A Systematic Investigation of WiMAX and its Standards, Development, Technology and Security

Renuka Sharma
Department of CSE
NIET, Greater Noida

Pankaj Kumar
Department of CSE
NIET, Greater Noida

Devottam Gaurav
Department of CSE
NIET, Greater Noida

ABSTRACT
WiMAX is an emerging new technology that offers opportunities to telecom operators for enhanced broadband coverage and service offering. The broadband wireless Technologies is based on IEEE 802.16. It is known as WiMAX (Worldwide Interoperability for Microwave Access). Broadband wireless access (BWA) is the hottest technology aims to deliver high data rate over the large distance and offer multimedia services in metropolitan areas with a simpler installation and low cost compared to the wired network. WiMAX is nascent in the field of communication, operates in MAC and physical layer. Nowadays, usages of the mobile Internet have grown rapidly and required very high-speed access to internet application. In this paper, we discuss on 802.16 standards and its evolution with related issues.

Keywords
Mobile WiMAX, Fixed WiMAX, IEEE 802.16, Security, Mobile Station, Base Station

1. INTRODUCTION
Today's broadband Internet connections are limited to wired infrastructure using digital subscriber line (DSL), T1 or cable-modem based connection. However, these wired infrastructures are considerably more costly and time-consuming to deploy than a wireless connection. Whenever, in undeveloped areas and developing countries, provide are unwilling to install then required equipment including optical fibre or copper wire or etc. other for broadband services expecting the low profit. Broadband Wireless Access (BWA) has emerged as a promising solution for large distance access technology to provide very high-speed connections. IEEE 802.16 standard for Broadband Wireless Access and its linked industry consortium, Worldwide Interoperability for Microwave Access (WiMAX) Forum promise to offer high data rate over the large distance to a large number of customers, where broadband is unreachable. This is the first industry-wide standard that can be used for fixed wireless access (IEEE 802.16d) with substantially higher bandwidth than most cellular networks [13]. Development of this standard provides the low cost equipment, ensure interoperability, and reduce investment risk for operators. WiMAX is one of the nascent and hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise users in an economical way. WiMAX would operate or work similar to Wi-Fi, [8] but at higher speeds over larger distances and for a greater number of customers. WiMAX can provide service even in areas that are most difficult for wired infrastructure to reach and the capability to overcome the physical limitations of traditional wired infrastructure. The Wireless system is considered to be a perfect and attractive solution to provide high data rates over large distance communications, particularly for mobile users. The IEEE 802.16 standards are also known as WiMAX standards, are intended to offer wireless broadband access for the long range propagation. WiMAX is based on Wireless Metropolitan Area Network (WMAN) which provides very high data throughput over long distance (20 or 30 miles) in Non-Line of Site (NLOS) propagation [6]. This technology aims to provide broadband wireless access as well as internet access. The IEEE 802.16 standards have divided the WiMAX system into two groups [6]. Fixed WiMAX (IEEE 802.16d-2004), Mobile WiMAX (IEEE 802.16e-2005)

1.1 Evolutions of WiMAX
In the recent years, the working group of IEEE 802.16 has developed some number of standards for WiMAX. The first standard was published in 2001 and focused on the frequency range between 10 to 66 GHz and required line-of-sight (LOS) transmission between the sender and the receiver. This reduces multipath distortion, thereby enhancing communication efficiency. Theoretically, IEEE 802.16 can provide single transmission data rates 10 to 75 Mbps on both the uplink and downlink. Service -Providers could use multiple IEEE 802.16 channels for a single transmission to provide bandwidths of up to 350 Mbps [12]. The line of sight (LOS) transmission is fixed in nature so, cost-effective deployment is not possible. Consequently, several versions came with new features and techniques. The fixed WiMAX (IEEE 802.16-2004), has been developed to enhance the scope to licensed and license-exempt bands from 2 to 10 GHz. Fixed WiMAX specifies the air interface with including the Media Access Control (MAC) of wireless access for fixed operation in metropolitan area networks(MAN). Support for portable or mobile devices is considered in IEEE 802.16e std., which is published in 2005 (end of the year). WiMAX networks consist of some Subscriber Stations and a central radio Base Station. In the WiMAX network, Base station is fixed in nature is connected to the public network and can handle multiple sectors simultaneously, and Subscriber station are mobile. In this section, we describe the development phases of IEEE 802 .16 extension from the beginning to last release. In this section we describe the development phases of IEEE 802 .16 extension from the beginning to last release [4, 7] of WiMAX.

Table 1: Evolution of WiMAX standards [4]

IEEE Std.	Year	Frequency Band	Specific features
802.16	2001	10-66 GHz	The Initial version of WiMAX based on the single carrier physical layer and the burst TDM MAC layer. Use (line of sight towers) to fixed

			location.
802.16a	2003	2-11 GHz	Operates with Non-Line of Sight. Max transmission rate is 75 Mbps.
802.16c	2003	10-66 GHz	Broadband Wireless Access. Interoperability specification.
802.16d	2004	2-11 GHz	Based on 802.16 std. With some improvement and support both TDD and FDD transmission.
802.16e	2005	2-6 GHz	Privacy sub – layer for network security and power saving mode for MS. Mobility support to 65 mph with data Transmission rate up to 15 Mbps and distance area 1-3 miles.
802.16f	2005	2-11GHz	The 802.16f define the mesh networking and management information base. Improve the coverage area.
802.16g 802.16h 802.16i 802.16j 802.16k 802.16m	2007-2011	2-11 GHz	Data transfer rate: mobile user 100Mbps Fixed user 1 GB. Multi-hop relay specification. Advanced air – interface. Management plan procedure and services, mobility at the higher level.

