WIMAX AND IT'S STATE OF DEPLOYMENT USING AVAILABLE TECHNOLOGY

BY

ISAKO MAIMUNA SHEHU

2005/22168EE

DEPARTMENT OF ELECTRICAL/COMPUTER ENGINEERING

SCHOOL OF ENGINEERING AND ENGINEERING TECHNOLOGY

FEDERAL UNIVERSITY OF TECHNOLOGY MINNA.

A THESIS SUBMITTED TO THE DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING, FEDERAL UNIVERSITY OF TECHNOLOGY MINNA
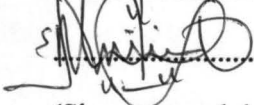
NOVEMBER, 2010

DEDICATION

I dedicate this project to Allah (SWT) for all His blessing upon my life. To my parents for their unconditional love and care. To my husband for his support, care and always being there for me.

DECLARATION

I, Isako Maimuna Shehu, declare that this work was done by me and has never been presented elsewhere for the award of a degree. I also hereby relinquish the copyright to the Federal University of Technology, Minna.
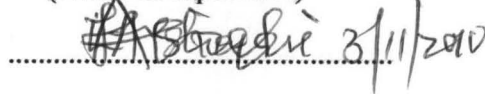

ISAKO MAIMUNA SHEHU

(Name of student)

03/11/2010

(Signature and date)

ENGR A.G. RAGI
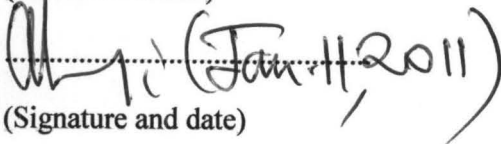
(Name of H.O.D)

(Jan-11,2011)
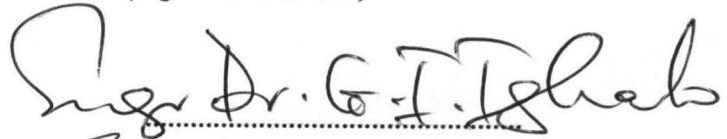
(Signature and date)

MR ENESI A. YAHAYA

(Name of supervisor)

3/11/2010

(Signature and date)

Engr. Dr. G.I.Ishako

(Name of External Examiner)

1/12/10

(Signature and date)

ACKNOWLEDGEMENT

Alhamdulillah! As this project marks the end of a chapter and opens a new one of self-actualization, realization, and a dream come true. This couldn't have been possible without the support of people who matter the most in my life.

I thank Allah (s.w.t) for his amazing grace, guidance, protection and indeed all forms of blessings he has bestowed on my life.

To those two people whom without, I will not have been here today, Alh Shehu Muhd Isako and Hajiya Aishatu Shehu Isako, you are incomparable, your tender and unconditional love, care, passion, support in all aspects of my life is worthy of mentioning. May you live long to reap the fruits of your labour. Also to my siblings Hauwa, Ahmad, Aisha, Abdurrahman and Baby Yahya, thanks for your moral support.

I cannot but express my innermost heartfelt gratitude and appreciation to my most precious treasure, (my husband) Alh Aliyu Sidi Ndako for the love, care, supports (physically, emotionally, financially and otherwise). You are my source of joy and happiness, my role model and a mentor worthy of emulation. I couldn't have wished for something better. Thanks for your kindness and encouragement. My wonderful kids; Aisha, Muhd, Amina and Walid, you all are most loved and appreciated for your understanding.

Also of immeasurable appreciation are my able and friendly supervisors Mr Enesi A. Yahaya and Mrs Asindi whose guidance and inspiration has given me confidence and built me for challenges ahead.

The staff of Spectrum Management Department of the Nigerian Communications Commission (NCC) particularly Engr Atiku Lawal, Engr (Mrs) Bilkisu Kida, Engr Fidelis

ABSTRACT

WiMAX (World Wide Interoperability of Microwave Access)is a technology based on the IEEE 802.16 specifications to enable the delivery of last mile wireless broadband access an alternative to cable and DSL. It transmits data using a variety of transmission modes from point-to-point links to a portable and fully mobile internet access. The technology provides up to 50KM of service area and allows users to get broadband connectivity without the need of direct line of sight to the base station. It also provide a total data rate of up to 75mbps which is enough to simultaneously support a lot of business and home requirement.

The WiMAX technology could be deployed in both licensed and unlicensed frequency bands. The licensed spectrum bands are 2.3GHz, 2.5GHz, 5.8GHz and possibly 700MHz. it uses both LOS(Line-of-sight) and NLOS(Non-line-of-sight) types of connection supports very high bandwidth solutions where large spectrum deployments(i.e. >10MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth needed to support a full range of high value multimedia services. It is intended to serve as the next step in the evolution of 3G (3rd Generation) mobile phones via a potential combination of WiMAX and CDMA(Code Division multiple Access) standards called 4G(4th Generation).

It was deployed in Nigeria by Galaxy wireless in 2006 and since then companies such as DoPC(Direct on PC), Spectranet among others have acquired licensed on different spectrum bands in which WiMAX operates with plans of deployment in parts of the country.

TABLE OF CONTENTS

List of figures page number

CHAPTER ONE

1.0; INTRODUCTION

1.1 NEED FOR WIRELESS DATA TRANSMISSION

Since the final decades of the twentieth century, data networks have known steadily growing success. After the installation of fixed internet networks in many places over the planet and their now large expansion, the need is now becoming more important for wireless access. There is no doubt that by the end of the first decade of the twentieth century, high-speed wireless data access, i.e. in Mb/s, will be largely deployed worldwide.

Wireless communication dates back to the end of the nineteenth century when the Maxwell equations showed that the transmission of information could be achieved without the need for wire. A few years later, experimentations such as those of Marconi proved that wireless transmission may be a reality and for rather long distances. Through the twentieth century, great electronic and propagation discoveries and inventions gave way to many wireless transmission systems.

In the 1970s, the bell laboratories proposed the cellular concept, a magic idea that allowed the coverage of a zone as large as needed using a fixed frequency bandwidth. Since then, many wireless technologies had large utilisation, the most successful until now being GSM, the Global System for mobile communication (previously Groupe Sp&eUcial Mobile), technology mainly used for voice transmission such as the Short Message Service (SMS). The GSM has evolutions that are already used in many countries. These evolutions are destined to facilitate relatively high-speed data communication in GSM-based networks. The most important evolutions are:

a) GPRS (General Packet Radio Service), the packet-switched evolution of GSM;

1

b) EDGE (Enhanced Data rates for GSM Evolution), which includes link or digital modulation efficiency adaptation, i.e. adaptation of transmission properties to the (quickly varying) radio channel state.

In addition to GSM, third-generation (3G) cellular systems, originally European and Japanese UMTS (Universal Mobile Telecommunication System) technology and originally American cdma2000 technology, are already deployed and are promising wireless communication systems. Cellular systems have to cover wide areas, as large as countries. Another approach is to use wireless access networks, which were initially proposed for Local Area Networks (LANs) but can also be used for wide area networks.

1.2 Wireless not Mobile

Different scenarios of mobility can be considered. The most simple one is when two neighbouring Base Stations (BSs) belong to the same operator. Hence the same billing system and customer care apply to two BSs. In this case, a user moving from one cell to a neighbouring one has to start the session again. This feature is nomadicity rather than mobility. Mobility (or full mobility) is the scenario where the session is not interrupted, whether this is a data session, a voice communication (over IP or not), a video transmission e. t. c.

The distinction is made between wireless (but yet geographically) fixed access, nomadicity, portability and mobility. Portability is when a user can move with a reasonable speed over a large area, covered by many BSs without interruption of a possible open session or communication. The value considered as a reasonable speed is of the order of 120km/h. Mobility is the same as portability but with no real limit for speed: i.e if mobility moves from on cell to another. This is called 'handover'. The cellular systems are then real mobile networks.

2

Wireless technology being the backbone of worldwide interoperability for microwave access, (WiMAX) is a means of transmitting signals using radio waves as a medium instead of wires. Nowadays cordless keyboards, mise, digital and cellular phones have become part of our daily lives.

Some of the inherent characteristics of wireless communication system which make it attractive for all globally are;

1. MOBILITY; A wireless communications system that allows users to access information beyond their desk and conduct businesses from anywhere without having a wired connectivity.

2. REACHABILITY; wireless communications system that enables people to be better connected and reachable without any limitation from any location

3. SIMPLICITY; communication system that's easy and fast to deploy in comparison of cabled network. Initial setup cost could be a bit high but other advantages overcome that high cost.

4. MAINTAINABILITY; Once setup, much is not needed for maintenance services.

5. ROAMING SERVICES; using a wireless network system you can provide services anywhere anytime including train, aeroplanes e t c

1.3 WIRELESS NETWORK TOPOLOGIES

There are basically three ways to setup a wireless network connection;

a) Point-to-point bridge; A bridge is used to connect two networks; A point-to-point bridge interconnects two buildings having different networks.

