CHAPTER 1

INTRODUCTION

Wireless networking is a promising technology that allows users to access a broad range of information and applications. Mobile communications services pierces into our society at an explosive growth rate (David Tse & Pramod Viswanath 2005). Achieving communication services at anytime, anywhere is considered as the evolution of communication technologies from wired to wireless with the miniaturization of devices (Hakima Chaouchi et al 2009). Wireless networks originated many applications that are benefited from the features like mobility and higher reliability.

Four resources used for wireless communications are radio, microwave, satellite and free space optics. The selection among these means depends on communications technologies, network elements and desired frequency spectrums for communications. Radio Frequency (RF) based technologies have progressed from analog systems to digital systems and from voice to data communications. The main development in wireless was the cellular mobile networking and application which was used to support voice communications. The next was radio-based fixed wireless technologies such as Wireless Local (WLAN)/Personal (WPAN)/Metropolitan Area Networks (WMAN) and near-field sensor networks developed to support data communications (Wale Soyinka 2010). The best achievement in the history of wireless and the evolution of wireless access technologies is at its fourth generation (4G) which was developed in a short span of time. Glancing past, wireless access technologies have followed different evolutionary paths aimed
to achieve high performance and efficiency in mobile communication (Harte 2006).

1.1 EVOLUTION OF CELLULAR WIRELESS NETWORKS

Cellular wireless network technology has been budding for the last three decades through different generations. Each new generation adds new capabilities to make the network more attractive to the users. Four generations of cellular wireless networks are popularly referred as 1G, 2G, 2.5G and 3G, respectively (Smith & Collins 2007). The important networks belonging to each of these generations will be described in this section.

First generation (1G)

These networks were solely for voice communication and employed Frequency Division Multiple Access (FDMA). The best known 1G system was the Advanced Mobile Phone System (AMPS) that was invented at Bell labs in the USA and was first established in 1982. Although it was voice-only wireless network, it had incorporated much of the cellular network concepts. However, it is now almost obsolete and was replaced by its Second Generation (2G) version called Digital AMPS (D-AMPS).

Second Generation (2G)

2G networks were also designed for voice communication but it incorporated digital technology rather than analog technology. A 2G cell phone converts the input analog voice signal into a digital format before its transmission into the free space. Most of today’s cellular providers like Interim standard 136(IS-136), Global System for Mobile communication (GSM) and first Code Division Multiple Access (CDMA) based cellular standard named IS-95 use 2G technology (Todor Cooklev 2004).
2.5 Generation (2.5G)

The broadly used 2G systems were mainly designed for digital voice communication. They were unable to provide adequate data communication services and hence internet services. On the other hand, the proposed 3G standard would take a long time to develop and be deployable. At this instant, many companies designed interim protocols and standards to provide data communication services over the existing 2G infrastructure. Such systems are jointly recognized as the 2.5G cellular system (Smith & Collins 2007) and some of them are General Packet Radio Service (GPRS), Enhanced Data Rate for Global Evolution (EDGE), CDMA 2000 Phase 1 (Andrews et al 2007).

Third generation (3G)

The objective of 3G cellular system is to afford both telephone and data services at drastically higher speeds compared to 2G systems. The data speeds are 144 Kbps driving speeds, 384 Kbps walking speeds and 2 Mbps for indoors. The major standards developed in 3G are Universal Mobile Telecommunication Services (UMTS) and CDMA 2000 (Kaaranen 2005, Eric Dahlman 2008).

Fourth Generation (4G)

Even though 3G networks are not fully deployed, effort on the design of 4G wireless networks has also started blooming (Garg 2007 and Zhang et al 2012). Important features of 4G systems include mobile internet with multimedia, anytime anywhere internet connectivity, highest possible data rate, seamless integration with wired IP networks, automatic and transparent switching from one access technology to another, support of real time voice and video over IP, automatic discovery of user location by the network, etc. The technologies on which the attentions are focussed on achieving the goals
set forward in 4G (Muntean & Otesteanu 2010, Mustafa Ergen 2009) are the Worldwide Interoperability for Microwave Access (WiMAX) and the Long Term Evolution (LTE).

Exponential growth of cellular telephone use and wireless internet access has led to great buoyancy about wireless technologies in general (David Tse & Pramod 2005). Obviously not all wireless technologies had flourished and there are also examples of failures such as first generation cellular LAN, Iridium satellite system, wide area data service Metricom and fixed wireless cable to home. It is more important to update the technology according to the requirement of users more than developing a new technology. At present, WiMAX is developed in the same motive of enhancing it according to the needs of users. WiMAX is ahead of other technologies, since it operates similar to Wi-Fi but at higher speeds, over larger distances and for a greater number of users. WiMAX could potentially obliterate the suburban and rural blackout areas that currently have no broadband Internet access.