1.2 Architecture of WiMAX

The WiMAX network architecture is based on an all-IP model. The WiMAX Forum has defined an architecture reference model, in which a WiMAX network can be linked to an IP-based core network, which is typically chosen by network operators that serve as Internet Service Providers, otherwise, the WiMAX Base Station provide seamless integration abilities with other types of architectures as with packet switched Mobile Networks [5].

1.3 Mobile Subscriber Station (MS)

It [4] is a mobile device used by the mobile subscriber to provide connectivity between mobile subscriber equipment and the base station equipment, Show in figure 3.

1.4 Base Transceiver Station (BTS)

BTS is known as base station which is an electronic device with tower provides large area coverage also known as the cell. Any wireless device located in the cell can access Internet. Maximum radius of a cell is 30 miles.

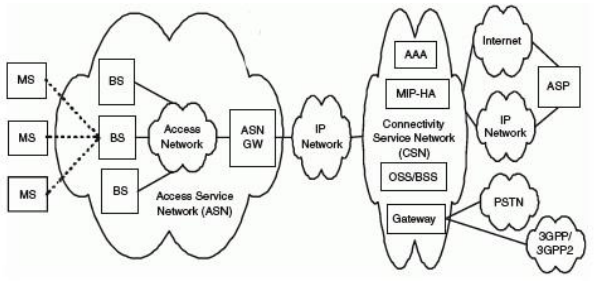

Figure 1: Architecture of WiMAX component [5]

1.5 Access Service Network (ASN)

ASN is a complete set of n/w function that provides radio access to the subscriber.ASN includes DHCP addressing function, proxy AAA server, and other IP-based recourses, including n/w management.ASN is used in the handover process, Quality of Service (QoS), Radio resource management.

1.6 ASN Gateway

The Access Service Network (ASN) gateway within the WiMAX network architecture works as a layer 2 traffic aggregation point within the almost ASN. The Access Service Network-Gateway (ASN-GW) may also provide additional functionality that includes: intra – Access service network (I-ASN), location management, paging, radio resource management and caching of subscriber profiles and encryption keys. The Access Service Network-Gateway (ASN-GW) may also include the AAA client functionality, establishment and management of mobility tunnel with base stations, Quality of Service (QoS) and policy enforcement, visited user functionality for mobile IP, and routing to the selected CSN.

1.7 Connectivity Service Network (CSN)

Connectivity Service Network (CSN) provides the IP connectivity service to the subscriber through the ASP. The Network Service Provider (NSP) uses CSN for internet connectivity, authentication, authorization, management of IP addresses, and roaming among the ASNs. There are following key components of CSN.

Home Agent (HA): In the WiMAX network, the Home Agent is located within the Connectivity Service Network. In which Mobile- internet protocol forming a key element of WiMAX technology and the Home Agent works in conjunction with an "Outer Agent", in the ASN Gateway, to provide an efficient end-to-end Mobile IP solution. The Home Agent serves as an anchor point for subscribers and providing secure roaming with Quality of Service (QOS) capabilities.

Authentication, Authorization and Accounting Server (AAA): it is included within the Connectivity Service Network (CSN), any communications or wireless system requiring subscription services, an Authentication, Authorization and Accounting server is used.

Domain Name Server (DNS): DNS translates the domain name into IP address.

Dynamic Host Configuration Protocol (DHCP): DHCP provides IP to entities in the network (including subscriber) dynamically. DHCP allow IPs to be assigned automatically to the computer.

1.8 Network Service Provider (NSP)

Network Service Provider uses Connectivity Service Network for internet connectivity, authentication, authorization, management of IP addresses, and roaming among the ASNs [7].

1.9 Application service provider (ASP)

It is a system-based service to customers over a network; such as access to a particular software application using a standard protocol (such as HTTP).

1.10 Characteristics of WiMAX

Following are the Characteristics of WiMAX are discussed here:

- It uses microwave to transfer the data in wireless mode.
- It specifies a frequency band in the range between 2GHz to 66 GHz For high-speed wireless networking
- A WiMAX is a wireless internet service that is capable of covering a wide geographical area by serving hundred of uses at a very low cost.
- Uses Orthogonal Frequency Division Multiplexing (OFDM) that is best for multipath environments.
- It includes Time Division Duplexing and Frequency Division Duplexing support.
- An easy and fast system to install
- Flexible channel size(3.5 MHz,5MHz,10MHz)
- Leading to low installation cost, when compare to fibre , cable or DSL deployment

1.11 Types of WiMAX (IEEE 802.16)

The IEEE 802.16 standard have divided the WiMAX system into two groups: Fixed WiMAX (IEEE 802.16d-2004) and Mobile WiMAX (IEEE 802.16e-2005)

1.11.1 Fixed WiMAX

It is defined as IEEE 802.16d -2004 standards, Fixed WiMAX system based on the Wireless MAN-OFDM physical layer specifications with 256 carriers. Fixed WiMAX delivers point to multipoint (P2M) broadband wireless services to our homes and offices. WiMAX forum promises to offer high data rate over long-distance to a large number of users where broadband service is unreachable. The Forum defines WiMAX as "a standard-based technology which is based on IEEE 802.16d and authorises the delivery of last mile wireless broadband access as an alternative to cable and DSL". An air interface based on orthogonal frequency division multiplexing (OFDM) is used by it, which is very secure against multi-path propagation an frequency selective fading. An adaptive modulation technique is used to increase performance when the link characteristics vary. In fixed WiMAX system used Frequency Division Duplexing (FDD), where the Base Stations (BSs) and the user terminals transmit in different frequency bands. The IEEE.802.16 standard define MAC layer, which is connection oriented and uses a Time Division Multiplexing (TDM) for the downlink (DL) and a Time Division Multiple Access (TDMA) schemes for the uplink (UL). This reflects the Point to Multipoint (PMP) architecture[6].

