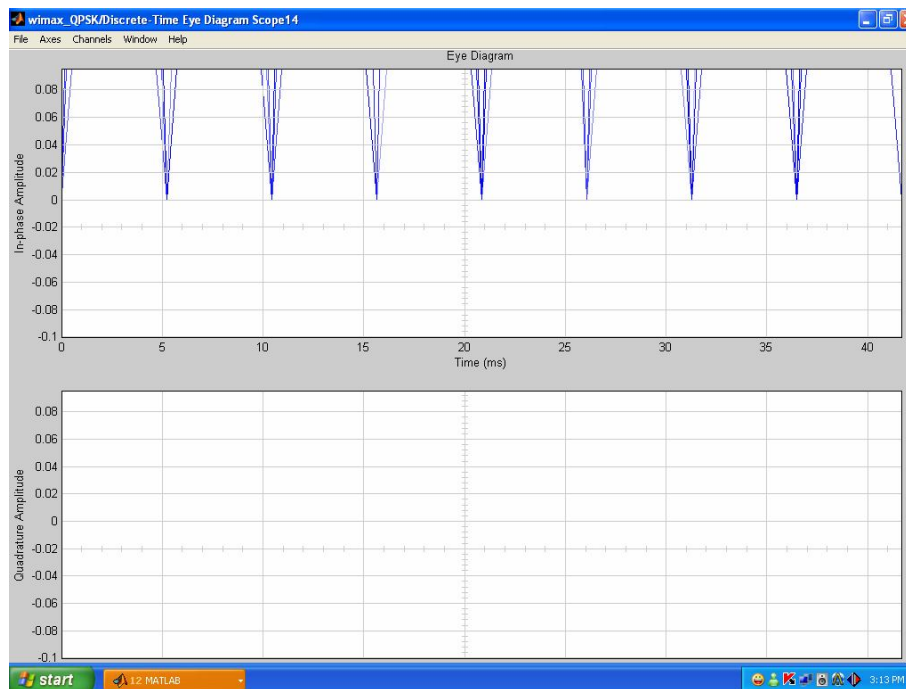


Fig 2.18: received signal after demodulation

Decoding:

After demodulating the signal we have to decode the signal. Then we have to decode the signal to recover the main signal from the demodulated signal.

We have to pass through some step. They are –

- Deinterleaver
- Inserting zero
- Viterbi Decoder
- Reed Solomon decoder

Here is the block diagram of decoding process.

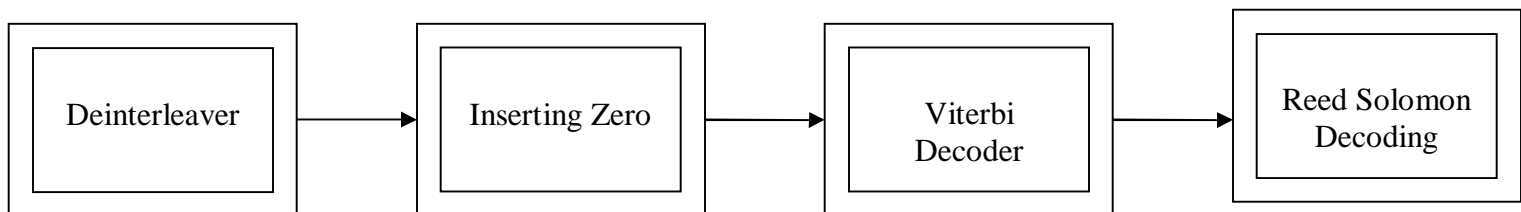


Fig 2.19: Block diagram of decoding [1]

Deinterleaver:

Deinterleaver is the reverse process of interleaver. After the demodulation the signal is passes through the deinterleaver. It consists of two blocks, a general block deinterleaver and a matrix deinterleaver. These blocks work similarly as the ones used in the interleaver. The general block deinterleaver rearranges the elements of its input according to an index vector. The matrix deinterleaver performs block deinterleaving by filling a matrix with the input symbols column by column, and then, sending its contents to the output row by row. The parameters

used in both blocks are the same as those ones used in the interleaving process. This matrix deinterleaving process is done by the code [1].

Inserting Zero:

The block named "Insert Zeros" deals with the task of reversing the process performed by the "Puncture" block. The receiver does not know the value of the deleted bits but it can know their position from the puncturing vectors. Thus, zeros are used to fill the corresponding hollow of the stream in order to get the same code rate as before performing the puncturing process.

The inserted zeros can also be seen as erasures from the channel. They have no influence on the metric calculation of the succeeding Viterbi decoder described in the following section [1].