3

b) Point-to-multipoint bridge; this is used to connect three or more LANS that may be located on different floors in a building or across buildings.

c) Mesh or Adhoc Network; this is an independent local area network that is not connected to a wired infrastructure and in which all stations are connected directly to one another.

Wireless Technology can also be classified in different ways depending on their range. Each technology is depending on their range. Each technology is designed to serve a specific usage segment.

1.4 Wireless Broadband Access (WBA}

Wireless broadband is a technology that promises high-speed connection over the air. It uses radio waves to transmit and receive data directly to and from the potential users whenever they are in need of it. Technologies such as 3G, Wi-Fi, Wimax and UWB work together to meet these global needs

1.5 Objectives of the Research

1) To gain in-depth knowledge about wimax technology and how it works.

2) To understand the problems about the wimax technology in maintaining and deployment using the available technology.

3) To suggest the solutions and the enhancements found during the research.

4) To validate that the new enhancements will provide more security and reliability in the other people's research and context.

5) To compare and contrast between the different techniques used for wimax technology deployment.

1.6 Research Methodology

1) Study and investigation of technical features of the wimax network.

2) Research about the requirements for the deployment of the wimax technology.

3) Research about the basic requirements for the wimax technology.

4) Research for negative aspects, threats and vulnerabilities of wimax technology.

5) Discussion about the security functions of wimax technology.

6) Discuss about the future of wimax technology and related work for enhancements.

7) Discuss proposals for the solutions of threats to wimax technology.

1.7 SCOPE OF RESEARCH

The scope of this work is to have a background information on the deployments of the wimax technology by Nigerian telecom operators (case study of direct on pc and galaxy wireless) and also to know the modulation techniques used by these operator.

It also seeks to compare and contrast between the varying techniques used, the distances covered and the quality of service achieved using those schemes.

CHAPTER TWO

2.0 Historical Background

The worldwide interoperability of microwave access (WiMAX) is a telecommunication protocol that provides fixed and fully mobile access (which is based on the IEEE 802.16 standard also called broadband wireless access).The name "WiMAX "was formed by the WiMAX forum (an industry led non-profit organization whose founding fathers included; W-LAN, Ensemble, CossSpan, Harris, Nokia e.t.c. which as of the first quarter of 2008 has more than 540 member companies industry service providers, with the primary mission of products through its certification process.

It is also a "standard"-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.

2.1 Theoretical Background

2.1.1 Standardisation

WiMAX refers to interoperable implementation of the IEEE 802.16 wireless networks standard (ratified by the WiMAX forum), in similarity with Wi-Fi which refers to interoperable implementations of the 802.11 wireless LAN standard (ratified by the Wi-Fi alliance).The WiMAX certification forum allows vendors to sell their equipment as WiMAX (Fixed or mobile) certified, thus ensuring a level of interoperability with other certified products so long they fit the same profile.

2.2 pre-WiMAX systems

The first version of 802.16 standard appeared in 2001. The first complete version was published in 2004. There was evidently a need for wireless broadband much before these

6

dates. Many companies had wireless broadband equipment using proprietary technology since the 1990s and even before. Evidently these products were not interoperable. With the arrival of 802.16 standards, many of these products claimed to be based on it. This was again not possible to verify as WiMAX /802.16 interoperability tests and plug fest started in 2006. These products were known as pre-WiMAX equipments.

2.3 TYPE OF SERVICES

WiMAX can provide two forms of wireless service;

1) Non-line-of-sight; Similar to the Wi-Fi service, here a small antenna on the computer connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range, of between 2-11 GHz

2) Line-of-sight; here a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it's able to send a lot of data with fewer errors. Line-of-sight transmissions use higher frequencies with ranges reaching a possible 66GHz

2.4 USAGE MODELS OR TYPES

- 802.16-2004; often called 802.16d, since that was the working party that developed the standard. It is also frequently referred to as "fixed wimax". It has no support for mobility.

- 802.16e-2005; this is an amendment to 802.16e-2004 as is often referred to in shortened form as 802.16e. It introduced support for mobility among other things and is therefore also known as "mobile WiMAX"

However, IEEE 802.16e-2005 upon IEEE 802.16-2004 by;

1) Adding support for mobility

7

2) Scaling of the fast Fourier transform (FFT) to the channel bandwidth in order to keep the carrier spacing constant across different channel bandwidths (typically 1.25MHz, 5MHz, 10MHz, or 20MHz)

3) Advanced antenna diversity schemes, and hybrid automatic repeat-request (HARQ).

4) Adaptive antenna systems (AAS) and multi-input multi-output technology (MIMO).

5) Fast Fourier transform algorithm.

6) Adding an extra QoS class for V.I.P application.

It should be noted here that; fixed WiMAX is similar to WLAN in some aspects with an OFDM-based physical layer. Mobile WiMAX is based on an OFDMA physical layer.

Meanwhile, the basic element that differentiates these systems is the ground system at which the systems are designed to manage based on mobility.

2.5 Deployment

The existence of WiMAX since 2004 made it possible for equipment manufacturers to start the production of necessary promotion and certification of compatibility of equipments that conforms to the IEEE 802.16 standard.

However, actual deployment started in 2006 when Korea telecom started the deployment of a 2.3GHz version of a mobile wimax service called WiBRO in the Seoul metropolitan area to offer high performance for data and video. In a recent study by (wimax forum 2008c) more than 133 million wimax users globally are projected by the year 2012. The forum also claims that there are more than 250 trials and deployment worldwide.

In Nigeria, the Nigerian communication commission (NCC) has so far issued out licenses on the 2.3, 2.5 and 3.5 GHz to various telecom operators among which are Direct on pc, Cobra net, Galaxy wireless, XS broadband e.t.c

However, Galaxy wireless communications limited has launched Nigeria's first portable plug-and-play broadband wireless service. G-MAX based on the emerging mobile wimax 802.16e standard in Abuja, and Portharcourt. The G-MAX brand provides fixed and mobile broadband internet and data services at highly affordable costs designed to massively increase internet penetration in Nigeria. Xs broadband has wimax licenses for 24 of the 36 states in the country. Networks have however been deployed in most major cities to serve banks enterprises and other applications.

2.6 **Transmission method**

The IEEE 802.16-2004 standard specified orthogonal frequency division multiplexing (OFDM) as the transmission method for NLOS connections. The OFDM signal is made up of many orthogonal carriers, and every individual carrier is digitally modulated with a relatively slow symbol rate. This method has unique advantages of multipath propagation because more time is needed to transmit a symbol compared to the single method at the same transmission rate.

2.7 **Protocol layers and Topologies**

The IEEE 802.16 Broadband wireless access (BWA) network standard applies the open systems interconnection (OSI) network reference seven layered model also called the OSI seven layer models. This is very often used to describe the different aspects of a network technology. However, only the two lowest layers are defined. i.e. the physical layer (PHY) and media access control layer(MAC) layer, Which is the main part of the data link layer.

9

CHAPTER THREE

3.0 IEEE STANDARDS

WiMAX is loosely standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as cable modem, DSL and TI/EL) to provide broadband access.

The IEEE 802.16, also known as the IEEE wireless. Metropolitan area network (MAN) air interface is an emerging suite of standards for fixed, portable and mobile BWA in Metropolitan Area Network. These standards are issued by IEEE 802.16 work group that originally covered the wireless local loop (WLL) technologies in the 10.66GHz radio spectrum, which were later extended through amendment projects to include both licensed and unlicensed spectra from 2 to 11GHz.

The WiMAX network currently includes 802.16-2004 and 802.16e. 802.16-2004 utilizes OFDM to serve multiple users in a time division fashion in a sort of round-robin techniques, but done extremely quickly so that users have the perception that they are always transmitting/receiving. 802.16e utilizes OFDMA and can serve multiple users simultaneously by allocating sets of tones to each user.

3.0.1 CHART OF VARIOUS IEEE 802.16 STANDARDS RELATED TO WIMAX

	802.16	802.16a	802.16e
Spectrum	10-66 GHz	2-11 GHz	$\leq$ 6 GHz
Configuration	Line of sight	Non –line of sight	Non –line of sight
Bit rate	32-134 Mbps(28 MHz	$\leq$ 70 or 100 Mbps	Up to 15 Mbps

	channel)	(20MHz channel)	
Modulation	QPSK, 16-QAM, 64-QAM)	256 Sub-carriers OFDM using QPSK,16-QAM, 64-QAM,256-QAM	Same as 802.16a
Mobility	Fixed	Fixed	≤75 MPH
Channel bandwidth	20,25 28 MHz	Selectable 1.25 to 20 MHz	5 MHz (planned)
typical cell radius	1-3 miles	3-5 miles	1-3 miles
Completed	Dec , 2001	Jan , 2003	2nd Half of 2005

Fig3.1 Charts of IEEE standards related to WiMAX

3.1 CARRIER WAVES

Radio waves are electromagnetic waves that move at the speed of light in a sine wave formation and can be used to carry a message over a distance. They can have different frequencies which describes how fast they are moving up and down which is measured in cycles per second or hertz. Carrier waves with different frequencies have different properties. For example, light waves are visible to the naked eye but cannot travel through walls. Radio waves (especially those of lower frequency) can penetrate walls and buildings as well as bending (diffraction) around the corner.