Following key features of fixed WiMAX are described as;

- Fixed WiMAX support fixed and nomadic application.
- Operate in the frequency band of 2GHz to 11GHz.
- Provide the transmission range up to 75 Mbps for the distance approx.30 miles (50kms).
- SC (single-carrier) modulation is use.

1.11.1.1 Applications

Fixed WiMAX include wireless E1 enterprise backhaul and residential 'last mile' broadband access.

1.11.1.2 Drawback

- Fixed WiMAX is costly due to its fixed infrastructure nature more cable connections are require, and It does not support mobile application(service provided fixed and not portable)
- 802.16d does not supports multicast and broadcast services
- Fixed WiMAX does not support power reduction function. While mobile WiMAX defines a series of sleep and idle mode power management functions to preserve battery life for a, enable power conservation end-user devices.

1.11.2 Mobile WiMAX

It is defined as IEEE 802.16e-2005 standards, offers scalability in both radio access technology and network architecture, so it provides flexibility in network deployment and service offerings. Mobile WiMAX adds significant improvements:

It improves Non-Line of Sight coverage by utilising advanced antenna diversity schemes and hybrid automatic repeat request (HARQ). It selects dense sub-channelization, so it was enhancing system gain and improving indoor penetration. It uses multiple input multiple output (MIMO) technologies and adaptive antenna system (AAS) to improve service offering coverage. It defined a downlink sub-channelization scheme, enabling better coverage and capacity trade-off.

There are several key features supported by mobile WiMAX:

- Mobile WiMAX support fixed, nomadic, mobile, portable application
- Mobile WiMAX operates in the frequency band of 2GHz to 6GHz.
- Transmission range up to 75 Mbps for the distance 10 miles (15 KMs)
- Multicarrier signal (OFDM) is use.
- Higher peak and user data rates using wider-band carriers(20 MHz)
- Lower latency through faster MAC signalling.
- Enhanced coverage in high inference environment with improvement preamble and control channel.
- Support for both multi-hop relay and femtocells.
- Improved power saving operation.

All this features and enhancements in mobile WiMAX make it backwards compatible with the previous version.

K. Etemad [1] define a WiMAX can be deployed as a green field network without any unnecessary complexity due to legacy circuit – switched system support. It can be deploy as an overlay to existing fixed and mobile access network such as 2.5 G /3.5G cellular system and or cable/digital subscriber line (DSL) by supporting different levels of interworking to ensure service continuity.

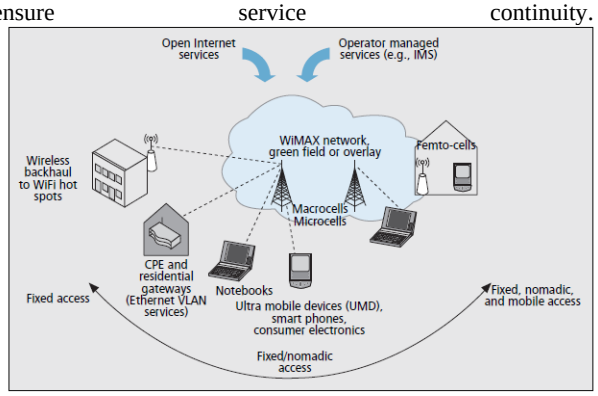

Figure 2: Mobile WiMAX with a verity of usage models in the same network [1]

The same network use for a variety of usage models such as wireless backhaul to Wi-Fi hot spots, fixed/nomadic access to customer premises equipment (CPE) and residential gateways (RGs), and mobile access to notebooks, smart phones, and next-generation WiMAX embedded ultra-mobile devices (Fig. 1). All this show how WiMAX have the seamless connection with different IP network that shows interoperability features of WiMAX with low installation cost and high-speed data without destroying the old connection.

1.11.2.1 Mobile WiMAX Release

IEEE 802.16 and mobile WiMAX release. The next generation of mobile WiMAX is expected to be based on IEEE 802.16m was completed in 2010 and certification /development in 2011/2012.

The following are some of the key enhancement expected in 802.16m

- Lower latency through faster MAC signalling.
- Enhanced coverage in high inference environment with improvement preamble and control channel.
- It allows both combination of multi-hop relay and femtocells.
- Improved power saving operation. All these features and enhancements in mobile WiMAX make it backwards compatible with the previous version.

1.11.2.2 Working principle of Mobile WiMAX

Working principle of mobile WiMAX is based on MIMO and OFDMA, which are described here:

Multiple inputs multiple output (MIMO)

The effective development of wireless communication sets for the system capacity and frequency band efficiency. There have been various efforts to meet these requirements, such as the raising bandwidth of the system, optimising modulation mode or adopting a complex Code Division Multiple Access system. After all, the application of these methods is restrictive. Officially, neither the expansion of bandwidth nor the enhancement of modulation order is limitless, and the channels of complex Code Division Multiple Access system are not orthogonal to each other perfectly. The Multiple Input Multiple Output (MIMO) systems was nascent at the right moment, by using Space Time Coding technology, it realises space division multiplexing using the multi-element array, which greatly improves the frequency band efficiency within the limited bandwidth.