1.2 WIMAX NETWORK

1.2.1 Overview of WiMAX

The global boom in the number of users of the Internet has led to the development of different fixed and mobile broadband technologies providing support for high speed streaming multimedia, customized personalized services, ubiquitous coverage and unhampered Quality of Service (QoS). Though the existing Wireless Local Area Network (WLAN) and third generation (3G) technologies have been providing broadband access for the last several years, they have their own drawbacks. The culmination of the recent IEEE 802.16 WiMAX standards for WMAN has filled the gap between the LAN and Wide Area Network (WAN) technologies. Devised as a truly broadband access solution, the WiMAX technology offers promising features
in terms of high bandwidth, extended coverage area and low cost (Bo Li et al 2007).

This has led to its rapid rise as one of the most popular broadband access technologies and as a component in 4G networks. The Orthogonal Frequency Division Multiplexing (OFDM) based IEEE 802.16d technology provides fixed broadband access within a Metropolitan Area Network (MAN). The new mobile air interfaces specified in the IEEE 802.16e has successfully addressed the requirements for higher data rates and spectral efficiencies. An IEEE 802.16e-based Base Station (BS) can support both fixed and mobile broadband wireless access (Fan Wang et al 2008). WiMAX network architecture has the major features like Security, Mobility and Handovers, Scalability, Coverage & Operator Selection, Multi-Vendor Interoperability and Interworking with other Networks

1.2.2 IEEE WiMAX Standards

Currently, the WiMAX Forum has two different system profiles: one is based on IEEE 802.16-2004, OFDM Physical (PHY) layer, called the fixed system profile and the other one is based on IEEE 802.16e-2005 Scalable Orthogonal Frequency Division Multiple Access (SOFDMA) PHY, called the mobility system profile (Andrews et al 2007). Hence, IEEE 802.16 is a collection of standards, but not one single interoperable standard are listed in Table 1.2 and initial standards are briefed below.

IEEE 802.16a:

The IEEE 802.16 group subsequently produced 802.16a, an amendment to the standard, to include Non-Line-of-Sight (NLOS) applications in the 2-11 GHz band instead of LOS 2-66 GHz. The significant difference between these two frequency bands lies in the ability to support
NLOS operation in the lower frequencies, something that is not possible in higher frequency bands. It introduced major changes to the PHY layer specification as compared to the upper frequency, as well as significant Media Access Control (MAC) layer enhancements with a support for Orthogonal Frequency Division Multiple Access (OFDMA) were also included.

Table 1.1 Different standards of WiMAX

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.16-2001</td>
<td>Fixed Broadband Wireless Access (BWA) for 10–66 GHz</td>
</tr>
<tr>
<td>802.16.2-2001</td>
<td>Recommended practice for coexistence</td>
</tr>
<tr>
<td>802.16c-2002</td>
<td>System profiles for 10–66 GHz</td>
</tr>
<tr>
<td>802.16a-2003</td>
<td>Physical layer and MAC definitions for 2–11 GHz</td>
</tr>
<tr>
<td>802.16-2004</td>
<td>Air Interface for Fixed BWA System(Merged version of 802.16-2001, 802.16a, 802.16c and P802.16d)</td>
</tr>
<tr>
<td>802.16.2-2004</td>
<td>Recommended practice for coexistence (Maintenance and rollup of 802.16.2-2001 and P802.16.2a)</td>
</tr>
<tr>
<td>802.16f-2005</td>
<td>Management Information Base (MIB) for 802.16-2004</td>
</tr>
<tr>
<td>802.16e-2005</td>
<td>Mobile BWA System</td>
</tr>
<tr>
<td>802.16k-2007</td>
<td>Bridging of 802.16(an amendment to IEEE 802.1d)</td>
</tr>
<tr>
<td>802.16g-2007</td>
<td>Management Plane Procedures and Services</td>
</tr>
<tr>
<td>802.16-2009</td>
<td>Air Interface for Fixed and Mobile BWA System (Merged version of 802.16-2004, 802.16e/f/g and P802.16i)</td>
</tr>
<tr>
<td>802.16j-2009</td>
<td>Multihop relay</td>
</tr>
<tr>
<td>802.16h-2010</td>
<td>Improved Coexistence Mechanisms for License-Exempt Operation</td>
</tr>
<tr>
<td>802.16m-2011</td>
<td>Advanced Air Interface with data rates of 100 Mbps mobile and 1 Gbps fixed. Also known as Mobile WiMAX Release 2 or Wireless MAN-advanced.</td>
</tr>
<tr>
<td>P802.16n</td>
<td>Higher Reliability Networks</td>
</tr>
<tr>
<td>P802.16p</td>
<td>Enhancements to Support Machine-to-Machine Applications</td>
</tr>
</tbody>
</table>
IEEE 802.16-2004:

This standard was the first practical standard of the IEEE 802.16 family. It is popularly called as fixed WiMAX, the name of the industrial alliance for its production. It integrated all the previous standards and re-edited PHY and MAC layer contents to improve the system performance. The standard is specified to allow nomadicity, where users can access the service from various locations covered by the network (Loutfi Nuaymi 2007).

IEEE 802.16e:

In December 2005, the IEEE group completed and approved IEEE 802.16e-2005, an amendment to the IEEE 802.16-2004 standard that added mobility support. The IEEE 802.16e-2005 forms the basis for the WiMAX solution for nomadic and mobile applications and is often referred to as mobile WiMAX (Pareit et al 2012). Meanwhile, there have been several amendments to the IEEE 802.16 standard which are listed in table 1.1.

1.2.3 End-to-End WiMAX Network Architecture

The WiMAX Forum’s Network Working Group (NWG) is responsible for developing the end-to-end network requirements, architecture and protocols for WiMAX, using IEEE 802.16e-2005 as the air interface (Pareit et al 2012). The network reference model envisions unified network architecture for supporting fixed, nomadic and mobile deployments and is based on an Internet Protocol (IP) service model. The network reference model developed by the WiMAX Forum NWG defines a number of functional entities and interfaces between those entities are shown in Figure 1.1 and is discussed briefly below.

- **Mobile station (MS):** used by the end user to access the network.
• **Base Station (BS):** The BS is responsible for providing the air interface to the MS. Additional functions such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, Dynamic Host Control Protocol (DHCP) proxy, key management, session management and multicast group management.

• **Access Service Network (ASN):** It comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.

• **Access Service Network Gateway (ASN-GW):** The ASN gateway typically acts as a layer 2 traffic aggregation points within an ASN. Additional functions include intra-ASN location management & paging, radio resource management & admission control, caching of subscriber profiles & encryption keys, QoS & policy enforcement and routing to the selected CSN. Typically the ASN includes numerous BSs with one or more ASN gateways and it interfaces the BS with the IP core network.

• **Connectivity Service Network (CSN):** The CSN provides connectivity to Internet, Application Service Provider (ASP), other public networks and corporate networks. The CSN performs core network functions including policy and admission control, IP address allocation, billing and settlement. The CSN is also responsible for internetworking with non-WiMAX network and for roaming through links to other CSNs. Communication between entities like BS, ASN and CSN is effectively by the links listed in Table 1.2.
Figure 1.1 WiMAX Architecture with interconnections

Table 1.2 Interfaces of Reference Network Model

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Interface between the MS and the ASN. Functionality: air interface.</td>
</tr>
<tr>
<td>R2</td>
<td>Interface between the MS and the CSN. Functionality: Adaptive Antenna Polarity (AAP), IP host configuration, mobility management.</td>
</tr>
<tr>
<td>R3</td>
<td>Interface between the ASN and the CSN. Functionality: AAP, policy enforcement, mobility management.</td>
</tr>
<tr>
<td>R4</td>
<td>Interface between ASNs. Functionality: mobility management.</td>
</tr>
<tr>
<td>R5</td>
<td>Interface between CSNs. Functionality: internetworking, roaming.</td>
</tr>
<tr>
<td>R6</td>
<td>Interface between BS and ASN gateway. Functionality: IP tunnel management to establish and release MS connection.</td>
</tr>
<tr>
<td>R7</td>
<td>Interface between BSs. Functionality: handoffs</td>
</tr>
</tbody>
</table>
1.2.4 **The Protocol Layers of WiMAX**

The IEEE 802.16 BWA network standard applies the Open Systems Interconnection (OSI) network reference seven-layer model, also called the OSI seven-layer model.