3.2 MODULATION

1 0 1 0 0 1
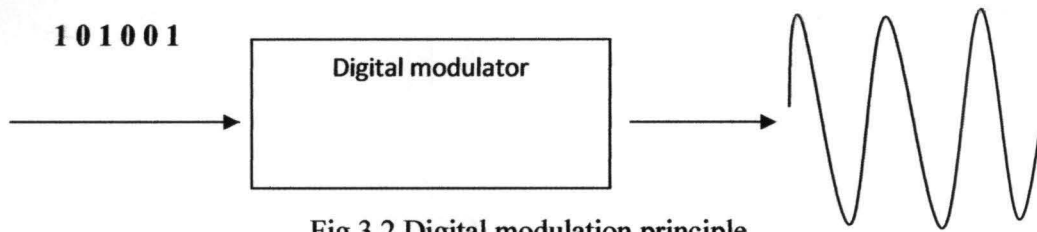
Fig 3.2 Digital modulation principle

Modulation is the process by which carrier wave is able to carry the message or digital signals (series of ones and zeroes). There are three basic methods of this: amplitude, frequency and phase shift keying. Higher orders of modulation allow us to encode more bits per symbol or period (time). Amplitude shift keying (ASK) involves increasing the amplitude (power) of the wave in step with the digital signal (in other words, low=0, high=1) and is used in AM radio. Frequency shift keying (FSK) changes the frequency in step with the digital signal. Systems that use this modulation (broadcast FM radio) tend to be more resilient to noise since noise usually changes the amplitude of the signal. In figure 1, different bits are represented by different frequencies which can then be detected by a receiver.
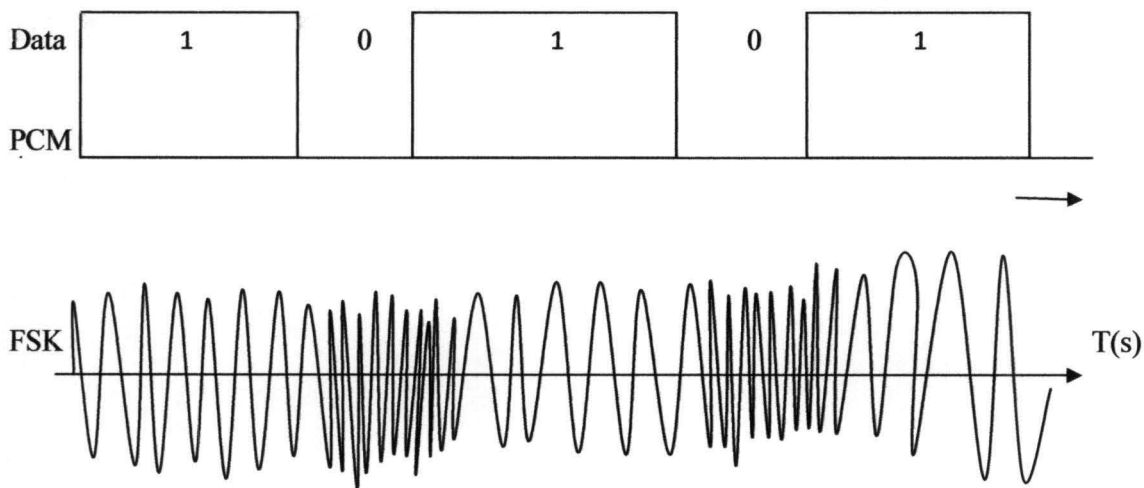
FIGURE 3.3: FREQUENCY SHIFT KEYING

Phase shift keying (PSK) changes the phase of the carrier in step with the digital message. For binary phase shift keying (BPSK), each symbol could indicate two different states or one

bit per symbol (in other words, 0=0, 180=1). In figure 2, the second wave is shifted by half a period or 180 degrees. The receiver can then recognize this shift indicating a digital one or zero.

3.2.1 MODULATION SCHEMES USED

Similar to all recent communication systems, WiMAX/802.16 uses digital modulation. Digital modulation principle uses an analogue signal with a digital sequence in order to transport this digital sequence over a given medium; fibre optics, radio link, wired line etc. This has great merit with regards to classical analogue modulation; better resistance to noise (i.e SNR is higher), use of high performance digital communication and coding algorithm e.t.c

Many digital modulations can be used in a telecommunication system. The variants are obtained by adjusting the physical characteristics of a sinusoidal carrier, the frequency, phase or amplitude, or a combination of some of these. Four modulation schemes i.e BSPK, QPSK, 16-QAM, and 64-QAM are used.

3.2.2   BINARY PHASE SHIFT KEYING (BPSK):   The Bpsk is a binary digital modulation; i.e one modulation symbol is one bit. This gives high immunity against noise and interference and a very robust modulation. A digital phase modulation, like Bpsk modulation, uses phase variation to encode bits; each modulation symbol is equivalent to one phase. The phase of the Bpsk modulated signal is n or –n according to the value of the data bit.

3.2.3   QUADRATURE PHASE SHIFT KEYING (QPSK):   When a higher spectra efficiency modulation is needed, i.e more bit/second/hertz, greater modulation symbols can be used e.g QPSK considers two bit modulation symbols. QPSK is less noise resistant than BPSK as it has a smaller immunity against interference.

13

3.2.4 QUADRATURE AMPLITUDE MODULATION (16-QAM and 64-QAM): The QAM changes the amplitudes of two sinusoidal carriers depending on the digital sequence that must be transmitted, the two carriers being out of phase of +n/2, this amplitude modulation is called quadrature. It should be mentioned that according to digital communication theory, QAM-4 and QPSK are the same modulation (considering complex data symbol). Both 16-QAM (4bits/modulation symbol) and 64-QAM (6-bits/modulation symbol) modulation are included in the 8092.16 standard. The 64-QAM is the most efficient modulation of 802.16 i.e 6-bits are transmitted with each modulation symbol. Optimal in some cases; license example bands, when the OFDM physical layer is used.For OFDMA layer, yet the mobile WIMAX profiles indicates that 64-QAM is mandatory in the downlink.

3.3 LINK ADAPTATION

Adaptation modulation implies having more than one modulation which is of great advantage; link adaptation can be used as used in recent communication systems like GSM/EDGE, UMTS, WIFI e.t.c. This is simple in the sense that when the radio link is good, use a high-level modulation, when radio link is bad, use a low-level but also robust modulation

Note that a greater data symbol modulation is more spectrum efficient but less robust.

3.4 ORTHOGONAL FREQUENCY DIVISION DUPLEXING

In 1966, Bell laboratory proposed the orthogonal frequency division multiplexing (OFDM) patent. Later, in 1985, ETSI included OFDM in the DVB-T system. In 1999, the Wi-Fi WLAN variant IEEE 802.11g considered OFDM for it's physical layer. Through time, it was discovered to be a reliable and good communication technology.

OFDM is therefore a powerful transmission technique. It is based on the principle of transmitting simultaneously many narrow-band orthogonal frequency, often called OFDM subcarriers or subcarriers. The number of subcarriers is often noted N. these frequencies are orthogonal to each other which (theoretically) eliminates the interference between channels.

Each frequency channel is modulated with a positively different digital modulation (usually the same in the first simple version). The frequency bandwidth associated with each of these channel is then much smaller than if the total bandwidth was occupied by a single modulation. This is known as the single carrier (SC). A data symbol time is N time longer, with OFDM providing a much better multipath resistance to multipath and the fact that the carriers are orthogonal allows a high spectral efficiency in the network. OFDM is often presented as the best performing transmission technique used for wireless systems.

3.4.1 BASIC PRINCIPLE USING THE INVERSE FAST FOURIER TRANSFORM

The Fast Fourier Transform Operators(FFT): this is a matrix computation that allows the discrete Fourier transform to be computed. The FFT works for any number of points. The operation is simpler when applied for a number N which is a power of 2 (e.g. N+256). The IFFT is the inverse fast Fourier transform operator and realizes the reverse operation. OFDM theory shows that the IFFT of magnitude N, applied on N symbols, realizes an OFDM signal, where each symbol is transmitted on one of the symbols of the type BPSK, QPSK, Qam-16 and Qam-64 (as discussed earlier).

If the duration of one transmitted modulation data symbol is Td, then Td=IΔF, where ΔF is the frequency bandwidth of the orthogonal frequencies. As the modulation symbols are transmitted simultaneously,

15

Td= duration of one OFDM symbol

= duration of one transmitted modulation data symbol.