Viterbi Decoder:

The Viterbi Algorithm (named after Andrew Viterbi) is a dynamic algorithm that uses certain path metrics to compute the 'most likely' path of a transmitted sequence. From this 'most likely' path, certain bit errors can be corrected to decode the original bit sequence after it has been sent down a communicative line. An important feature of the Viterbi algorithm is that ties are arbitrarily solved (can be picked randomly) and still yield an original sequence. What the Viterbi algorithm can do is correctly replicate your input string at the output even in the presence of one or more errors. Obviously, with more errors introduced the likelihood of a successful decryption does go down. But the algorithm has proved to be effective [3].

The main purpose of Viterbi decoder is to decode the convolutional encoded data. The Viterbi algorithm reduces the computational load by taking advantage of the special structure of the trellis code. Another advantage is its complexity, which is not a function of the number of symbols that compose the codeword sequence. The Viterbi algorithm performs approximate maximum likelihood decoding. It involves calculating a measure of similarity or distance between the received signal at time t_i , and all the trellis paths entering each state at the same time.

The algorithm works by removing those trellis paths from consideration that could not possibly be candidates for the maximum likelihood choice. When two paths enter the same state, the one that has the best metric is chosen as the "surviving" path. The selection of the different "surviving" paths is performed for all the states. The decoder continues in this way to advance deeper into the trellis making decisions by eliminating the least likely paths. The early rejection of unlikely paths is the fact that reduces the complexity. The goal of selecting the

optimum path can be expressed equivalently as choosing the codeword with the maximum likelihood metric, or as choosing the codeword with the minimum distance metric [1].

The Viterbi decoder block has 3 parameters to do the decoding. They are decision type, operation mode and trace back depth.

- ◆ As the decision process has been implemented in the demapper, the last kind of decision type, that is the "unquantized", is the one used in our simulator. It accepts real numbers as inputs for the decoder block. The positive numbers are interpreted as a logical zero, and the negative ones, as a logical one [1].
- ◆ The operation mode parameter controls which method the block uses for transitioning between successive frames. The "truncated" mode, in which each frame is treated independently and the trace back depth parameter starts at the state with the best metric and ends in the all-zeros state, is the operation mode used in the simulator [1].
- ◆ Here we have use the trace back depth as 8 because every data is consist of 8 bit [1].

Reed-Solomon Decoder:

The last part of the decoding process is the Reed-Solomon decoding. It performs the necessary operations to decode the signal, and get, at the end, the original message sent by the source. Thus, the RS decoder takes code words of length n , and, after decoding the signal, it returns messages of length k , being $n = 255$ and $k = 239$, the same as the ones described in the RS encoder.

The Reed-Solomon decoder is works with integer. So after Viterbi decoder we have to convert the data into integer form then operate the Reed-Solomon decoding process. The Reed-Solomon decoding process is same as Reed-Solomon encoding process. This was discussed before. After that we have use selector to select the rows then we have reorder the vector and then convert the data into bit format. Here is the eye diagram of the received signal after decoding and reorder the vector [1].

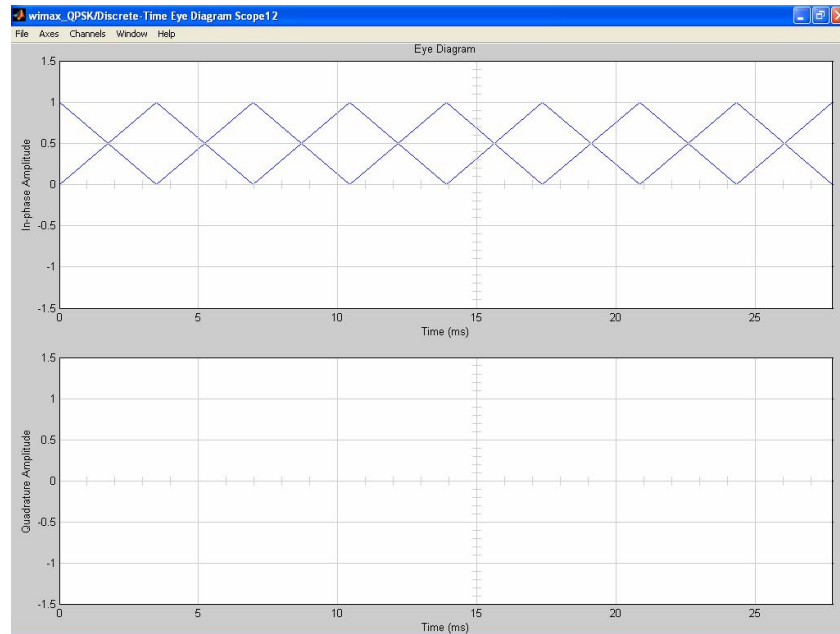


Fig 2.20: received signal after Decoding & Reorder

Here we can see that the eye diagram is same as the data of transmitter part before encoding. So we can see that we can decode the encoded data successfully.