![Diagram of the protocol layers of the 802.16 BWA Standard](image)

**Figure 1.2 Protocol layers of the 802.16 BWA Standard**

The protocol layers architecture defined in WiMAX/802.16 is shown in Figure 1.2. It depicts that the 802.16 standard defines only the two lowest layers, the Physical Layer and the MAC Layer. The MAC layer itself is made of three sub-layers, the Convergence Sublayer (CS), the Common Part Sublayer (CPS) and the Security sublayer. Each of these layers and their functions are described as follows:
Convergence Sublayer (CS): The service-specific Convergence Sublayer (CS), often simply known as the CS, is just above the MAC CPS sublayer. The CS uses the services provided by the MAC CPS, via the MAC Service Access Point (SAP). It Classifies and maps the MAC Service Data Units (MSDUs) into appropriate Connection Identifiers (CID). It delivers CS Protocol Data Units (PDUs) to the appropriate MAC SAP and receives CS PDUs from the peer entity.

Medium Access Control Common Part Sublayer (MAC CPS): The Common Part Sublayer (CPS) resides in the middle of the MAC layer. The CPS represents the core of the MAC protocol and is responsible for bandwidth allocation, connection establishment and maintenance of the connection. Security Sublayer: The MAC Sublayer also contains a separate security sublayer providing authentication, secure key exchange, encryption and integrity control across the BWA system (Ramjee Prasad & Fernando 2010).

Physical Layer: The PHY Layer establishes the physical connection between both sides in uplink and downlink two directions. The PHY Layer is responsible for transmission of the bit sequences and the PHY Service Access Point (SAP) is defined to allow a single MAC to control/support multiple PHY entities over a shared physical link. It defines the type of signal used, the kind of modulation and demodulation, the transmission power and also other physical characteristics.

Absence of mobility is a major drawback which acted as barrier for the commercial use of WiMAX technology. Since the design and layered architecture are based on fixed WiMAX, the additional features needed for adapting mobility in WiMAX have originated the roots of research works. Mobile WiMAX IEEE 802.16e is developed in such a way that the advancements should be incorporated without modifying the underlying architecture of WiMAX network.
1.3 MOBILE WIMAX

Mobile WiMAX is a broadband wireless solution that enables convergence of mobile and fixed broadband networks with flexible network architecture. The mobile WiMAX Air interface adopts SOFDMA for improved multi-path performance in NLOS environments. The Mobile WiMAX System profile enables mobile systems to be configured based on a common base feature set, which ensures baseline functionality for terminals and base stations that are fully interoperable.

Fixed WiMAX products are already deployed and functioning in most of the countries. The problem is that they can only propose a fixed wireless access up to 20 km. The processing requirements of the mobile WiMAX terminal are much greater than the fixed WiMAX device. Taking into account the range and the price points of the BS, it is evident that IEEE 802.16d is cost effective for fixed wireless applications. By calculating the cost to cover a square km, IEEE 802.16e BS is 12 to 2900 times more expensive than IEEE 802.16d BS. Inspite of these limitations, Mobile WiMAX is preferred over fixed WiMAX for the following reasons:

- Improves NLOS coverage by utilizing advanced antenna diversity schemes, and Hybrid Automatic Retransmission Request (HARQ)
- Supports Multicast and Broadcast Service (MBS)
- Increases system gain by the use of denser sub-channelization, thereby improving indoor penetration
- Introduces high-performance coding techniques such as Turbo Coding and Low-Density Parity Check (LDPC), enhancing security and NLOS performance
• Improves coverage by introducing Adaptive Antenna Systems (AAS) and Multiple Input Multiple Output (MIMO) technology

• Supports two modes for power efficient operation which are sleep mode and idle mode.

1.3.1 Comparison of WiMAX with 3G

As WiMAX is in the commercialization phase, its merits over existing 3G cellular technologies are listed as follows:

• Unlike 3G systems, which have a fixed channel bandwidth, WiMAX defines a scalable channel bandwidth from 1.25MHz to 20MHz, which allows for a very flexible deployment (Bacioccola et al 2010).

• The reliance of Wireless Fidelity (Wi-Fi) and WiMAX on OFDM modulation, as opposed to CDMA in 3G, allows them to support very high peak rates.

• WiMAX can achieve higher spectral efficiencies by accommodating multiple antennas compared to 3G systems.

• WiMAX support more symmetric links for flexible and dynamic adjustment of the downlink-to-uplink data rate ratios. Typically, 3G systems have a fixed asymmetric data rate ratio between downlink and uplink.

• WiMAX is cost effective because of its lightweight IP architecture compared to 3G which has a complex & separate core network for voice & data.
Table 1.3 provides a comparison of WiMAX with 3G technologies. Inspite of the advantages of WiMAX over other technologies, it is limited by following features:

- WiMAX capabilities are unproven in terms of supporting roaming and high-speed vehicular mobility, when compared to those of 3G. In 3G, mobility was an integral part of the design and WiMAX was designed as a fixed system, with mobility capabilities as an addon feature.