This duration, ΔF, the frequency distance between the maximum of the real OFDM symbol is a little greater due to the addition of the cyclic prefix (CP)

3.4.2 TIME DOMAIN OFDM CONSIDERATIONS

After application of the IFFT, the OFDM theory requires that a cyclic prefix (CP) must be added at the beginning of the OFDM symbol. The CP however allows the receiver to absorb much more efficiency y=the delay spread due to the multipath and to maintain frequency orthogonal. The CP that occupies a duration called the Guard Time (GT), often denoted Ta, is a temporal redundancy that must be taken into account in rate computations. The ratio Ta/Td is very often denoted G in Wimax/802.16 documents. The choice of G is made according to the following considerations; if the multipath effect is important (a bad radio channel), a high value of G is needed, which increases the redundancy and then decreases the useful data rate; if the multipath effect is lighter (a good radio channel), a relatively smaller value of G can be used. For OFDM and OFDMA physical layer, 802.16 defined the following values for G: 1/4, 1/8, 1/16 and 1/32. For the mobile (OFDMA) Wimax profiles presently defined, only the value 1/8 is mandatory. The standard indicates that, for OFDM and OFDMA physical layers, and subscriber station (SS) searches, on initialization, for all possible values of the CP duration has link, it cannot be changed. Changing the CP would force all the subscribers to resynchronize to the based station (BS).

3.4.3 FREQUENCY DOMAIN OFDM CONSIDERATION

All the subscribers of an OFDM symbol do not carry useful data. There are four subcarrier types:

16

1. Data subcarriers; useful data transmission

2. Pilot subcarriers; mainly for channel estimation and subcarriers

3. Null subcarriers; no transmission. These are frequency guard bands.

4. Another null subcarrier is the DC9direct current) subcarrier.

In OFDM and OFDMA physical layers, the DC subcarriers are frequency of the transmitting station. It corresponds to frequency zero (direct current) if the FFT signals are not modulated. In order to simplify digital-to- analogue and analogue – to- digital converter operations, the DC subcarriers is null.

3.4.4 OFDM SYMBOL PARAMETERS AND SOME SIMPLE CONPUTATIONS:

The main Wimax OFDM symbol parameters are the following:

- The total number of subcarriers or equivalently the IFFT magnitude. For OFDM physical, Nfft=256, the number of lower frequency guard subcarriers is 28 and number of higher frequency guard subcarriers is 27. Considering also the DC subcarrier; there remains Nused, the number of used subcarrier, N excluding the null subcarrier. Hence, Nused=200 for OFDM physical, of which 192 are used for useful data transmission, after deducing the pilot subcarriers.

- BW, the normal channel bandwidth

- n, the sampling factor

  The sampling frequency, denoted Fs, is related to the occupied channel bandwidth by the following formula; Fs= nBW (simplified formula)

  From standard,

  Fs is truncated to an 8 KHz multiple. According to the 802.16 standard, the numerical value of n depends on the channel bandwidths. Possible values

17

8/7, 86/75, 144/125, 316/275 and 57/50 for OFDM physical and 8/7 and 28/25 for OFDMA physical.

3.4.5 DURATION OF AN OFDM SYMBOL

Based on the parameters defined above, the time duration of an OFDM symbol can be computed.

OFDM SYMBOL DURATION= useful time + guard time

= 1/cone subcarrier spacing + G * useful symbol time

= $(1/\Delta f)\ (1+G)$

= $(1/\ (fs_{/Nfft}))\ (1+ G)$

= $(1/\ (nBW\ /\ Nfft))\ (1+G)$

The OFDM symbol duration is a basic parameter for data rate computations.

3.4.6 DATA RATE VALUES

In OFDM physical, one OFDM symbol represents 192 subcarriers, each transmitting a modulation data symbol. The number of data transmitted for the duration of an OFDM symbol(value already known) can then be corrupted knowing the coding rate, the number of uncoded bits can be computed(table below) shows the data for different modulation and coding schemes (MCS) and G values. The occupied bandwidth considered is 7MHz and the sampling factor is 8/7 (i.e the value corresponding to 7MHz according to the standard)

Data rate = number of uncoded bits per OFDM symbol/ OFDM symbol duration

= $192 * 4*(3/4)/((256/7MHz* 8/7)(1+ 1/16))$

= 16.94Mbps

G ratio	Bpsk 1/2	Qpsk ½	Qpsk ¾	16-Qam1/2	16-Qam 3/4	64-Qam2/3	64-Qam 3/4
1/32	2.92	5.82	8.73	11.64	17.45	23.27	26.18
1/16	2.82	5.65	8.47	11.29	16.94	22.59	25.41
1/8	2.67	5.33	8.00	10.67	16.00	21.33	24.00
¼	2.40	4.80	7.20	9.60	14.40	19.20	21.60

Fig 3.4;The table above is the OFDM PHYSICAL data rates in Mbps(from IEEE standard 802.16-2004)

It should be noted here that these data rate values do not take into account some overheads such as preambles (of the order of one or two OFDM symbols per frames) and signaling messages present in frame. Hence they are known as raw data and are optimistic values

3.4.7 PHYSICAL SLOT (PS)

The physical slot (PS) is a basic unit of time in the 802.16 standard. The PS corresponding to four modulation symbols used on the transmission channel. For OFDM and OFDMA physical layers, a PS (duration is defined as

$$PS= 4/Fs$$

Therefore the PS duration is related to the system symbol rate. This unit of time defined in the standard allows integers to be used while referring to an amount of time, e.g. the definition of transition gaps(RTG and TTG) between uplink and downlink frames in the Time Division Duplexing (TDD) mode

3.4.8 The 802.16 physical transmission chains

The modulation and OFDM transmission are the major building blocks of wimax physical layer for both OFDM and OFDMA.

```
┌──────────────┐      ┌──────────────┐      ┌──────────────┐      ┌──────────────┐
│ Physical P D U│ ───▶ │ Randomisation │ ───▶ │ FEC encoder   │ ───▶ │ Repetition    │
│ to be        │      │              │      │ (cc turbo     │      │              │
│ transmitted  │      │              │      │ code)         │      │              │
└──────────────┘      └──────────────┘      └──────────────┘      └──────────────┘

        ┌──────────────┐      ┌──────────────┐
 ───▶   │ Modulation   │ ───▶ │ To OFDMA part:│
        │              │      │ IFFT CP;      │
        │              │      │ subchannels   │
        └──────────────┘      └──────────────┘
```
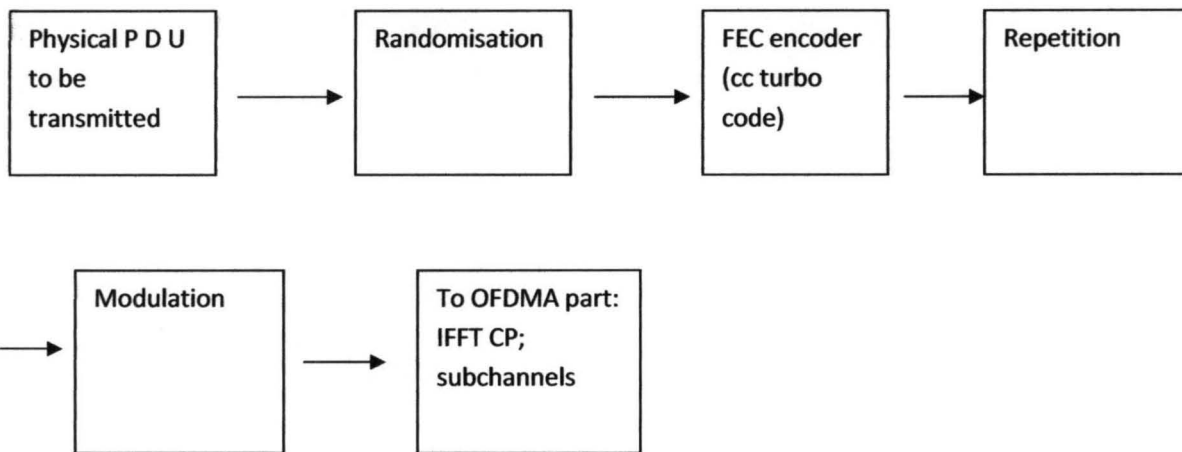
Fig3.5; OFDM PHY TRANSMISSION CHAIN

3.5 THE GLOBAL CHAINS

The physical chains of OFDM and OFDMA are illustrated in the figures below. The blocks are the same with the small difference that OFDMA physical includes repetition block. The modulated symbols are then transmitted on the OFDM orthogonal subcarriers. Wimax channel and coding are also described in the following.

```
┌──────────────┐      ┌──────────────┐      ┌──────────────┐      ┌──────────────┐
│ Physical PDU to│ ──▶ │ Randomization │ ──▶ │ FEC           │ ──▶ │ Interleaving  │
│ be transmitted │     │              │      │ encoder(CC    │      │              │
│              │      │              │      │ turbo code)   │      │              │
└──────────────┘      └──────────────┘      └──────────────┘      └──────────────┘

        ┌──────────────┐      ┌──────────────┐
 ───▶   │ Modulation   │ ───▶ │ To OFDM part: │
        │              │      │ FFT CP etc    │
        └──────────────┘      └──────────────┘
```

Fig3.6; OFDMA PHY TRANSMISSION CHAIN

3.5.2 CHANNEL CODING

The radio link is a quickly varying link, often suffering from great interference. Channel coding, whose main tasks are to prevent and to correct the transmission errors of wireless systems, must have a very good performance in order to maintain high data rates. The 802.16 channel coding chain is composed of three steps; Randomizer, Forward error correction(FEC) and Interleaving. They are applied in this order at transmission. The corresponding operations at the receiver are applied in reverse order.