Derandomizer:

Derandomizer is the same as randomizer. The decoding data is same as the data after randomizer. We have use the same PN sequence generator as randomizer which produces a PN sequence. Now we operate a logical operation same as randomizer (XOR). Then we get the main transmitted data which was transfer by the transmitter.

Output:

Now we have got the transmitted data and then store it to the workspace using “simout” block. Then plot the data.

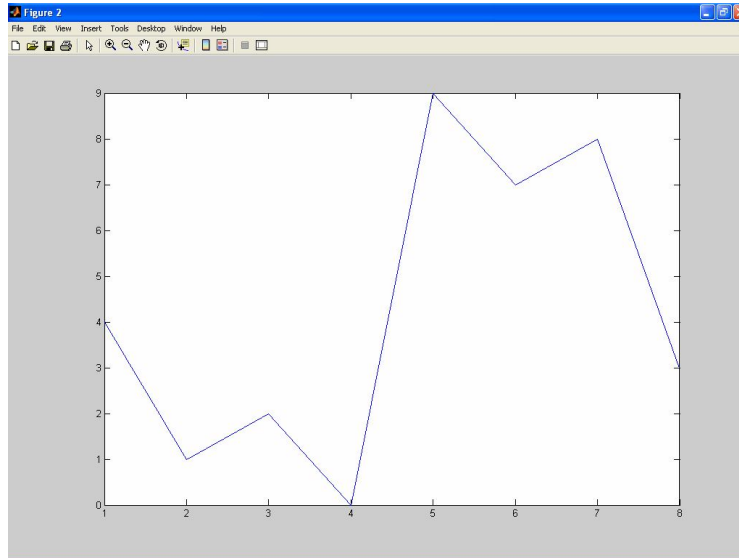


Fig 2.21: Output data

2.4 Result Analysis:

When the sensor is active then the control unit sends an integer data array from the transmitter to receiver. Then receiver receives the signal and recovers the main data after some process. Here we can see the graphical representation of input and output data.

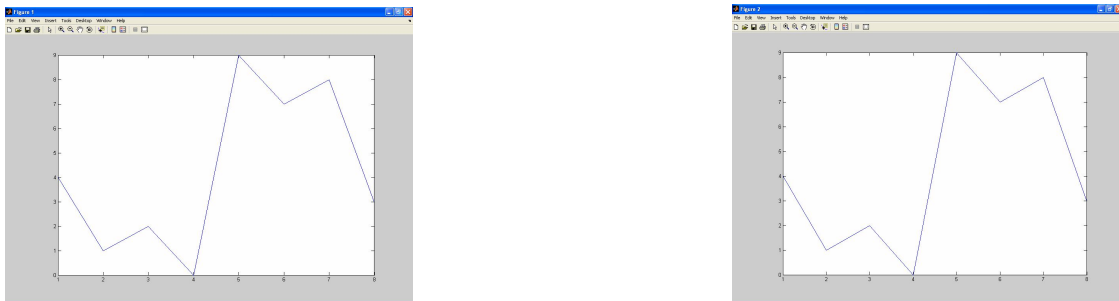


Fig 2.22: Graph of input and output data

Here we have used an Error rate calculation block which compares the input and output data and creates a vector named "ErrorVec" in workspace. The first element of it represents the Error rate; the second element is how many elements

and the third one is total compared element. Here we get the values of ErrorVec are:

Error rate = 0

Error elements = 0

If we plot the error rate from the ErrorVec the graph will be:

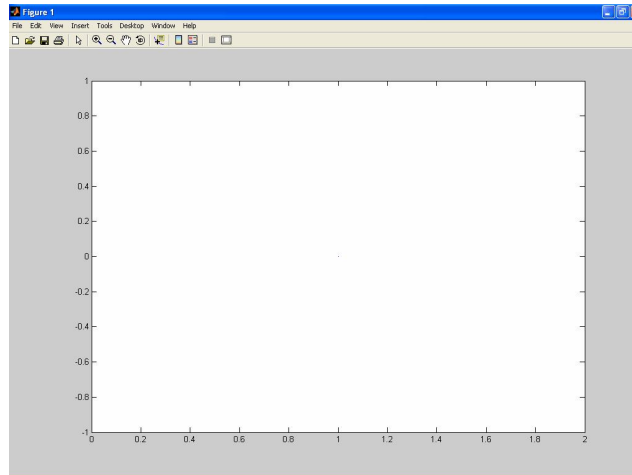


Fig 2.23: Graph of Error rate

So it represents that there is no error in the output data. If we see the graph of input and output curve we can see the both are almost same.