The Multiple Input Multiple Output (MIMO) using multiple antennae at the transmitting and receiving terminals respectively. The signals are transmitted and received by multiple antennae at the transmitting and receiving terminals, and accordingly the quality of service (QoS) is improved for each end user. Compared with the traditional single-element system, MIMO technology easily improves the unitization rate of the frequency band, which allows the system to transmit data with higher speed under limited bandwidth. The block diagram of MIMO system with N transmitting antennae and M receiving antennae was shown in Figure 3.

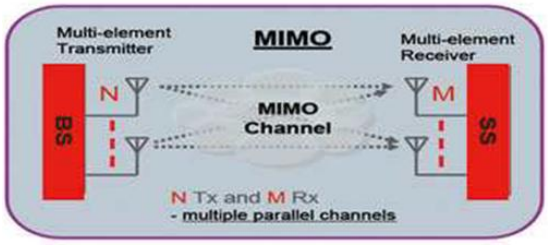

Figure 3: Architecture of MIMO system

WiMAX802.16e defines three types of MIMO. They are Space-time Transmit Diversity (STTD), Spatial Multiplexing (SM) and adaptive switching. It also has three coding matrix: Matrix A, Matrix B and Matrix C.

Orthogonal Frequency Division Multiple Access (OFDMA)

The OFDMA system divides the transmission bandwidth into a series of orthogonal sub-carrier (as the name implies OFDMA) sets without overlap, and allocates these sub-carrier sets to the different operator to realise the multiple-access. The Orthogonal Frequency Division Multiple Access (OFDMA) system allocates the bandwidth resources available to users in demand, which realises the optimized utilisation of system resources easily. As different operators occupy non-overlapped subcarrier sets, there is no interference between users in case of ideal synchronization, i.e., no Multiple Access Interference (MAI). The figure at right gives the sketch map of The OFDMA system, where the grey, white and dark grey time-frequency trellis represents different sub-carrier sets which do not overlap on the frequency band and allocated to different users. Orthogonal Frequency Division Multiple Access (OFDMA) solutions is considered as partitions total resources including time and bandwidth on the frequency to realise the multiuser access.

Sub-Channel OFDMA

The sub-channel Orthogonal Frequency Division Multiple Access (OFDMA) partitions the bandwidth of the entire Orthogonal Frequency Division Multiple Access system into several OFDMA sub-channels and each sub-channel has several sub-carriers allocated to an operator, and each user may occupy more than one sub-channel.

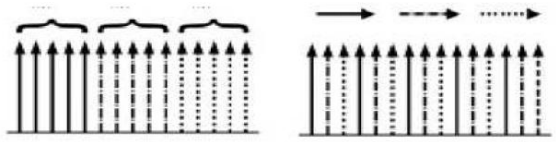

Figure 4: Sub-channel of OFDMA

Function of mobile WiMAX with MIMO and OFDMA

In the WiMAX 802.16e system, MIMO and OFDMA both are combined to improve the network coverage and redouble the WIMAX system capacity. Accordingly, the costs of network construction and maintenance are reduced greatly, which promotes the development of mobile WiMAX. MIMO is applicable for all wireless communication technologies. In the WiMAX802.16e system, the perfect combination of MIMO and OFDMA embodies the technical advantages of MIMO better. The MIMO system has the capacity of anti-multipath fading, but it cannot do anything about the selective fading of frequency. Other communication systems adopt equalisation technique to solve this problem in the MIMO system. The OFDMA of WiMAX conquers the selective fading of frequency successfully. The next generation of mobile communication system requires technologies with higher frequency band utilisation rate, but the ability of OFDMA to improve the frequency band utilisation rate is limited after all. Combined with the MIMO, the frequency band efficiency has further improved without increasing the bandwidth of the system. The MIMO + OFDMA technology not only offers higher data transmission speed but also achieves strong reliability and stability of the system by diversity.

Application

Network Coverage Ability Because of the higher frequency range, the transmission loss of WiMAX802.16e is much higher than other mobile communication systems. Expand the network coverage is a challenge to WiMAX. The advantage of MIMO technology in the WiMAX system greatly improves the network service coverage. In the diversity mode, MIMO enhancing the coverage radius of residential areas by diversity gain. In the multiplexing mode, it enhancing the coverage radius by diversity gain obtained from the increase of speed at the edges of the residential area. In the adaptive switching mode, the edges of residential area work in diversity mode, and the coverage gain is identical to that of diversity mode.

System Capacity

The WiMAX802.16e system provides very high data throughput and mobility, which keeps the users on-line at any time. The users can experience the right broadband service even if they are moving. In the multiplexing mode, the MIMO technology multiplies the system throughput and frequency band efficiency and also multiplies the peak speed of a single user. In the diversity mode, the system throughput and the frequency band efficiency are improved by raising the proportion of High-Order Modulation (HOM). In the adaptive switching mode, the centre of residential area works in multiplexing mode, and the edges work in diversity mode.

1.11.2.3 Applications

Content-Based Distribution

This type of routeing scheme is a service-oriented communication technique. In this scheme, the sender of a message does not need to explicitly specify its destination. The third layer (network layer) of OSI reference model will automatically deliver the message to receivers that are interested in the message.

Internet Access

Undoubtedly, Internet access will still be the major request in WiMAX networks, especially when they are initially deployed. To support Internet access, a basic method is to provide a unicast link between Subscriber station and the Base Station, which has the link toward.

Quality Guaranteed Applications

For many applications in WiMAX network, the network layer should provide a sufficient quality of service (QoS) guarantee, normally regarding of bandwidth, data rate, delay, and delay jitter. However, wireless communications are indeed error-prone. Thus it is difficult to provide such an assurance in a wireless network.