- Security sub layer can afford the security requirement of fixed WiMAX users but insufficient to the need of mobile WiMAX users.

At present, WiMAX occupies a relatively middle ground between Wi-Fi and 3G technologies in the key dimensions such as data rate, coverage, QoS, mobility and price. But WiMAX will overcome its issues and overtake the 3G cellular networks shortly. Security and Handoff are the topics of research interest which plays a vital role in the development of Mobile WiMAX are explained separately in the following sections. This thesis enhances the security and reduces the handoff delay to overcome the limitations of mobile WiMAX.
Table 1.3 Comparison of WiMAX with 3G and Wi-Fi

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Fixed WiMAX</th>
<th>Mobile WiMAX</th>
<th>HSPA</th>
<th>1xEV-DO Rev A</th>
<th>Wi-Fi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
<td>IEEE 802.16-2004</td>
<td>IEEE 802.16e-2005</td>
<td>3GPP Release 6</td>
<td>3GPP2</td>
<td>IEEE 802.11a/g/n</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Scalable 3.5, 7, 10 MHz</td>
<td>Scalable 3.5, 5, 7, 10MHz</td>
<td>5MHz</td>
<td>1.25MHz</td>
<td>20MHz</td>
</tr>
<tr>
<td>Multiplexing</td>
<td>TDM</td>
<td>TDM/OFDMA</td>
<td>TDM/CDMA</td>
<td>TDM/CDMA</td>
<td>CSMA</td>
</tr>
<tr>
<td>Duplexing</td>
<td>TDD, FDD</td>
<td>TDD initially</td>
<td>FDD</td>
<td>FDD</td>
<td>TDD</td>
</tr>
<tr>
<td>Frequency</td>
<td>3.5 GHz, 5.8 GHz</td>
<td>2.3 GHz, 2.5 GHz, 3.5 GHz</td>
<td>800/900/1800/1900/2100MHz</td>
<td>800/900/1800/1900MHz</td>
<td>2.4 GHz, 5GHz</td>
</tr>
<tr>
<td>Coverage</td>
<td>3-30 miles</td>
<td>&lt;2 miles</td>
<td>1-3 miles</td>
<td>1-3 miles</td>
<td>&lt;1000 ft</td>
</tr>
<tr>
<td>Mobility</td>
<td>No</td>
<td>Mid</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

1.3.2 Security Aspects

A wireless system uses an intrinsically open and insecure radio channel for transmission of user signalling and traffic between the BS and MS. As such, reliable & robust security and encryption procedures must be employed in order to protect confidentiality, privacy and integrity of user identity and data (Hakima Chaouchi et al 2009). The security sub layer is solely used for this purpose and it employs an authenticated client/server key management protocol in which the BS (the server) controls the distribution of keying material to the MS (the client). As shown in Figure 1.3, the privacy
function has two component protocols: (1) an encapsulation protocol for securing packet data across the network, and (2) a Key Management Protocol (PKM) providing the secure distribution of keying data from the BS to the MS. The MS and the BS can synchronize keying data via the key management protocol.

![Figure 1.3 WiMAX Security Sublayer](image)

The encryption algorithms applied in IEEE 802.16 for key exchange are Rivest Shamir Adleman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES) and Hashed Message Authentication Code (HMAC) & Cipher-based Message Authentication Code (CMAC). AES is the most widely and recommended algorithm of 802.16e security sub-layer as it performs stronger protection from theft of service and data across broadband wireless mobile network (William Stallings 2011 and Behrouz A. Forouzan & Debdeep Mukhopadhyay 2011).

Data encryption methods used for encrypting payload are Counter with Cipher block chaining MAC (CCM) -Mode AES, Electronic Code Book (ECB)-Mode AES, Cipher Block Chaining (CBC)-Mode AES, Counter (CTR)-Mode AES and AES Key-Wrap. Addition of security measures to the
existing fixed WiMAX to make secured mobile WiMAX is shown in Figure 1.4.

A Security Association (SA) is a set of security information parameters which is used to maintain the state of security relevant to a communication. Typically, it is shared between the BS and one or many of its client SS (to support multicast). By means of an SA, an SS will be authorized for a WiMAX service.