Chapter # 3

3.1 THE SYSTEM STRUCTURE:

Here a total communication scenario of that how WiMAX network work in our thesis project. Here we can see that the home or offices are connected with police station by WiMAX network.

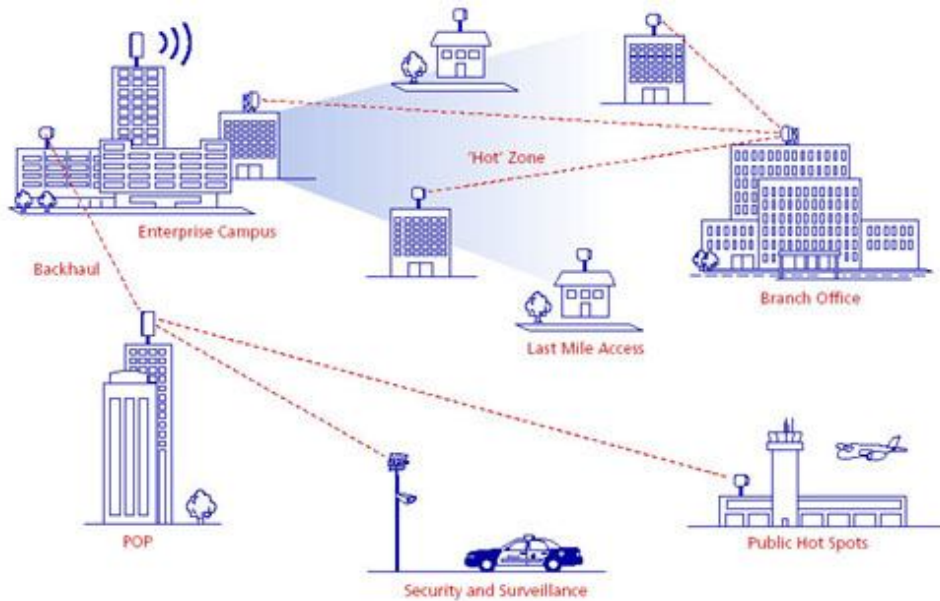


Fig 3.1: The scenario of the WiMAX system [4]

THEORY:

The main objective of our thesis is to create a wireless security system based on WiMAX technology. In our hardware setup we have constructed a security system where user enters his/her home entering own code or password. When password matches then the door is unlocked. If user inserts wrong code, a faded signal is sent to the receiver of the door lock as well as the police station and the door remain closed. When faded signal is sent more than once then the alarm system activates and police detect the location and take action.

3.2 SECURITY SYSTEM BASED ON WiMAX:

Our objective was to create a security system based on WiMAX technology. Since the components of WiMAX technology are too much expensive and not available we have constructed our security system based on RF signal for communication instead of WiMAX technology. For security system we have used a door lock system and window alarm system. These parts are described below-

Communication part

- Transmitter
- Receiver

Security part-

- Door lock system
- Window lock system

3.2.1 TRANSMITTER:

We have used 9v RF transmitter to transmit our signal to the all-receiving point. The gain of this transmitter can be higher using amplifier. Component count has been reduced however the power has been increased using a 9V battery. A bigger tuning film capacitor has been used to get more fine tuning anywhere in the FM band. It has a greater range, which is mainly the result of its higher operating voltage [5].

Equipments:

Resistors (carbon, 0.25W, 5%):		
100R (brown, black, brown)	R5	1
1K (brown, black, red)	R4	1
12K (brown, red, orange)	R1 R2	2
2M2 (red, red, green)	R3	1
BC338 transistor	T2	1
BC548 transistor	T1	1
9V Battery snap		1
10pF ceramic capacitor	C3 C4	2
4n7 ceramic capacitor	C1 C2	2
22n 223 ceramic	C6	1
trimmer capacitor 2-30pF	C5	1
K18 or K128 PCB (both are the same)		1
Hookup wire for aerial	160cm	

Circuit setup:

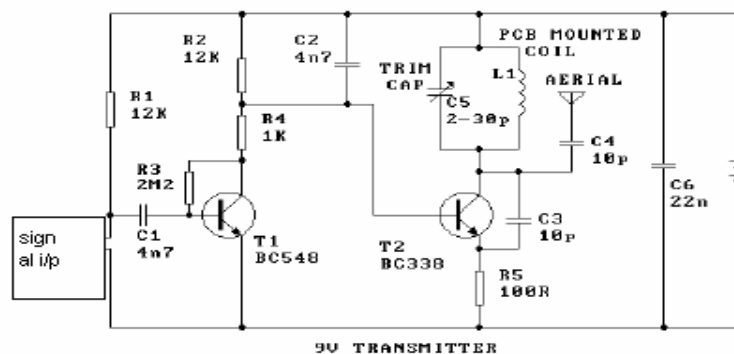


Fig: 3.2 Fm Transmitter [5]

