A Comprehensive Study on WiMAX Security

Murat Moran

A thesis Submitted to the
University of Essex for the degree of
Master of Science

Department of Computing and Electronic Systems
University of Essex

DECLARATION

I hereby declare that I am the sole author of this thesis. To best of my knowledge, the thesis contains no material previously published or written by another person except where due reference is made.

FOREWORD

The present thesis was prepared in the Computing and Electronic Systems Department of University of Essex, United Kingdom by October, 2007 until August 2008.

I am so pleased for the advice and support from my supervisors, Professor Stuart Walker, for his feedbacks and excellent guidance which kept me focused in my project until the end. Also, I would like to give my special thanks to Mr. Saleh Salah for his endless help and support when always needed. Finally, I am so pleased about the people that encourage and trust me in every piece of my life.

ABSTRACT

The IEEE 802.16e – 2005 standard (also called as mobile WiMAX) is a breakthrough in the area of wireless network technology providing high data rates, secure and seamless mobility, cost efficient deployment, and quality of services to the WiMAX users in a long range metropolitan area. Nevertheless, being a pioneer in such a crucial area for its providers and users carries a valuable and important role. In addition, the success of mobile WiMAX depends on a number of assets such as security of the system.

The focus of the thesis is the security architecture and vulnerabilities of the mobile WiMAX especially the security of MAC-layer and its components for instance Privacy and Key Management protocol (PKMv2) comparing with the previous version of the PKM (PKMv1). Meanwhile, the possible attacks against these weaknesses are identified and emphasized with the basis of them. Moreover, for the efficiency of the technology, various assessments are made also considering the safety of the system. As a result of this analysis, a number of security flaws have been found and the possible solutions have been proposed.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

1 INTRODUCTION

Wireless communications have become a reality of life by means of reduction of the cost, power consumption and providing mobility to user. However, besides having these advantages, efficiency, speed and the security issues became a growing concern. IEEE 802.11 (Wi-Fi) developed by IEEE 802.11 Working Group and released in 1997 is a set of standards for wireless and wired local area networks. Although 802.11 have a number of amendments for instance 802.11a, 802.11b, and 802.11y (the latest one), security problems couldn't be solved and it is still highly vulnerable to many kind of attacks. Moreover not providing efficient mobility is also another consideration.

As a result of this, IEEE 802.16 Working Group established a new air interface standard IEEE 802.16 WIMAX (the World Wide Interoperability for Microwave Access) in December of 2001 which is going to be next generation in wireless metropolitan areas. The main strengths of the standard are high bandwidth, high speed wireless connectivity, addressing the "last mile" problem and providing higher security. Furthermore, for portability and mobility purposes in BWA (Broadband Wireless Access) to mobile devices, IEEE 802.16e amendment was published in 2005 by WIMAX Forum. Notebooks, PDAs, cellular phones, in-vehicle devices, CCTV cameras, and game consoles are some of the mobile devices that have WIMAX interface (Hung-Min Sun, Yue-Hsun Lin, Shuai-Min Chen and Yi-Chung Shen, 2007). Moreover, some other applications supported by IEEE 802.16 including fixed and mobile services are illustrated in Figure 1.