3.5.3 TURBO CODING

Turbo codes are one of the few FEC codes to come close to Shannon limit, the theoretical limit of the maximum information transfer rate over a noisy channel. The turbo codes were proposed by Bemou and Glavieux from (ENST Bretagne, frame) in 1993. The main feature of the turbo codes that make them 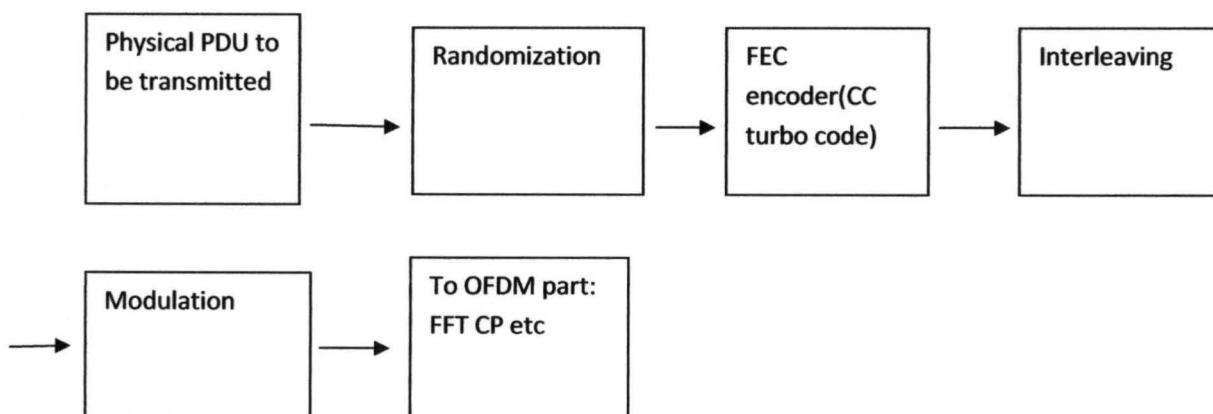different from the traditional FEC codes are the use of two error- correcting codes and an interleaver. Decoding is then made iteratively taking advantage of the two sources of transmission.

3.5.4 TRANSMISSION CONVERGENCE SUBLAYER(TCS)

The transmission convergence sub layer (TCS) is defined in the OFDM physical layer and the non-WiMAX SC physical layer. The TCS is located between the MAC and PHYSICAL layers. If the TCS is enabled, the TCS converts MAC PDU's of variable size into proper- length FEC blocks, called TCPDU. The TCS is an optimal mechanism for the OFDM PHY. It can be enabled on a preburst basis for both the uplink and downlink through the burst profile definitions in the uplink and downlink channel descriptor (UCD and DCD) message respectively. The TCS-ENABLE parameters coded as a TLV triple in the DCD and UCD burst profile encodings. At SS initialization, the TCS capability is negotiated between the BS and SS through

21

SBC-REQ/SBS-RSP MAC messages as an OFDM PHY specific parameter. The TCS is not included in the OFDMA PHY layer. Finally, the burst profile of OFDM and OFDMA PHY, an important building block of IEEE 802.16 MAC layer are described as thus;

3.5.5 BURST PROFILE

The burst profile is a basic tool in the 802.16 standard MAC layer, the burst profile allocation, which changes dynamically and possibly very fast, is about physical transmission. Here the parameter of the burst profile of WiMAX is summarized. The burst profiles are used for the link adaptation procedure

3.5.6 DOWNLINK BURST PROFILE PARAMETERS

The burst profile parameter of a downlink transmission for OFDM and OFDMA physical layers are proposal in the table below. The parameter called FEC code is in fact the modulation and coding, schemes (MCS). For OFDM PHY, there are 20 MCS combinations of modulation (Bpsk, Qpsk, 16-QAM, or 64-QAM) coding (CC, RS-CC, CTC or BTC, CC with optional interleaver) and coding rate(1/2, 2/3, ¾ and 5/6).

3.6 SCALABLE OFDMA (SOFDMA)

OFDMA multiple access is not the only specifying of OFDMA PHY. Another major difference is the fact that the OFDMA is scalable. Although this word does not appear in the standard, OFDMA PHY is said to have scalable OFDMA (SOFDMA). The scalability is the change of the FFT size and then the number of subcarriers. The supported FFT sizes are 2048, 1024, 512 and 128. FFT size 256 (of the OFDM layer) is not included on the OFDMA. Only 1024 and 512 are mandatory for mobile WiMAX profiles.

The change in the number of subcarriers, for fixed subcarrier spacing, provides for an adaptive occupied frequency bandwidth and equivalently, an adaptive data rate in the example in the table below. Here, the sampling factor is equal to 28/25, chosen according to the channel bandwidth. SOFDMA provides an additional resource allocation flexibility that can be used in the framework of radio resource management policy taking into account the dynamic spectrum demand, among others.

PARAMETERS	NUMERICAL VALUES	
Subcarrier frequency spacing	10.95KHz	
Useful symbol duration ($T_d=1/\Delta f$)	91.4µs	
Guard time($T_G = T_D/8$)	11.4µs	
OFDMA symbol duration($Ts=T_D+T_G$)	102.9µs	
Number of OFDMA symbol in 5ms frame	48	
FFT size(N_{fft}) or number of subcarriers	512	1024
Channel occupied bandwidth	5MHz	10MHz

Fig3.7; **OFDMA IN THE OFDM PHYSICAL LAYER**

3.7 SUBCHANNELISATION

As a matter of fact, the OFDM physical layer includes some OFDMA access.

Subchannelisation was included in 802.16-2004 for the uplink and also for the downlink in amendment 802.16e. the principle is as follows; the 192 useful data OFDM subcarriers of OFDM PHY are distributed in 16 subchannels made of 12 subcarriers each. Each subchannel is made of four groups of three adjacent subchannels each as shown below. . A subchannelisation transmission is a transmission on only part of the OFDM subcarrier space.

The subchannelisation transmission can take place on 1,2,4,8 or 16 subchannels. A five-bit indexation indicates the number of subchannels and the subcarrier indices used for each sub channel index for the uplink. One or more pilot subcarrier(s) (there are eight in total) are allocated only if two or more subchannels are allocated. The subcarriers other than the ones used for subchannelisation transmission are non-active (for the transmitted). The five-bit subchannel index is used in the uplink allocation message UL-MAP. Subchannelised transmission in the uplink is an option for an SS, it can be used only if the BS signals it's capability to decode such transmission. The BS must not assign to any given SS two or more overlapping subchannelisation allocations in the same time. The standard indicates that when subchannelisation is employed, the SS maintains the same transmitted power density unless the maximum power level is reached. Consequently, when the number of active subchannels allocated to an uplink user is reduced, the transmitted power is reduced proportionally, without additional power control messages. When the number of subchannels is increased the total transmitted power is also increased proportionally. The transmitted power level must not exceed the maximum levels dictated by signal integrity considerations and regulatory requirements. The subchannelisation can then represent transmitted power decreases and equivalently, capacity gains.

The 802.16e amendment defined an optional downlink subchannelisation zone in the OFDM PHY downlink subframe. Uplink subchannels are partly reused.

Burst profile parameter	Description
Frequency in KHz	Downlink frequency
FEC code type	Modulation and coding scheme(MCS); there are 20 MCSs in OFDM PHY(as updated in

	802.16e)
DIVC mandatory exit threshold	The CINR at or below where the burst profile can no longer be used where a change to a more robust(but also less frequency use efficient) burst profile is required expressed in 0.25db units
DIVC minimum entry threshold	The minimum CINR required to start using this burst profile when changing from a more robust burst profile expressed in 0.25db units
TCS-enable (OFDM PHY only)	Enables or disables TCS

Fig3.8; DOWNLINK BURST PROFILE PARAMETERS FOR OFDM AND OFDMA

PHYSCAL LAYERS

3.8 UPLINK BURST PROFILE PARAMETERS

The burst profile parameters of an uplink transmission for an OFDM PHY and an OFDMA

are shown in the tables below.