Hardware setup:

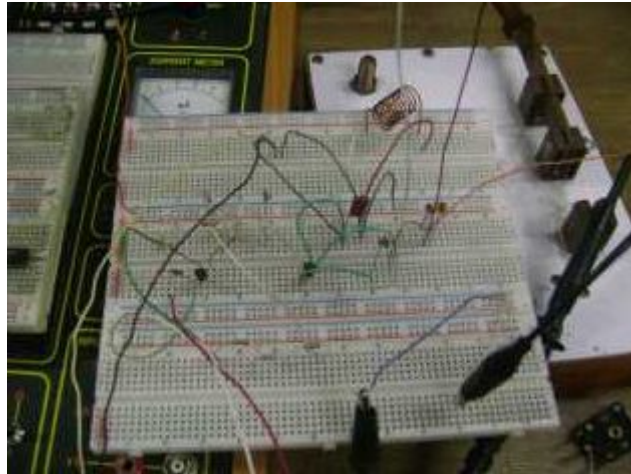


Fig: 3.3 Hardware implementation of Transmitter

Circuit description:

The circuit is basically a radio frequency (RF) oscillator that operates around 100 MHz (100 million cycles per second). Signal picked up and amplified by the signal generator is fed into the signal amplifier stage built around the first transistor. Output from the collector is fed into the base of the second transistor where it modulates the resonant frequency of the tank circuit (the coil built into the circuit board and the trim cap) by varying the junction capacitance of the transistor. Junction capacitance is a function of the potential difference applied to the base of the transistor.

First amplification stage:

This is a standard self-biasing common emitter amplifier. The 4n7 capacitor isolates the microphone from the base voltage of the transistor and only allows alternating current (AC) signals to pass.

The tank (LC) circuit:

Every transmitter needs an oscillator to generate the radio Frequency (RF) carrier waves. The tank (LC) circuit, the BC338 and the feedback 10pF capacitor are the (Colpitts). An input signal is not needed to sustain the oscillation. The feedback signal makes the base-emitter current of the transistor vary at the

resonant frequency. This causes the emitter-collector current to vary at the same frequency. This signal fed to the aerial and radiated

as radio waves. The 10pF coupling capacitor on the aerial is to minimize the effect of the aerial capacitance on the LC circuit. The name 'tank' circuit comes from the ability of the LC circuit to store energy for oscillations. In a pure LC circuit (one with no resistance) energy cannot be lost. (In an AC network only the resistive elements will dissipate electrical energy. The purely reactive elements, the C and the L simply store energy to be returned to the system later.) Note that the tank circuit does not oscillate just by having a DC potential put across it. Positive feedback must be provided

3.2.2 RECEIVER:

We have used simplest FM receiver for our signal reception. Since the range of this receiver is up to 400m we didn't use any amplifier here. The bandwidth of this receiver range is from 88 MHz to 108 MHz [6].

Equipments:

1. Variable capacitor (0-20pf)
2. Transistor (BF 199)
3. Resistor (12k)
4. Inductance (4 quirks, 4 mm internal diameter)
5. Dc Power supply
6. Oscilloscope
7. Wires

Circuit setup:

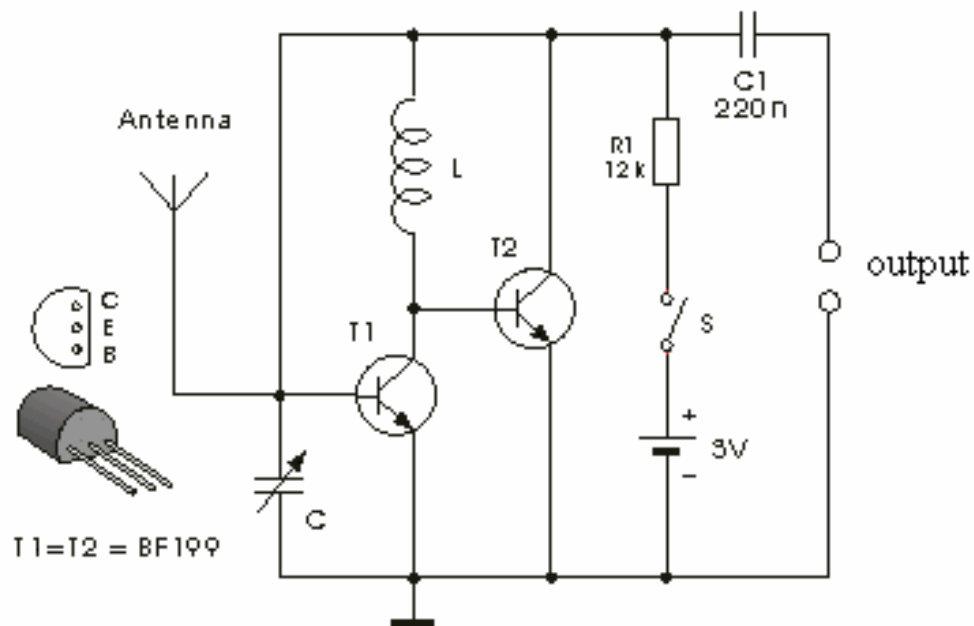


Fig: 3.4 FM Receiver [6]

Hardware setup:

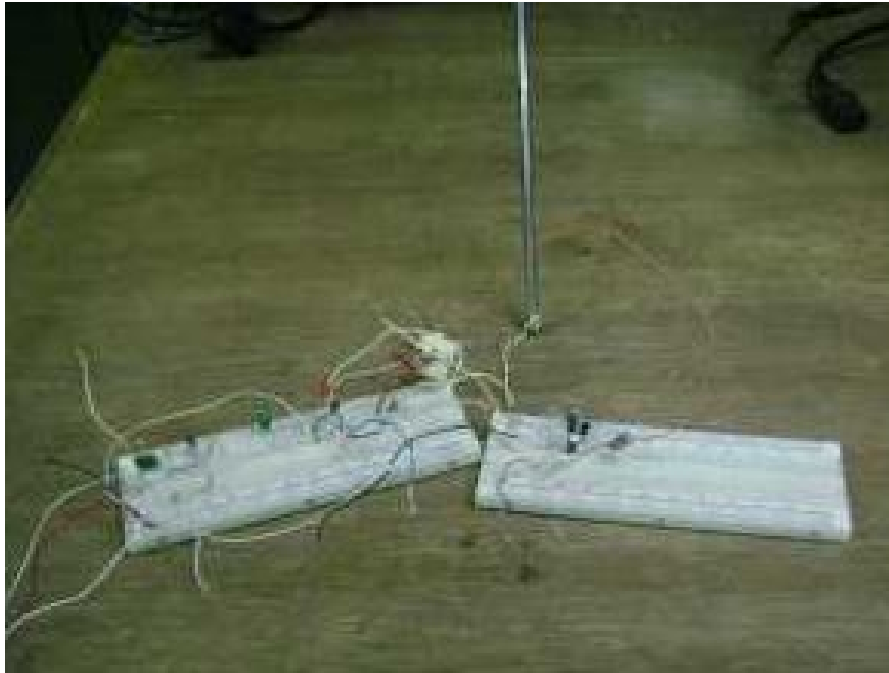


Fig: 3.5 Hardware implementation of Receiver

Circuit description:

The T2 transistor together with the R1 resistor, the coil L the variable capacitor C and internal capacitances of the T1 transistor, comprises the so-called Colpitts oscillator. The information being used in the transmitter to perform the modulation is extracted on the R1 resistor, and being led from it to the oscilloscope, over the coupling capacitor C1. The capacitance of the variable capacitor should be able to change from a couple of pF (Cmin) to app. 20 pF. The coil L has 4 quirks of lacquer-isolated copper wire (CuL), bended to have a 4 mm internal diameter. During the setup of the bandwidth, changing the distance between the quirks can alter the inductance of the coil. If the coil is stretched the inductance decreases, and vice versa. If this cannot give the desired results, new coil must be made. The telescopic antenna taken from a disused device can be used [6].

3.3.1 Door Security System

The door lock system is constructed using a very simple 2-bit comparator. Where we have used the logic of 2-bit magnitude comparator to design the digital lock system. The password given by the user is compared through this comparator [7].

Equipment:

1. AND Gate ()
2. OR Gate ()
3. NOT Gate ()

Circuit Diagram:

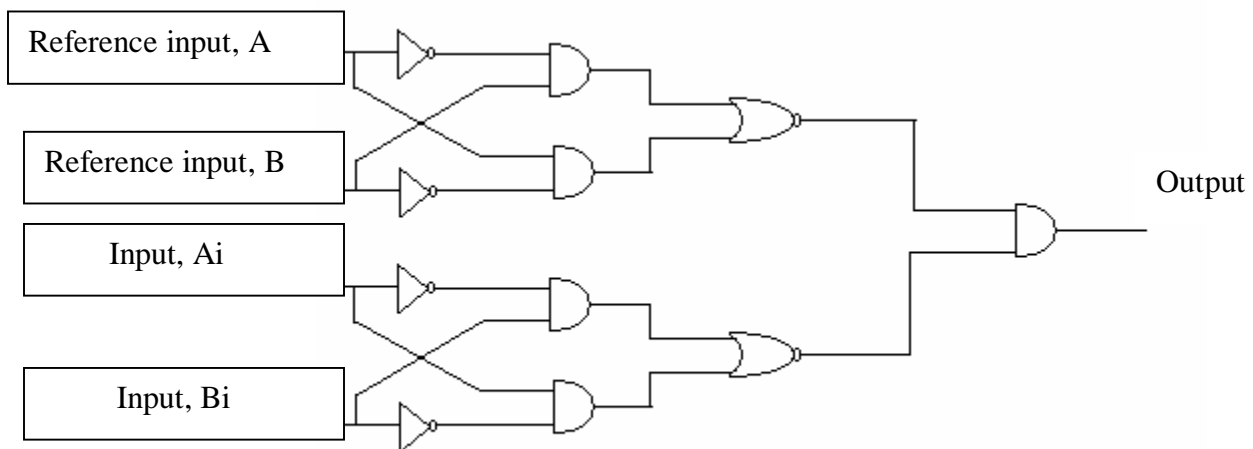


Fig: 3.6 Hardware implementation of Door security system [7]

Hardware setup:



Fig: 3.7 Hardware implementation of Door security system

Circuit Operation:

Consider two numbers A & B with two digits. So they can be represented as

$$A = A_1A_0$$

$$B = B_1B_0$$

Both numbers will be equal if all pairs of significant digits are equal. When the number is binary then the digits are either 0 or 1 and the equality of the pair of bits can be expressed by a function:

$$x_i = A_iB_i + A_i\bar{B}_i \quad \text{here } i = 0,1$$

x_i will be '1' when A & B will be same. So if we want to compare the whole part of both numbers we have AND x_0 and x_1 . Then the function will be expressed as:

$$(A=B) = x_1x_0$$

Here $A=B$ when $x_0=x_1$. This is the main logic, which is implemented here using logical gates. Here we have used NOT, AND & NOR.

Here we have used In1 and In2 as the password. Then we have used In3 and In4 as user input. When input matches with the set password then it sends logical '1' to the system then the door is unlocked and sends a signal to the receiver. Otherwise it sends Logical

'0' to the system so the door remains locked and send faded signal to the receiver. Here is the scenario of hardware of our door security, which we have implemented [7].

3.3.2 Window Alarm System:

We have used a very simple but effective alarming system. It is connected to the window. When any one illegally tries to open it then the alarming system is active at once and transmits the signal to the local server as well as neighbor's receiver.

Equipments:

1. Resistance, $R1=10k$
2. Capacitor , $C=1\mu f/12v$
3. 6v relay
4. Signal generator
5. power supply
6. One touch switch, S1
7. NPN Transistor, T1= SL 100.

Circuit Setup:

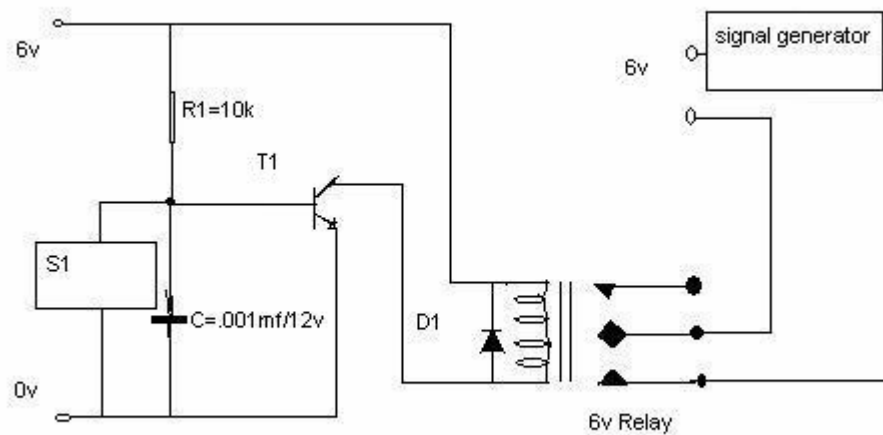


Fig: 3.8 Window alarm system

Hardware setup:



Fig: 3.9 Hardware implementation of window alarm system

Operation:

The switch S1 is always on. Thus current flows through resistance R1 and goes to the ground through switch. When anyone tries to open the window illegally the switch is turned off and the transistor triggers. The relay is activated as the transistor triggers and the signal generator generates the signal to send to the receiver.