![IEEE 802.16d and IEEE 802.16e security features](image)

**Figure 1.4 IEEE 802.16d and IEEE 802.16e security features**

### 1.3.3 Handoff Aspects

Handoff occurs when a mobile user goes from one cell to another without the interruption of the ongoing session (a phone call, data session or other application). The handover can also be due to radio channel condition changes or cell capacity variations. The handoff process has two phases. In the first phase, the system detects the need for handoff and makes a decision to transition to another BS. In the second phase, the handoff is executed which ensures that the MS & the BS involved are synchronized and all packets are
delivered correctly by using appropriate protocols (Ramjee Prasad et al 2010). In 802.16e, the two known generic types of handoff are defined as follows:

- Hard handoff (HHO), also known as break-before-make: The MS stops its radio link with the old BS before establishing its radio link with the new BS. This is a simple handover which is mandatory in WiMAX.

- Soft handoff (SHO), also known as make-before-break: The MS establishes its radio link with a new BS before stopping its radio link with the old BS. The MS may have two or more links with two or more BSs, which gives the soft handover state. The soft handover is evidently faster than the hard handover and it is optional (Seok-Yee Tang et al 2010).

Two types of soft handoff in 802.16e are:

- Fast BS Switching (FBSS). This is a state where the MS may rapidly switch from one BS to another. The switch is fast because the MS makes it without realising the complete network entry procedure regarding the new BS.

- Macro Diversity Handoff (MDHO). Transmissions are between the MS and more than one BS.

Two SHO techniques are seen as very costly to build, deploy and maintain, especially in terms of capacity requirements on the air interface and backhaul connection. From the commercial standpoint, the primary advantages of the HHO scheme in Mobile WiMAX are the low deployment complexity and cost, requires very few BSs spaced appropriately apart. Some of the disadvantages of HHO are the delay in searching and selecting a target BS, non-negligible packet losses and prolonged connection
disruption time. The present research works aims at reducing handoff overheads, handoff delays, resource wastages and cell drops in case of full-mobility WiMAX.

1.4 RESEARCH CHALLENGES IN MOBILE WIMAX

Research issues emerged from 2004, as the WiMAX standard came into existence in that period (Yang Xiao 2007, Alexander Bachmutsky et al 2009). Promising growth of mobile WiMAX demands the need for solving the challenges faced which are grouped as follows:

QoS based Bandwidth allocation: As the number of mobile users increasing exponentially, bandwidth allocation assured by the service provider should be provided without violating the QoS policies (Kamran Etemad 2008, Delannoy et al 2010, Ahmadzadeh et al 2012, Ahmet Sekercioglu et al 2012).

Roaming: Roaming enables the service providers to extend services to the subscribers beyond their home networks. The WiMAX Forum Service Provider Working Group (SPWG) provides set of guidelines for roaming.

Internetworking with other technologies: The MS moves from/to a BS of WiMAX to/from a BS of other technologies like UMTS, 3G, Wi-Fi, etc. Internetworking with them requires a well defined structure in order to maintain the universal QoS, speed, security, etc. (Kaaranen 2005, Marc Ibrahim et al 2009)

In addition to this, Security and handoff require more attention as they attract the users towards the technology. This necessitated the separate discussion of their issues in detail.
1.4.1 Issues in Mobile WiMAX Security

Even after having a separate sub layer of security, threats which hurdle secured WiMAX are blooming day by day (Kim 2009). According to IEEE Standard 802.16-2001, MAC header and all MAC Management messages are not encrypted. In case of vulnerabilities in management messages, authentication will be exposed to eavesdropping, Man In The Middle (MITM) attacks, active attacks and replay attacks. In the latest IEEE 802.16e standard, the payload of MAC PDUs is encrypted with DES in the CBC mode or AES in the CCM mode (Sassan Ahmadi 2011). The attacker attacks with Radio Frequency (RF) channel for PHY layer threats.

Authentication: For MAC layer threats, the attackers spoof, modify and reply the MAC layer messages. The need for mutual authentication to maintain a secure connectivity between MS and BS is reported by Johnston & Walker (2004), Wongthavarawat (2005), Michel Barbeau & Jean-Marc Robert (2006), Sen Xu et al (2006), Deininger et al (2007), Taeshik Shon & Choi et al (2007) discussed the security issues and vulnerability in Mobile WiMAX with proposed solutions. Perumalraja Rengaraju et al (2009) discussed about MAC layer issues and the suitable solutions for each of them. Though MAC layer issues are addressed, they still suffers because of unauthenticated messages, unencrypted management communication, man-in-the-middle vulnerabilities, lack of data privacy and absence of mutual authentication. The initial network entry process should overcome Denial of Service (DoS)/Replay attacks during Mobile Station (MS) entering the network, the latency during handover and unsecured pre-authentication. Constantinos Kolias et al (2013) grouped the research issues of WiMAX and provided the methodologies to solve them.
*Power Saving:* Attacks against power saving mechanisms were also grouped as Signaling DoS Attack, Water Torture Attack and Sleep control header DoS Attack (Kim et al 2006, Lee et al 2007, Ibikunle 2009).