Burst profile parameter	Description
FEC type and modulation type	There are 20 MCS in OFDM PHY
Focused contention power boost	The power boost in db of focused
TCS_enable	Enable or disables TCS
FEC types and modulation type	There are 52 MCS in OFDMA PHY
Ranging data ratio	Reducing factor, in units of 1db, between the power used for this burst and the power used for CDMA ranging encoded as a signal

	integer

Fig3.9; UPLINK BURST PROFILE PARAMETER FOR THE OFDMA PHYSICAL LAYER

3.9 MCS LINK ADAPTATION

The choice between different burst profiles or, equivalently between different MCS is a powerful tool. Specifically choosing the MCS most suitable for the state of the radio channel, at each instant, leads to an optimal highest are rage data rate. This is the so-called link adaptation algorithm in itself is not indicated in the 802.16 standard. It is left to the vendor or operator to decide.

The order of magnitude of SNR thresholds can be obtained from table below proposed in the standard for some text conditions. These SNR thresholds are for a BER Bit-Error Rate, measured after the FEC, that is smaller than 10^{-6}.

Modulation	Coding rate	Receiver SNR threshold(dB)
BPSK	½	6.4
QPSK	½	9.4
QPSK	¾	11.2
QAM-16	½	16.4
QAM-16	¾	18.2
QAM-64	½	22.7
QAM-64	¾	24.4

Fig 3.10; **RECEIVED SNR THRESHOLD ASSUMPTIONS, TABLE 266,(FROM IEEE STD 802.16-2004)**

3.10 TYPES OF DUPLEXING IN 802.16 STANDARD

Duplexing transmission is the simultaneous transmission of two information signals that allows simultaneous(2-way communication) or It refers to the way downlink and uplink data is arranged in a two-way wireless transmission. The downlink carries information from a Base Station (BS) to Subscriber Stations (SSs). Downlink is also known as forward link. The uplink carries information from a SS to a BS. It is also called reverse link. There are two types of duplexing scheme, i.e. FDD and TDD.
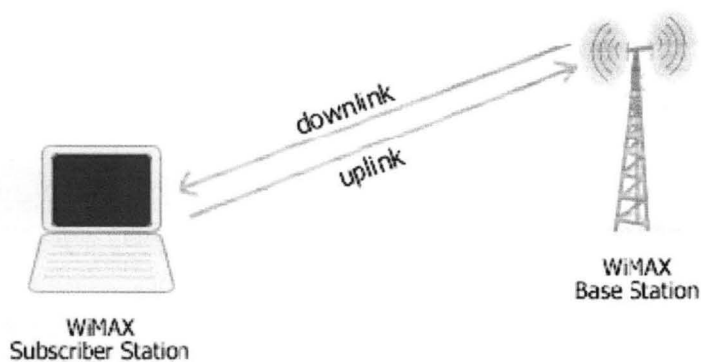
Figure3.11; Downlink and uplink traffic in a 2-way communication.

FDD (Frequency Division Duplex) requires two distinct channels for transmitting downlink sub-frame and uplink sub-frame at the same time slot. FDD is suitable for bi-directional voice service since it occupies a symmetric downlink and uplink channel pair. FDD is commonly used in cellular networks (2G and 3G). Meanwhile, WiMAX supports full-duplex FDD and half-duplex FDD (HFDD or HD-FDD). The difference is in full-duplex FDD a user device can transmit and receive simultaneously, while in half-duplex FDD a user device can only transmit or receive at any given moment.

Frequency Division Duplex (FDD)

frequency

frame

channel 2 ▓▓▓▓▓▓▓▓▓▓▓ downlink sub-frame
channel 1 ▓▓▓▓▓▓▓▓▓▓▓ uplink sub-frame   time

Figure3.12;   Frequency   Division   Duplex   (FDD)   -   full   duplex   mode
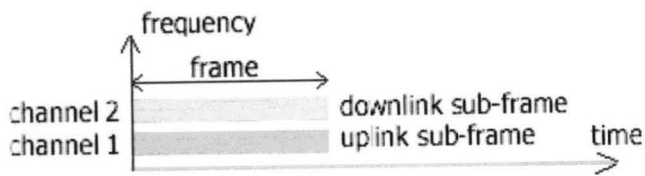
Downlink and uplink sub-frames are transmitted at the same time in two adjacent channels.

FDD is inefficient for handling asymmetric data services since data traffic may only occupy a small portion of a channel bandwidth at any given time. TDD (Time Division Duplex) is another duplexing scheme that requires only one channel for transmitting downlink and uplink sub-frames at two distinct time slots. TDD therefore has higher spectral efficiency than FDD. Moreover, using TDD downlink to uplink (DL/UL) ratio can be adjusted dynamically. TDD can flexibly handle both symmetric and asymmetric broadband traffic.

Time Division Duplex (TDD)

frequency

downlink   uplink
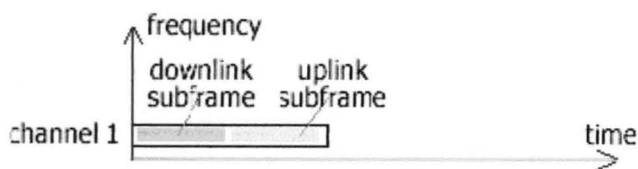subframe   subframe

channel 1 ▓▓▓▓▓▓   time

Figure3.13;TimeDivisionDuplex(TDD)

Downlink and uplink sub-frames are transmitted at different time slots in one channel.

When operating in the time division duplex mode, wimax devices require reversed time periods to allow for transmission time(guard time) and to allow the device to transition between receive and transmit mode(transition gap)

28

Guard time is an amount of time that is allocated within a single time slot period in a communication system to help ensure variable amounts of transit times(e.g. from close and distant transmitters) do not cause overlap(collision) between adjacent time slots. Transmission of information does not occur within the guard period.

Receive-transmit transition gap is the amount of time that is allocated between the reception of a packet and transmission of a packet in a time division duplex (TDD) system. Transmit-receive transition gap is the amount of time that is allocated between the transmission of a packet and the reception of a packet in a time division duplex (TDD) system.

WiMAX systems have the capability to dynamically change the amount of bandwidth that is transmitted in either direction through a process called adaptive time division duplex (ATDD). ATDD is a process of allowing two way communications between two devices by time sharing on the same communication channel (e.g. the same frequency) and the amount of transmission rate or time that is used by each device can dynamically change.

Most WiMAX implementations either on licensed or license-exempt bands will most likely use TDD. The reasons are TDD uses half of FDD spectrum hence saving the bandwidth, TDD system is less complex and thus cheaper, and WiMAX traffic will be dominated by asymmetric data. The first release of Fixed WiMAX profiles support both TDD and FDD, while Mobile WiMAX profiles only include TDD.

The figure below illustrates how the WiMAX system can use adaptive time division duplex transmission to vary the amount of bandwidth that is transferred in either direction. A base station initially sends data at a high rate. However, after the user has received the data, the base station begins to send a response at a high rate. The time periods allocated for transmission on the

downlink and uplink continually vary to allow for variable data   transmission rates.
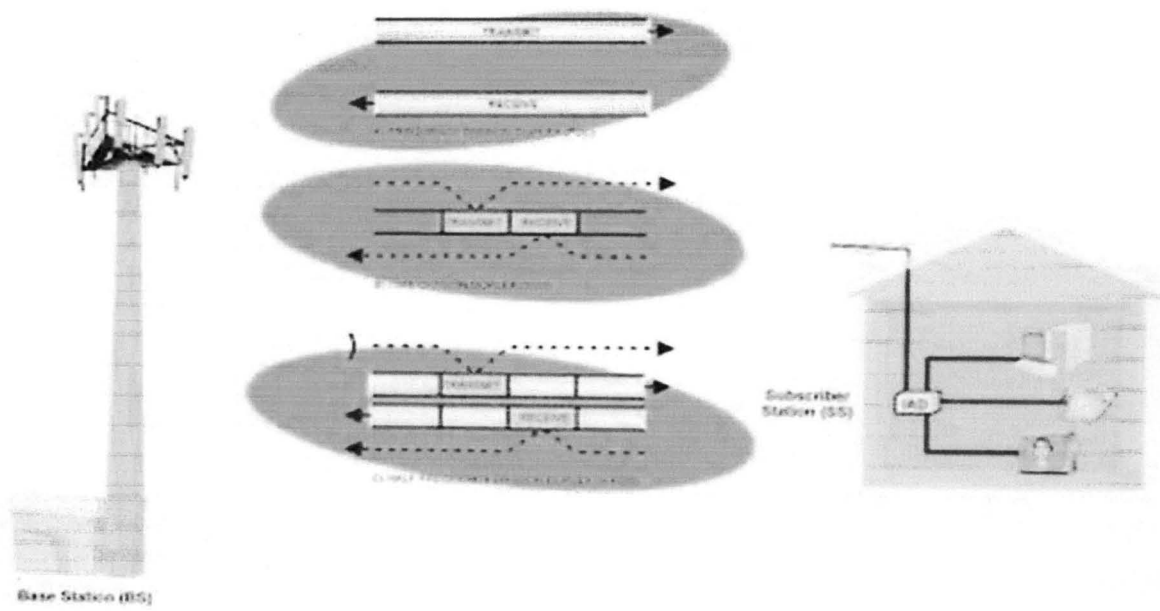
Fig3.14; Wimax duplex transmission