Group Communications

Since WiMAX networks can cover a relatively large area, it is usual to think that many group communications, such as video-conferences, will be essential in WiMAX networks. Multicast is the key technology to support such kind of communication scenarios. In WiMAX network, however, since all nodes are located inside, performing such group communication becomes possible.

Multi-servicing Applications

In WiMAX, multi-servicing is a technology that can provide services similar to those of multipath routing. The main difference between these two techniques is that in multi servicing, one subscriber station has two or more IP addresses and generally has the same number of interfaces. Thus, the station can have multiple paths to access the same resources. In brief, the last layer of OSI reference model (i.e. application layer) requirements must be addressed in the network layer design.

Metropolitan Area Distributed Service

With the deployment of mobile WiMAX networks, more and more value-added services can be provided in a MAN area to efficiently support a huge number of customers, distributed services can be enabled. In other words, an end user can access the service from any of the servers in the network in which these servers are distributed to serve the entire metropolitan area.

2. WIMAX FORUM

WIMAX Forum is a (not- profit organization) which has thousands of members, comprising most of the WiMAX network operators, component vendors and equipment vendors. It was established in Jun. 2001 and certifies wireless broadband equipment based on the IEEE802.16 and support ETSI Hiper-MAN (European Telecommunications Standards Institute High-Performance Metropolitan Area Networks) by awarding equipment manufacturers' products with the WiMAX Forum Certified' label (Worldwide Interoperability for Microwave Access). We can discuss three function areas of development within the WiMAX Forum. Show in fig. 5.

Air interface Specification: focus on the first and second layer of OSI reference model are based on IEEE 802.16.

Network Specification: apply to the upper layers and are not based on IEEE802.16 but developed within the WiMAX forum.

Roaming Specification: deal with the roaming business framework with a function for whole sale rating.

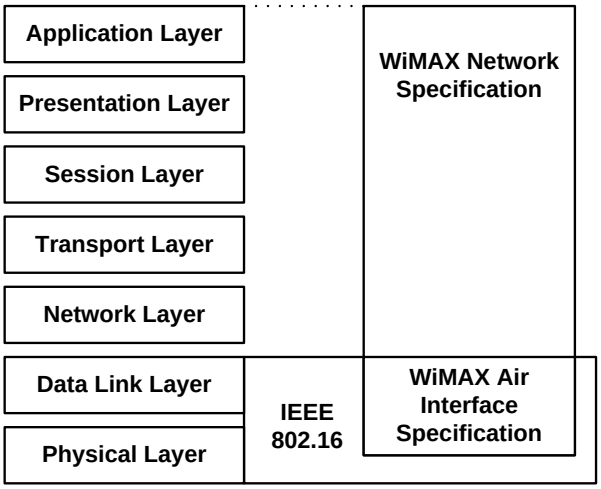

Figure 5: Relationship between IEEE802.16 and WIMAX, on the OSI reference model

2.1 Benefits of Certification

A vendor can make a system with a different subset of the IEEE 802.16 standard or even with the same subset but neglect to certify his products by the WiMAX Forum. Thus, if the vendor etc. other wants to use the 'WiMAX Forum Certified' label for its product, it requires permission of the Forum, to prevent legal proceedings for trademark infringement. The WiMAX Forum only grants this permission of their logo, if the vendor's product is certified by the WiMAX Forum [7]. Therefore, the vendors themselves are willing to certify their products to obtain this label, without any external obligation as this has many benefits for vendors, network operators and end users [18].

2.1.1 Vendors Benefits:

Improvement in cost: specialisation in the specific component can lead to lower-cost modules which can be integrated into the vendor's devices.

Innovation faster: there is no need to focus on a complete end-to-end product line, as with proprietary broadband wireless access systems. Vendors can specialize in specific components, allowing faster development cycles.

Easier and fastest targeting of the global market: it provides easier and fastest targeting of global market by using certification label which has a worldwide reputation.

Easy and fast Troubleshooting: due to easy troubleshooting, Interoperability problem detection before commercialization.

2.1.2 Network operators Benefits:

Easy Support of any subscriber device: all certified end devices are instantly supported, as well as roaming support for end devices that originate from another network operator, with the same certification profile.

Fast Backward compatibility: certified products are guaranteed to be backward compatible.

Fast and easy deployments: there is no vendor lock-in, and a multivendor network can be deployed in a more cost efficient and faster way**.**

2.1.3 End users Benefits:

Faster User mobility with the visited network: it has the faster user mobility with the visited network because they use the same device when switching to or roaming on the network of another network operator.

Increased end user confidence: the certified product will certainly work with any network operator that uses certified products, with the same certification profile, so it increases the confidence of end user.

2.2 WiMAX Profiles

Based on the IEEE 802.16 and ETSI Hiper MAN standards, the WiMAX Forum developed system profiles, which define mandatory and optional capabilities for WiMAX products. The number of features that are mandatory and optional in the standards may be tested by the WiMAX Forum Certified TM program, but does not include any new feature that is not included in the standards [7]. Within the WiMAX Forum, there is currently two system profiles: the first system profile that are based on IEEE Std 802.16-2004 known as the Fixed WiMAX, using the Wireless MAN-OFDM physical layer specifications with 256 carriers, and Second WiMAX system profile that are based on the IEEE Std 802.16e-2005 known as the Mobile WiMAX, it using the Wireless MAN-OFDMA physical layer specifications. Table 2 show some key ieee std 802.16-2009 parameters values and the Subset of values that are mandatory in mobile WiMAX Release 1.5, indicated in bold

Table 2: Some key IEEE STD 802.16-2009 parameters values and the Subset of values that are mandatory in mobile WiMAX Release 1.5