*Key management:* Key management struggles with attacks in key material exchange phase, impersonation attacks and confidentiality of key management details (Hasan et al 2009). Authentication process can be modified to use timestamps (synchronized clock time) and nonces (randomly generated Hexadecimal digits) in order to protect against simple replay attacks. An updated framework namely Wireless Public Key Infrastructure (WPKI) is introduced which adopts ECC instead of RSA in order to reduce the computation power substantially (Habib et al 2009). Traffic Encryption Key (TEK) identifier can be used to identify only four generations of TEK keys. It is stated that due to this fact it is straightforward for an attacker to inject or replay expired TEKs(Eren 2007, Mishra 2008, Fernandez 2008).

*Ranging process:* In addition to computational power, immune to attacks and the infeasibility of cryptanalysis are also required which are not focussed more. The utilization of Diffie-Hellman (DH) key exchange algorithm for the sensitive, protected process of initial network entry is discussed by Muhammad Sakibur Rahman et al (2009), Taeshik Shon et al (2010). The generation of public/private keys depends on Basic Connection Identifier (BCID) and initial ranging codes. In this way, both the BS and MS can be sure of knowing the right chosen keys. However, this process is vulnerable as it hides the risk for an attacker of knowing the BCID, ranging codes and then deducing the key pairs (Syed Shabih Hasan & Mohammed Abdul Qadeer 2011).

*Multicast and Broadcast Services (MBS):* In the mean time attacks on MBS of WiMAX are also identified. MBS allows the dissemination of data across multiple MS of the network, from a single BS. Communication in
MBS is unidirectional and is offered in the DownLink (DL) Request only (Xu et al 2008, Georgios Kambourakis et al 2010).

1.4.2 Handoff Issues in Mobile WiMAX

Seamless mobility of WiMAX is stressed due to handoff delays in Cross layer, Network layer, and MAC layer. Handoff is delayed in cross layer by explicit handoff notification to upper layers, imprecise Layer 2 triggers, seamless integration of Layer 2 and Layer 3 mobility management messages and two-way cross-layer handover information flow. MAC layer handoff issues are listed with excessive scanning and association activities, wastage of ranging slots, prolonged handoff Connection Disruption Time (CDT), network re-entry activity due to ping-pong effects, IP connectivity delay during network re-entry and optimizing handover-based load distribution. Mobile WiMAX is not limited to above mentioned challenges but is important to be addressed.

*Excessive scanning and association activities:* A continuous scanning algorithm was proposed to speed up the handoff process by Daniel et al (2009). Shun-Ren Yang et al (2010) addresses the solutions to handoff problems and advances the concept of relay station (RS) grouping as a likely methodology in the IEEE 802.16j is Multihop Relay standard. It explores the prospect of upgrading the RS grouping performance with regard to throughput and handoff frequency, while proposing a novel RS grouping algorithm, which utilizes greedy grouping policy to diminish handoff. Direction of movement based scanning technique is discussed by Ben-Mubarak et al (2011).

*Location Management:* Predicting the movement of MS before handoff reduces the delay of handoff with BS (Tseng & Feng 2008, Lu 2009). Reduction of handover delay in the Multicast and Broadcast Services (MBS)
of the IEEE 802.16e standard is obtained by using the method explained by Ji Hoon Lee et al (2011). It focuses on the concept of MBS Zone which is a group of base stations that are broadcasting the same multicast packets. The MBS architecture has location-management areas (LMAs) as its basis, which attempts to reduce the average handover delay by enlarging the MBS zones without unnecessary bandwidth expense.

**Network re-entry delay:** Re-use of TEK is encouraged by the existing handoff process with the help of TEK sequence number leads to handoff delay reduction but at the cost of compromise in security (Eren 2007). Another research by Shih Feng Hsu & Yi Bing Lin (2009) comes forward with a solution to this issue, in which a key caching mechanism is adopted to do away with the dispensable authentication cost in WiMAX handoff along with a study on time taken for key caching.

**Ping-pong processing delay:** The MS handoff between two adjacent BS continuously burdens the network as well as experience unwanted delay in both BSs. These types of calls are avoided to some extent by dynamically increasing the handoff threshold. Handover overheads caused by unnecessary re-entry procedures resulting from such ping-pong effects may degrade the overall system performance. Reducing this delay relies on identifying the ping-pons and avoids the duplication of handoff procedures at both BSs (Vesely & Breuer (2009), Kang et al 2010c, Feher & Veres 2012).