3.4 Result analysis:

In this part the results are calculated and analyzed. When password matches with the reference one then a sharp signal is transmitted and at the receiving end a sharp but a bit distorted signal is received. But when the password does not matches then faded signal is transmitted and more faded signal is received at the reception.

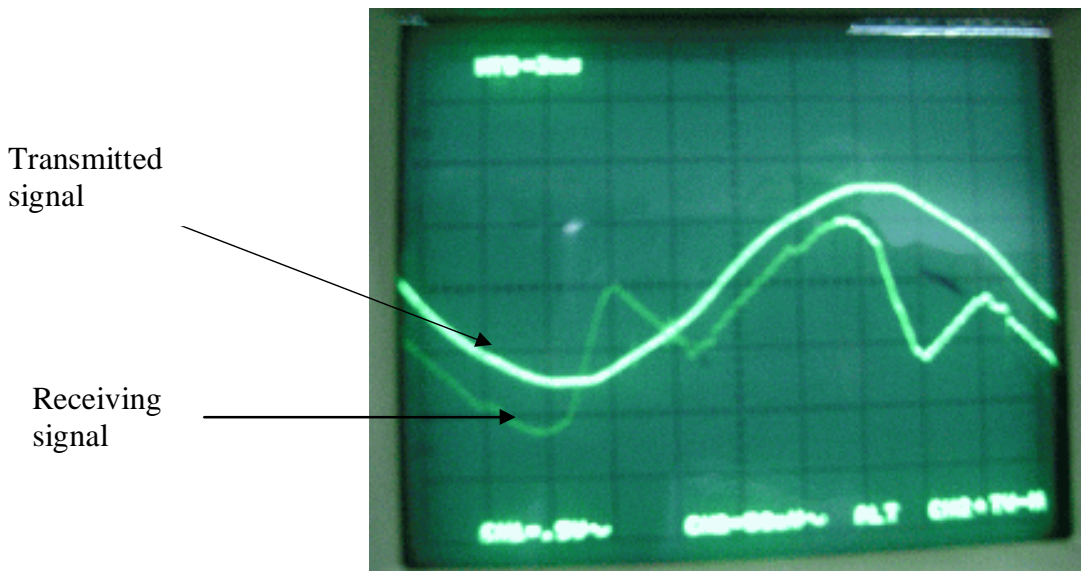


Fig: 3.10 Result analysis

Chapter # 4

FUTURE PLAN & CONCLUSION

We have some future plan. We will implement the following thing in future. They are –

- **Implemented MIMO transmission of Simulation:**

In future we will implement multiple inputs and multiple outputs with our main simulation of WiMAX security system. That will be more practical.

- **Introduce sensor & control unit to the hardware:**

We will introduce sensor for more security purpose and the whole system will be controlled by a control unit which can be a logical device or CPU.

- **Introduce Interfacing to the hardware:**

To make our hardware part more practical we can introduce hardware interfacing to our hardware part. Here the reference password is set from the bread board and the user enters the input password from pc. Then the door security system check whether the password matches or not.

- **Simulate network architecture of WiMAX with other networks like Wi-Fi, 3G mobile and RF etc:**

We have a plan to simulate our WiMAX network with other networks like Wi-Fi, 3G and RF etc. Those can be used as intermediate network of whole network architecture.

Conclusion:

WiMAX technology brought revolution in both fixed and mobile wireless communication. In present communication world, wireless communication does not mean only data and voice transmission. It also supports high data rate transmission which supports various types of service (voice, data, multimedia). Since, WiMAX supports high data rate transmission. So it can fulfill the demand of the present end users. Wi-Fi system is widely being used in the first world countries. WiMAX embedded devices support the Wi-Fi standards. So the people who are using Wi-Fi can easily switch to WiMAX technology. Moreover in the developing countries where high data rate wireless communication infra structure is not strong enough. WiMAX can be a good solution for these countries which is more secured, reliable and cheap. For these reasons the user of this technology is increasing day by day. As WiMAX is the latest technology and better solution in the wireless communication world, we have chosen this technology for our thesis. Our objective was to analyze the basic concept of this technology and design a security system based on WiMAX technology.

Reference:

1. Implementation of a WiMAX simulation in Simulink by Amalia da Roca
2. www.wikipedia.org
3. What Is A Convolutional Encoder / Convolutional Encoding... By: Kia Javadi
4. www.google.com
5. www.kitsrus.com
6. www.mikroe.com
7. digital logic and computer design, author M. Morris Mano
8. Fundamentals of WiMAX , author Jeffrey G. Andrews
9. www.wimax.com
10. www.wimaxforum.org
11. www.wimax.industry.com
12. www.buzzle.com
13. computer.howstuffworks.com
14. www.intel.com
15. scholar.google.com