PARAMETER	IEEE STD 802.16-2009 AND MOBILE WIMAX RELEASE 1.5 VALUES
Air interface	Wireless MAN-SC, Wireless MAN-OFDM, **Wireless MAN-OFDMA**, Wireless HUMAN
Cyclic prefix	1/4, 1/8, 1/16, 1/32,1/64
Frame length [ms]	2, 2.5, 4, 5, 8, 10, 12.5, 20
Convolutional code	Tail biting, Zero tail
Downlink modulation	**QPSK, 16-QAM, 64-QAM**
Uplink modulation	**QPSK, 16-QAM, 64-QAM**

3. RELATED WORK

In 2007, J. D. Kenneth al. discussed [12], To understand the working of WiMAX system and the role of various parameters on the system performance, the simulation model of WiMAX physical layer using MatLab 7.5 version has been developed. Jagdish D. Keneet al. define Efforts are taken to understand the effect of various Modulation techniques, Coding rates, cyclic prefix factors and FFT size on the system performance. From the simulation results analysis conclude that BPSK modulation consumes less signal power (4dB) compared to higher ordered 64 QAM (20.5dB) modulations. Hence system performance is optimised with adaptive modulation. For good propagation conditions, a high order modulation scheme with low coding redundancy such as 64 QAM is used to increase the transmission data rate. During fading signal, the system selects an energy efficient modulation scheme such as BPSK or QPSK. BPSK or QPSK making efficient use of the bandwidth and increases overall

system capacity. In addition, higher values of cyclic prefix factor help to improve the signal strength up to 7.9dB for QPSK ¾ modulation scheme. Apart from 256, the higher size of FFT can also be chosen to upgrade the performance of the system in concern with system complexity.

In 2008, K. Etemad al. discussed [1], this paper provides a review of mobile WiMAX technology and its evolution from both radio and network perspectives. The technology utilises advanced PHY and MAC techniques in radio to provide high spectrum efficiency and QoS control as well as IP-based flat network architecture supporting multivendor plug and play deployments. Mobile WiMAX has defined the technology evolution roadmap for the next few years, which includes, but goes beyond, further improvements in system efficiency and user experience.

In2008, P. Taaghol, et al. discussed [17], the authors describe, the wireless industry makes its way to the next generation of mobile systems, in which it describe important of enabling the seamless integration of emerging 4G access technologies within the currently deployed or evolved 2G/3G infrastructures. In this paper the authors address a specific case of such a seamless integration that of mobile WiMAX in evolved 3GPP networks. In this article, they investigate the architecture and the key procedures that enable this integration, and they also introduce a novel handover mechanism that enables seamless mobility between legacy 3GPP access, and mobile WiMAX such as UTRAN or GERAN. The main features of this novel handover mechanism are that subscriber station does not need to support simultaneous transmission on both 3GPP accesses and WiMAX; therefore, it mitigates the RF coexistence issues that exist otherwise and improves handover performance.

In 2010, K. Etemad, et. al. discussed [16], in this paper the author define Introduction of WiMAX with its Basic Network Reference Model and its component and WiMAX Network Roadmap: different release (1.0, 1.5, 1.6, 2.0), Overview of Major Features in Release 1.0, Overview of Major Features in Release 1.5, Major Features in Network Release 1.6, Comparison of Mobile WiMAX and 3GPP/SAE Network Architecture.

In 2011, S. Tang discussed [15], the authors describe they propose an analytic model using WiMAX as backhaul support for Wi-Fi traffic and evaluate the system performance. One unique feature is that the Wi-Fi traffic completely reflects the realistic user behaviour. The author also describes how Wi-Fi user may be overflowed to its overlaid WiMAX cell when it is rejected at the Wi-Fi cell. In which the Wi-Fi user may also work for some time duration in the Wi-Fi cell and then make a vertical handoff to its overlaid WiMAX cell when it needs to move from its current Wi-Fi cell (e.g., office) to its target Wi-Fi cell (e.g., airport). The target Wi-Fi cell may be located at another place in the same WiMAX cell, or at a different WiMAX cell.

In 2012, Khokhar al. discussed [14], In this paper use of cognitive radio network composed of wireless devices able to opportunistically access the shred radio resource. The core of such networking paradigm has the capability of cognitive radio to monitor band occupation to exploit band holes for the transition. In this extensive simulations are conducted under MATLAB and analysis the performance of our routing protocol with Ad-hoc On Demand Distance Vector (AODV) for Mobile WiMAX environment. The proposed algorithm shows high throughput, reduce end to end delay, and increase packet delivery ratio. Successfully results found that on an average CRN perform better than AODV. It has a less average end to end delay. However, for other metrics (packet delivery ration and throughput), AODV demonstrate poor performance.

In 2014, P. Dattaet et al. discussed [13], A detailed analysis of different 4G technologies, *e.g.* WiMAX and LTE network is presented in this paper. The author also presents a discussion about the architecture of LTE network and various issues faced in LTE technology. Successfully results found that LTE is advantageous over WiMAX in every aspect. In LTE architecture consists of two networks- the access network, *i.e.*, E-UTRAN network and the core network, *i.e.*, EPC network. In which author also discussed some challenging issues for research in LTE networks.