CHAPTER FOUR

PROBLEMS OF DEPLOYMEN OF WIMAX TECHNOLOGY

The availability of the right spectrum and in right amount is the key to the success of any wireless technology, and WiMAX is no exception. As in the case of WiMAX, it is more complicated in the sense that as of now WiMAX equipment are meant to operate in a scattered spectrum environment. In other words, there's no single frequency band common across the globe for WiMAX equipment. As it is the list of frequencies that a WiMAX equipment would need to incorporate include; 2.3GHz, 3.4GHz, 3.5GHz, 3.6GHz, 5.4GHz, 5.8GHz and possibly others such as 700MHz issues related to inoperability cannot be sorted out unless spectrum is harmonized. It also means that equipment vendors would have limited ability to drop WiMAX equipment prices.

WiMAX forum consists which of vendors and service providers, considers global harmonization or uniform allocation of spectrum worldwide as crucial for inventing equipment cost because radios are a major cost component in developing wimax forum certified systems.

Broadband operators and vendors across the world feel that the 2.5GHz and 3.5GHz frequencies would be ideal for WiMAX. The first of the products that were certified by the wimax forum where meant to operate in 3.5GHz band.

HIGH COST OF COSUMER PREMISE EQUIPMENT(CPE);

High cost of CPE is part of the major problems faced in the deployment of wimax besides issues relating to spectrum. The cost of CPE is likely to remain on the higher side for years to come, making it difficult to roll out WiMAX on a mass scale. At last, they can use it to compliment their existing DSL or Ethernet based broadband offerings.

WIMAX LIMITATIONS

Low bit rate over long distance.

WiMAX technology offering long distance data range which is 70km or 30 miles and high bit rate which is 70Mbits/s. This is good but both features doesn't work together when we will increase distance range, the bit rate wall is deceased and if increase in the bit rate is desired, there must be a reduction in the distance range.

SPEED OF CONNECTIVITY

Amongst the drawbacks of wimax technology is high connectivity which can be up to 20Mbits/s speed if a user is close to the cell and can degrade to as low as about 14Mbits/s speed, if the user exists at the cell edge from the tower.

WIMAX OVER WIFI

Compared to Wi-Fi which can easily be set up by anyone, WiMAX network is really expensive a reason which makes it very hard or everyone to pay a large amount for the setup and frequency license of WiMAX in a region.

WIMAX TECHNOLOGY AND DIFFERENT ARCHITECTURE

Because of low bit range on long distance, speed of connectivity from long range and low bandwidth among users. So many different granular and dispersed network architectures are being unsupported into WiMAX autonomous progress.

WIMAX QUALITY OF SERVICS (QoS)

The IEE 802.16 standard supports up to five QoS classes. The level o quality of service differentiation is per service flow. Each of the service flow is having one o the

scheduling types; Best effort (BE), non-real time polling (nrtps), real-time polling service (rt-ps), extended or unsolicited grant service (UGS).

WiMAX provides the five QoS classes through an architecture that is able to process requests perform access control and allocate the required radio resources that are able to meet the requests that are accepted. The five QoS classes are described below;

1) UGS; This is designed to support real-time data stream that consist of fixed sized packets issued at periodic intervals, such as backhaul and voice over (VOIP) without silence suppression

2) Ert-ps; It is designed for the extended real-time services at variable rates such as VOIP with silence suppression, interactive gaming and video telephoning.

3) Rt-ps; Designed t support real-time data streams of variable rates that are issued at periodic intervals, such as MPEG video, audio and video streaming, and interactive gaming.

4) Nrt-ps; This is designed to support delay-tolerant data streams consisting of variable-sized data packets such as file transfer protocol (FTP), browsing, video download, and video on demand

5) BE; This is also designed to support data streams for which there is no minimum service requirements and no guarantee of timely delivery of packets such as E-mail and internet browsing.

WiMAX differentiates the service flows at the IP layer through the different server code points (DSCP). DSCP is a field in the header of IP packets used for classifying packets entering the network in order to provide QoS

From an IP transport perspective, the WiMAX network is divided into multiple DSCP domains. On domain is between the base station and the ASN gateway

33

(ASN-GW) in every ASN termed as ASN different server domain, is between the ASN-GWs and the HAS. The third is between the HAS and internet or operator service network.

Threats to WiMAX technology

Rouge base station; Is an attacker station that duplicates a legitimate base station>the rouge base station puzzles a set of subscribers trying to get service through what they believe to be legitimate base station. It may result in long disturbance of service. The exact method of attack depends on the type of network. In a Wi-Fi network, which is carrier sense multiple access, the attacker has to capture the identity of a legitimate access points identity. It then injects the crafted messages when the medium is available. In a WiMAX network, this is more difficult to do because wimax uses time division multiple access. The attacker must transmit while the rouge base station is transmitting. The signal of the attacker however, must arrive at targeted receiver subscribers with more strength and must put the signal of the rogue base station in the background. Again the attacker has to capture the identity of a legitimate base station. Then it builds messages using stolen identity, the attacker has to wait until time slots allocated to the fake base station. The receiver subscriber reduces their own gain and decodes the signal of the attacker instead of the one from the fake base station. The rogue base station is likely to occur as there are no technical difficulties resolve. Extensible Authentication protocol (EAP) support mutual authentication that is, the base station also authenticates itself to the subscriber. When EAP mutual authentication is used, the likelihood of the threat is mitigated, but not totally and remains possible for reasons similar to EAP based authorization. The rogue base station or access point attack is therefore a threat for which the risk is critical.

34

DATALINK LAYER THREATS TO WIMAX

In a typical Wi-Fi mechanism, a digital subscriber line (DSI) feeds a packet-ized bit stream in to a modern or access point. Which in turn broadcast a radio signal; often encrypted to Wi-Fi enabled clients that de-packet this data into information? In a WiMAX installation, a fixed wireless base station similar in concept to a cell phone tower, serves an always on radio signal directly accessible by WiMAX enable clients with no need for leased lines or an intermediate access point.

Like Wi-Fi, the WiMAX (MAC) protocol, a sub-layer of the datalink layer, manage the consumer's access to the physical layer. However, the scheduling algorithm within the WiMAX MAC protocol offers optimal prioritization of this traffic based on first-in first-out (FIFO) scheduling in which clients seeking access to the (BS) are allocated bandwidth upon time of initial access, instead of random queue assignment based on order of (MAC) address as in Wi-Fi. Furthermore, the WiMAX media access control (MAC) protocol, ensures optimal(QoS) over its Wi-Fi predecessor, allocating bandwidth effectively by balancing clients needs instead of best effort service; that is, equal distribution of what remains after allocation of other consumers.

In addition, before encrypting the radio signal with wired equivalent privacy (WEP), WPA/PSK, or any other existing layer to security protocol, WiMAX basic authentication architecture by default, X509 based public key infrastructure (PKI) certificate authorization. In which BS authenticates the clients digital certificate prior to granting access to the physical layer.[micheal barbeau 2005]

PHYSICAL LAYER THREATS TO WIMAX TECHNOLOGY

Physical sub-layer resides on the top of physical layer in IEEE802.16 standard. Therefore, WiMAX network are opened to physical layer attacks for example, blocking and rushing. Blocking is done by activating a source of strong noise to significantly lowering the capacity of the channel, therefore, denying services (DoS) to all stations. However, blocking or jamming is detectable with radio analyzer devices. Rushing or scrambling is another type of jamming, but it takes place for short interval of time aimed at particular frames. Control or management messages could be jumbled, but it is not possible with delay sensitive message i.e., scrambling uplink slots are comparatively hard, because attacker has to interpret control information and to send noise during a particular interval. [Michel barbeau]

There are other several threats to the WiMAX technology such as the application layer threat, the privacy sub-lay threat, the mutual authentication, key management problem, threat of identity theft. Water Torture and blacks that threat which are also known as hackers who crack into the network or the computer system for their own financial benefit or mental satisfaction.