**Call admission control (CAC):** Each BS has its own capability of serving the MSs. When BS gets over burdened, the seamless mobility of MS is affected and hence the admission rate of MSs should be controlled according to the load, memory capacity and holding time of MS (Rong et al 2008, Cristiano Bonato Both et al 2012 and Chiapin Wang & Kun-Yeh Chan 2013). BS initiated handoff procedures, by only changing the position of QOS negotiation process and modifying handoff request and reply message,
enhances the handoff speed (Shun-Ren Yang et al 2010). Georgios Theodoridis & Fotini-Niovi Pavlidou (2011) introduced the combined resource management and admission control in mobile WiMAX.

1.5 SCOPE OF THE THESIS

The research challenges mentioned in the previous section paves the way to fix the problem. Current scenarios of wireless communication necessitate both security and speed with equal importance. Compromise on anyone of this leads to the degradation of technology. Diversified research works grow exponentially in improving security and reducing delay that motivated to do a combined research on Mobile WiMAX to afford a non negotiated secured seamless mobility. The first motive of the proposed research is to secure WiMAX network entry process from various threats. This research mainly focuses on the MAC layer issues and Key Management issues and as a subset, security threats in network entry process and various attacks are also resolved.

A secured environment should be created by which all parties of the communication should trust each other with the help of certificate authority. The vulnerabilities in the ranging process should be avoided by modifying the existing methodology. It should also be generalised to provide security measures to protect from all possible attacks. Time consumption of the proposed process should be affordable by the users who demand security. But the less secured existing process can be enhanced to a well secured process only with the additional computation time which definitely will lead to increase in handoff delay.
A balanced contribution in the security and handoff should be done without modifying the underlying architecture of mobile WiMAX. This motivated to reduce the authentication cost which in turn reduces handoff delay without compromising the security requirement. This can be achieved by solving the issues in existing security and handoff delay. The objectives were set accordingly followed by handful of proposed techniques. The proposed work furnishes considerable improvements in the existing performance of security and handoff delay reduction for mobile WiMAX by solving some of the issues mentioned above with the objectives as follows:

1. To enhance the security of ranging process by protecting the network from the various attacks and to secure the access between the entities like BS, ASN-GW and CSN.

2. To protect the message exchanges for key refreshment by the proposed automated mutual key generation algorithm which also minimizes the number of transactions between the mobile station and base station.

3. To reduce the authentication cost of mobile WiMAX users who re-enter the network by the proposed key caching techniques.

4. To reduce the authentication cost of ping-pong users who frequently move between adjacent BSs.

5. To reduce the authentication of mobile WiMAX users by proposing pre-authentication techniques.

1.6 ORGANIZATION OF THESIS

The thesis has been classified into seven different chapters including Introduction and Conclusion. The introductory chapter traces the development of WiMAX technology and establishes the need for the present research.
Chapters 2 and 3 deal with security enhancement and chapters 4, 5 and 6 discuss the strategies for authentication cost reduction which in turn leads to handoff delay reduction. **Chapter 2** discusses Initial network entry process of mobile WiMAX and its security threats. It proposes two types of secured ranging process to make the clear text initial network entry process as a secured one. It also discusses the need for access network security among the entities of mobile WiMAX and proposes the secured access techniques between two BS, BS & ASN-GW and ASN-GW and CSN. **Chapter 3** explains the key management of mobile WiMAX and discusses the research issues. To secure the key refreshing process and to minimize the bandwidth requirement of message exchanges, an automated mutual key generation technique is proposed. **Chapter 4** presents the steps accomplished for handoff management. It evaluates the need for key caching which enhances the handoff speed of re-entries of mobile stations. Three types of key caching techniques are proposed to reduce the authentication cost of mobile re-entries which in turn reduces the handoff delay.

Analysis of mobile WiMAX network done in chapter 4 necessitated the concentration on ping-pong MSs (Users who travel frequently between adjacent base stations). **Chapter 5** proposes to separate the ping-pong users from the large pool of mobile stations by registering them as ping-pong user and facilitating them according to their arrival time. **Chapter 6** facilitates the reduction of the authentication cost of MS which enters the mobile WiMAX by the proposed techniques which are processed before the occurrence of handoff. It includes pre-authentication technique for the intra-ASN handoffs and Reserved CID based passport handoff. The Proposed techniques of all the chapters are simulated and their results out of them are also depicted.