In 2014, V. j Singh et al. discussed [4],in this author concentrate on the physical layer threats (i.e. scrambling and jamming), MAC layer threats (i.e. user authentication and data confidentiality) and routing layer threats (i.e. black-hole attack and other miscellaneous attacks e.g. Man-in-th e-Middle (MITM), Denial of Service (DoS) and Bandwidth Spoofing). In this paper author observed that eavesdropping of management messages jamming attack are the most destructive attacks on WiMAX network. Successfully results found that like other wireless networks, WiMAX network is also uncovered to many of the security flaws at both the protocol layers i.e. Physical Layer and MAC Layer. This survey paper categorises the security threats related to the WIMAX and presents them along with the proposed solutions for the ease of new researchers.

4. CHALLENGES & SECURITY OF MOBILE WIMAX

4.1 Challenges

There are various challenges of WiMAX which are defined here:

***Confidentially*:** Confidentiality is essential to ensure that important information is well protected and not revealed to unauthorized third parties. The objective of confidentiality is required in a mobile WiMAX network environment to protect information moving between different stations, since an opponent having the appropriate equipment may eavesdrop on the communication.

***Authentication*:** As in traditional systems, authentication techniques verify the identity of the users in communication, thus distinguishing legitimate users from the attacker.

***Integrity*:** By integrity, we mean that there is a risk that information could be modified when transferred over insecure networks. Lack of integrity could result in various problems, because the consequences of using inaccurate or incomplete information could be harmful. Integrity controls must be implemented to ensure that information will not be modified in any unexpected manner.

***Availability*:** Availability will be a major security issue in a wireless network since an attacker can launch a malicious attack to block a legitimate user's access to the network.

4.2 Layer Architecture and Security

To understand WiMAX related security issues, we first need to understand WiMAX architecture, its component and how securities specifications are addressed in WiMAX. In this section we describe the layer architecture of mobile WiMAX show in fig. 4 and security &security attacks.

***IEEE 802.16 protocol architecture*:** The WiMAX protocol architecture is divided into two layers: the Medium Access Control (MAC) layer and the Physical (PHY) layer, as brief discussion in the fig. 6. [9]

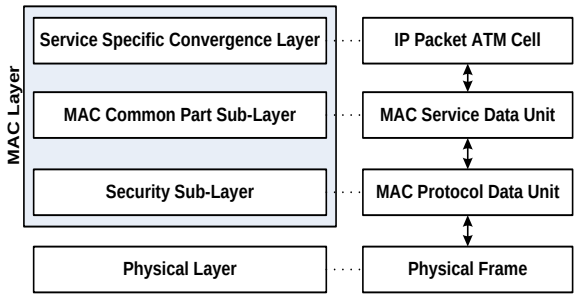

Figure 6: IEEE 802.16 protocol architecture

MAC layer consists of three sub-layers: [4, 9]

- Service Specific Convergence Sub-layer (CS)
- Common Part Sub-layer (CPS)
- Security Sub-layer

Service Specific Convergence Layer (CS): Service-specific convergence layer is first sub-layer in MAC layer. Which maps higher level data services to MAC layer service flow and connections.

Common Part Sub-layer (CPS): This common part sub-layer (CPS) is the base of the standards and it is tightly integrated with the security sub-layer. It also defines the rules and mechanisms for bandwidth allocation, system access and connection management. The Media Access Control (MAC) protocol data units are designed in common part sublayer.

Security Sub-layer: Security Sub-layer which lies between the Media Access Control (MAC), Common Part Sub-layer (CPS), and the Physical layer, addressing the authentication, encryption, key establishment and exchange, and decryption of data exchanged between Media Access Control (MAC), and Physical layers.

Physical Layer: In IEEE 802.16 Protocol architecture, the Physical layer provided a two-way mapping between Media Access Control protocol data units and the Physical layer frames received and transmitted through coding and modulation of radio frequency signals.

The WiMAX network, which is based on the IEEE 802.16e standard, In which, most of security issues are addressed and handled in the MAC layer, and it also provides strong support for authentication, control and management of plain text protection, key management, encryption and decryption, and security protocol optimization security sub-layer. Fig.7 show all the security specification related to IEEE802.16 standard.

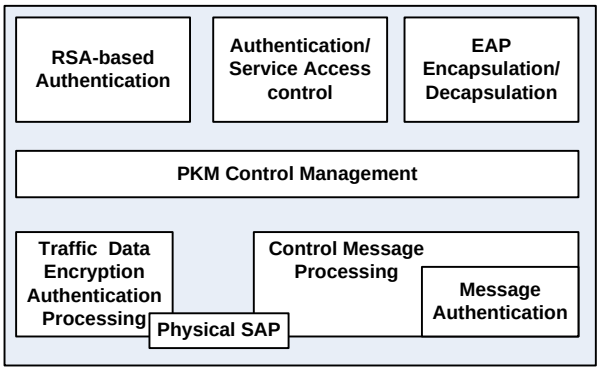

Figure 7: IEEE 802.16 MAC security sub-layer

Security sub-layer applies three steps to support WiMAX security [4].

1. ***Subscriber Authentication*** (At the time of entry in the network)
2. ***subscriber Authorization*** (if the subscriber is provisioned by the NSP)
3. **Encryption** (for the secure key exchange and data traffic)

Component protocol at security sub-layer guarantees the authorization and confidentiality at the time of link establishment between the authorized parties (service provider and subscriber). Two main entities in WiMAX, including Base Station (BS) and Subscriber Station (SS), are protected by the following WiMAX security features:

a) ***Security association* [4, 9]:** the first security feature of WiMAX is SA, which has its own identifier (SAID) and also contains a cryptographic suite identifier (for selected algorithms), initialization vectors and traffic encryption keys (TEKs).