WIMAX AVAILABILITY PROBLEMS

WiMAX deployment will use licensed radio frequency(RF) spectrum, positively granting them some degree of protection from unintentional interference. It is reasonably simple, however, for an attacker to use readily available tools to jam the spectrum for all planned wimax deployments. In addition to physical layer[DoS] ATTACKS, an attackers can use legally management frames to forcibly disconnect legitimate stations. This is similar to the de-authenticated flood attacks used against 802.11(Wi-Fi) networks. [Joshua Wright, Dec 12,2006]

To prevent the wimax network to be jammed, plenty the system from[DoS] attacks will be most suitable by proposing physical layer security measures by extensive research.

OTHER THREATS TO WIMAX TECHNOLOGY

According to experts, wimax technology is still facing problems security and also vulnerable to [DoS] attacks, because there is no mechanism in place to specifically detect and discard the repeated packets in the message. An attacker could repeat many messages, valid or not, in an attempt to interfere with the operation of the network. The impact of this type of attack can be very high because it might affect the operation of the communication system within wimax technology.

The risk is significant and that it might be sensible to employ a second line of defense against such an attack. Several weaknesses in (PKM) have also been discovered. PKM prevents eavesdropping and passive attacks by using hashed-message-authentication code and traffic encryption keys(TEK). AL key negotiation and data –encryption –key generation rely on the authentication keys(AK) secret. The AK is generated by the base station and the TEK is generated from the AK but only has a 2-bit identifier space, which is insufficient during the AK lifetime. (wimax vision).

SECURITY

A wireless system uses the radio channel, which is an open channel. Hence, security procedure must be included in order to protect the traffic confidentiality and integrity and to prevent different network security attacks such as theft of service. The IEEE802.16 MAC layer contains a security sub-layer.

The privacy key management (PKM) ; this is included in the 802.16-2004 standard security sub-layer in order to provide secure distribution of keying data from the BS to the SS. It is

also used to apply conditional access to network services, making it the authentication protocol, protecting them from theft of service (or service hi-jacking) and providing a secure key exchange.

The security sub-layer has been redefined in the IEEE802.16e amendment mainly due to the fact that 802.16-2004 had some security lapses.(e.g. there is no authentication of BS) and that the security requirements for mobile services are not the same as for fixed services.

The security sub-layer has two main components protocols as thus;

1. A data encapsulation protocol for securing packet data across the fixed BWA network. This protocol defines a set of supported cryptographic suites, i.e. pairing of data encryption and authentication algorithms and the rules of applying these algorithms.

2. A key management protocol (PKM) providing the secure distribution of keying data from the BS to the SS. Though this key management protocol, the SS's and BS does synchronize keying data. The BS also uses the protocol to enforce conditional access to network services.

ENCRYPTION ALGORITHMS

Many encryption algorithms are included in the 802.16 standard security sub-layer. They can be used for securing ciphering key exchange and for encryption of transport data. Some of these algorithms are optional for some applications.

The encryption algorithms included in 802.16 are;

RSA (Rivest Shamir adleman) RSA is a public key asymmetric encryption algorithm used to encrypt the authorization reply message using the SS public key. The authorization reply message includes the authorization key (AK). RSA may also be used for the encryption of traffic encryption keys when these are transmitted from the BS to the SS.

DES(data encryption standard); the DES and 3-DES are shared(secret)-key encryption algorithms. The DES algorithm may be used for traffic data encryption. It is mandatory for 802.16 equipment. The 3-DES algorithm can be used for the encryption for the traffic encryption keys.

AES(advanced encryption standard). The AES algorithm is a shared (secret) –key encryption algorithm. The AES algorithm may be used for traffic data encryption and can also be used for the encryption of the traffic encryption keys. Its implementation is however optional

ENCRYPTION KEYS AND SECURITY ASSOCIATIONS

802.16 standard security uses many encryption keys. The encryption keys defined in 802.16-2004 are listed in the table below where notation and the number of bits in each key are given.

ENCRYPTION KEY	NOTATION	NUMBER OF BITS	DESCRIPTION
Authorization key	AK	160	Authentication of an SS by BS shared secret used to secure further transactions and generating encryption keys. Lifetime is between 1-70 days
Key encryption key	KEK	128	3- DES key used for the encryption of the

39

			TEK
Traffic encryption key	TEK	128	Data encryption key lifetime between 30min-7days
HMAC key for the downlink	HMAC- key-D	160	Used for authenticating messages in the down link direction.
HMAC key for the uplnk.	HMAC-key-U	160	Used for authenticating messages in the uplink direction
HMAC key in the mesh mode	HMAC-key-S		Used for authenticating messages in the mesh mode

Fig 4.1;The main keys used in the 802.16 standard after the 802.16e amendment.[table by L.nuaymi, M.boutin and M. jubin]

The standard defines a security association(AS) as a set of security. A BS and one more of its client SS's (or MSS) share in order to support secure communications. An SA's shared information includes the cryptographic suite employed within the SA. A cryptographic suite is the SA's set of methods for data encryption, data

40

authentication and TEK exchange. The exact content of the SA is dependent on the SA's cryptographic suite encryption keys, keys lifetime, e.t.c.

The security association identifier (SAID) is a 16-bit identifier shared between the BS and the SS that uniquely identifies an SA. These are 3 types of security associations; the SA for unicast connections, the group security association (GSA) for multicast groups and the MBS group security association (MBSGSA) for MBS services.

The SA's are managed by the BS. When an authentication event takes place The BS gives the SS a list of security association associated with its connections. Generally, an SS has a security association (primary association) for its secondary management connection and two more for the downlink and the uplink links. After that, the BS may indicate one or more new SA's to the SS.

Static SA;s are provisioned within the BS. Dynamic SA's are created and deleted as required in respond to the initiation and termination of specific service flows.

CHAPTER FIVE

CONCLUSION

FUTURE TRENDS IN WIMAX DEPLOYMENT

Deployment of WiMAX technology has known no bounds since its standardization world over , Nigeria is not an exception as recently. The Nigeria communication commission has auctioned the 2.3GHz band to companies such as mobitel, DoPC, Spectranet, multi links amongst others which is most suitable for the technology of interest to this work is that of DoPC as before now it has only regional license in some frequency bands on which WiMAX operates but now has National licensed, this means in no time, all the 36 states will have a feel of the technology. The company also had only about 45 BS deployments as at the first quarter of 2009 but now has about 200 more deployments across some states with plans to deploy about 250 BS's before the end of 2011.

Adaptive modulation which allows the WiMAX system to adjust the signal modulation scheme depending on the signal to noise ratio (SNR) condition of the radio link also has a new techniques which is the 256QAM, this techniques allows 8-bits/modulation symbols but has not yet been incorporated by the equipment manufacturers in the production of WiMAX certified equipment as stated in the standard.

The WiMAX technology is a broadband access that delivers wireless access of up to 40mbps with the IEEE 802.16m update expected after up to 1Gbps fixed speed. Its transmit using both LOS and NLOS connection with the WiMAX physical layer (PHY) being based on OFDM, a scheme that offers good resistance to multipath and allows it to operate in the NLOS condition. It is capable of supporting very high peak data rates. The peak PHY data rate can be as high as 74mbs when operating using a 20MHz wide spectrum.

42

However, the limitations of the technology are that it either operates efficiently at high speed or over a long distance with efficiency traded off. This has however made it to be deployed in areas where wired line cannot get to with degraded quality of service.

REFERENCES

1. IEEE 802.16e, IEEE standard for local and metropolitan Area Network, Air Interface for fixed Broadband wireless access systems, amendment 2; physical and medium access control layers for combined fixed and mobile operation licensed bands and corrigendum 1, February 2006 (approved; 7 December 2005)

2. PKCS #1 V2.0, RSA Cryptography Standard, RSA laboratories, October 1998.

3. National Technical Information Service(NTIS), Fip 46-3, Data encryption standard(DES) October 1999, http:/www.ntis.gov/

4. National Technical Information Service (NTIS), FIPs 197, Advanced encryption standard (AES), November 2001.

5. www.googlsearch.com

6. www.mamma.com

7. www.ask.com

8. Lecture note on Communication System by Dr. Onwuka

9. Van Nee, R and Pascal, R, OFDM for Wireless multimedia Communication,2000.

10. IEEE 802.16-2004, IEEE standard for local and metropolitan Area Networks, Air interfaces for fixed broadband wireless access System, October 2004.

11. WiMAX forum white paper, mobile wx-part1:9 technical overview and performance evaluation, March 2006.

12. www.IEEE 802.org/16

13. A text book of WiMAX technology for Brad Wireless Access

14. Voip.fact.net/wimax/deployment/galaxy-ne.com

15. www.coursework4you.co.uk

16. www.freewimax.com

17. Technology for broadband access by Loutfi Nuaymi ENST Bretagne, France

18. http:/www.tutorialspoint.com/cgi-bin/printversion.cgi?

19. http:/etutorials.org/Network/wimax+technology+broadband+wireless+access/part
   +one

20. http:/en.wikipedia.org/wiki/WiMax