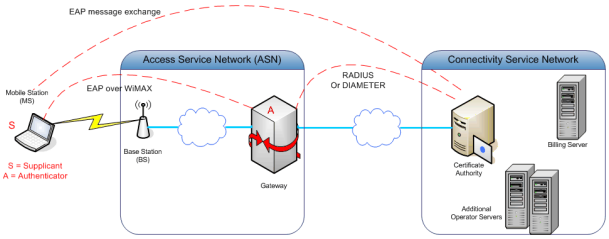

Figure 8: EAP based authentication [9]

b) ***Public key infrastructure:*** WiMAX uses the Privacy and Key Management Protocol (PKM) in public key infrastructure for secure key management, transfer and exchange between mobile stations, and also authenticates a Subscriber Station to a Base Station. The PKM protocol uses X.509 digital certificates, a strong encryption algorithm Advanced Encryption Standard (AES) and RSA (Rivest-Shamir-Adleman) public-key algorithm. The starting version of WiMAX uses Public key infrastructure -version1 (PKM-Vi), in which it provide one-way authentication method and has a risk for Man-In-The-Middle (MITM) attack. To deal with this type of issue, in the latest version (802.16e) mobile WiMAX, the PKMv2 was used to provide the two-way authentication mechanism.

c) ***Device/User Authentication:*** WiMAX supports three types of authentication which are handled in the security sub-layer.

RSA-based authentication: This applies X.509 certificates together with RSA encryption.

EAP (Extensive Authentication Protocol): The network operator can select three types of EAP.

- EAP-AKA (Authentication and Key Agreement)
- EAP-TLS (Transport Layer Security)
- EAP-TTLS MS-CHAP v2 (Tunneled Transport Layer Security with Microsoft Challenge-Handshake Authentication PV2).

The security sub-layer supports is the RSA-based authentication followed by EAP authentication.

d) ***Data privacy and integrity:*** WiMAX uses the AES algorithm for encryption. V. Kumar, J. Walker et. al. [2, 4, 9], is deeply described this section in WiMAX security threats and solution are not describe here, to know more about it paper [9][3][2][6][4] presented more detailed about it.

5. CONCLUSION

In this paper, we can do a systematic investigation of WiMAX and its standards, development, technology, and security. WiMAX techniques and its security issues. Mobile WiMAX is next generation technology it could facilitate new deployments and developments that can offer the best opportunities to telecom operators. The mobile WiMAX utilize advanced PHY and MAC technique in radio to provide high spectrum efficiency and QoS(quality of service) control. A wireless network system makes the use of an open and insecure radio channel with different kind of security issues (traffic confidentially, integrity) and network attack .Security plays an important role in performance &reliability of a network. In our future work, we focus on QoS of different routing protocol for WiMAX network by using a different parameter.

6. REFERENCES

[1] K. Etemad, Intel Corporation," Over View of Mobile WIMAX Technology and Evolution" IEEE Communication Magazine Oct 2008.

[2] D. Johnston, J .Walker," Over view of IEEE 802.16 security & privacy", IEEE, 2004, PP, 40-48.

[3] H. Yang, K. Alimgeer, "improved secure network authentication protocol for IEEE 802.16",the international conference on information and communication technologies (ICICT'09), IEEE, 2009. PP-101 – 105.

[4] V. K Jatav, V.J Singh," Mobile WiMAX network security threat and solution: A survey", 2014 5th international conference on computer and communication technology.

[5] Web Site: Http://enwikipedia.corg/wiki/ WIMAX.

[6] D. kene , D.kulat, Jagdish , "Performance evaluation of IEEE 802.16e WIMAX physical layer", institute of technology ,NIRMA University, AHEMDABAD 382481, 08-10 DEC.2011.

[7] D. Pareit, B. Lannoo, J. Moerman," The history of WIMAX: A complete survey in certification and standardization for IEEE 802.16 and WiMAX". IEEE communication surveys & tutorials, Vol 14, No. 4 fourth quarter 2012.

[8] Web Site: https://www.tutorialspoint.com/ WIMAX/index.html

[9] Web Site: http://www.cs.wustl.edu/~jain/cse571-09/ftp/ WIMAX2/index.html#Bogdanoski08

[10] B. Li, Y. Qin and C. Ping Low, Choon Lim Gwee," A Survey on Mobile WIMAX", IEEE Communications Magazine ,December 2007

[11] IEEE 802.16-2004, "Local and Metropolitan Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems," 2004.

[12] M Azizul Hasan, "Performance Analysis of WIMAX/IEEE 802.16 OFDM Physical Layer" , Helsinki University of Technology, Finland 2007.

[13] P. Dattaet et al. presented [13]," Exploration and Comparison of Different 4G Technologies Implementations: A Survey", 2014 RAECS UIET Panjab University Chandigarh, 06-08 March, 2014.

[14] R. Hafeez Khokhar al. presented [12] ,"On QoS Routing in Mobile WIMAX Cognitive Radio Networks" , International Conference on Computer and Communication Engineering (ICCCE 2012), 3-5 July 2012, Kuala Lumpur, Malaysia.

[15] S.Tang," Performance analysis of an integrated wireless network using WIMAX as backhaul support for WiFi traffic", Ieee, Military Communications Conference, 2011 - Milcom .

[16] K..Lai, M, Etemad ,"Overview of WiMAX Network Architecture and Evolution", Wiley-IEEE Press, WIMAX Technology and Network Evolution,2010

[17] P.Taaghol,; Salkintzis, A.K.; Iyer, J.,"Seamless integration of mobile WIMAX in 3GPP networks", IEEE, Communications Magazine, IEEE,2008

[18] R. Prasad and F. J. Velez," WiMAX Networks - Techno-Economic vision and challenges", Springer, 2010, no. ISBN 978-90-481-8751-5.