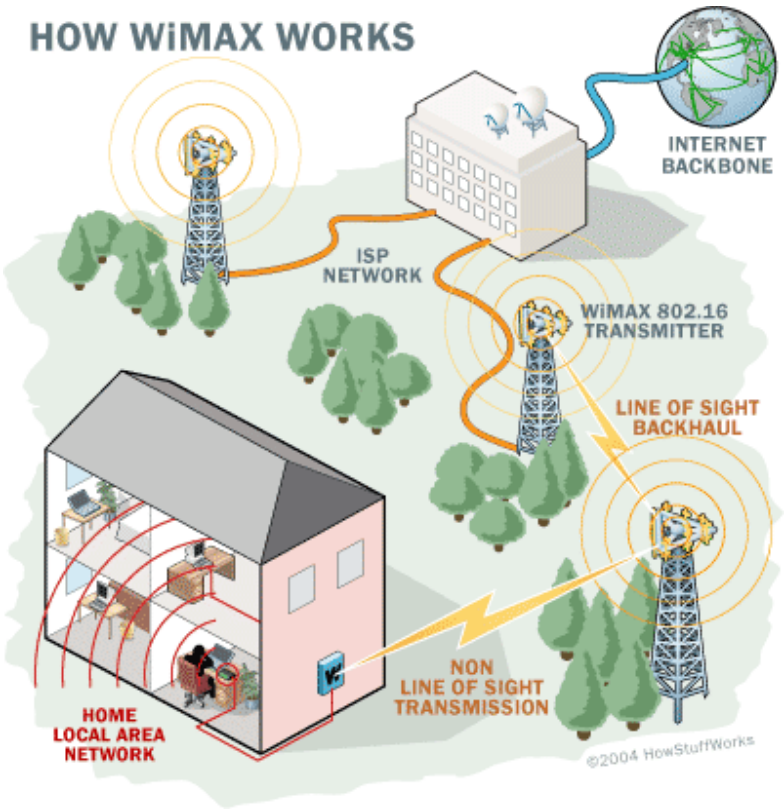

Figure 1 How WiMAX works (Meyer, 2006)

Although 802.16 has addressed some significant security vulnerabilities of 802.11 networks such as need of mutual authentication, lack of message integrity, weak encryption, and authorization vulnerabilities, IEEE 802.16 security protocols failed to protect mobile ad hoc networks (MANET) properly (Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed, 2007) until 802.16e (also called mobile WIMAX) was published. Afterward, these security flaws have been solved with 802.16e amendment using PKMv2 (Privacy Key Management Protocol).

1.1 PURPOSE

Since the WiMAX is an emerging technology in the broadband wireless networks area and attracts the attention of the service providers and the mobile devices users it needs to be analyzed carefully. The purpose of the thesis is to examine the network structure of the (IEEE 802.16e - 2005) mobile WiMAX regarding network security aspects and discover the parts that might put the system in danger having crucial vulnerabilities and provide

possible solutions for these bottlenecks of the mobile WiMAX. In addition, comparing two main standard IEEE 802.16 – 2004 which is mainly used in Wi-Fi networks and IEEE 802.16e- 2005 which is the standard for the mobile WiMAX is another main objective of this thesis. The problem questions which form the bases of this thesis can be specified as follows;

1. What are the strengths and the weaknesses of the mobile WiMAX network structure over other networking technologies both wireless and wired?
2. What are the existing security shortages of the system and attacks targeting them, and how can these vulnerabilities be suppressed?
3. What are the innovations in Privacy Key Management protocol second version (PKMv2)? and Are they good enough to provide security to the mobile communications among mobile WiMAX networks and also between heterogeneous networks?
4. What are the ways of the reducing handover latency during macro and micro handoff process?

Furthermore, understanding how mobile WiMAX and its mechanisms work and giving a theoretical background considering its network security characteristics.

1.2 THESIS OUTLINE

The thesis is separated into the following areas; Chapter 2 gives an overview of the WiMAX networking technology beginning from its genesis till nowadays. In addition, a numbers of important features of the WiMAX, also including its physical layer characteristics, are presented as well as MAC-layer features and elements. Additionally, WiMAX network architecture is mentioned roughly in this chapter. In Chapter 3, more specifically, WiMAX security is studied and the mechanism of the security sublayer is examined. Chapter 5 shows overall picture of the PKMv1 highlighting that it needs to be improved by giving theoretical evidences. Chapter 5 makes comparisons between PKMv2 and its previous version, PKMv1 and identifies the differences among them. Moreover, suitable pre-authentication schemes are proposed in order to reduce handover

latency which causes unwanted connection loss and power consumption for the restricted devices. Lastly, in Chapter 6, the problem questions, which are clarified in the purpose subsection, are answered and the conclusions are made. In addition, the further work that needs to be addressed is suggested.

CHAPTER 2

2 WiMAX OVERVIEW

The need for the wireless data transmission has become very significant since first decade of the twenty first century when the fixed internet network expands worldwide. The most successful technology was the Global System for the Mobile communication (GSM) which is primarily used voice transmission. Afterwards, third-generation (3G) cellular technology has been developed which was capable of providing wireless communication system and deployed across the world. Different types of wireless communication technologies have been designed such as Wireless Personnel Area Network (WPAN) and Wireless Area Network (WLAN) which are used in Bluetooth devices and Wi-Fi networking technologies respectively and where the coverage areas are quite small compared to WiMAX networking technology. Figure 2 illustrates the different types of wireless data transmission technologies.

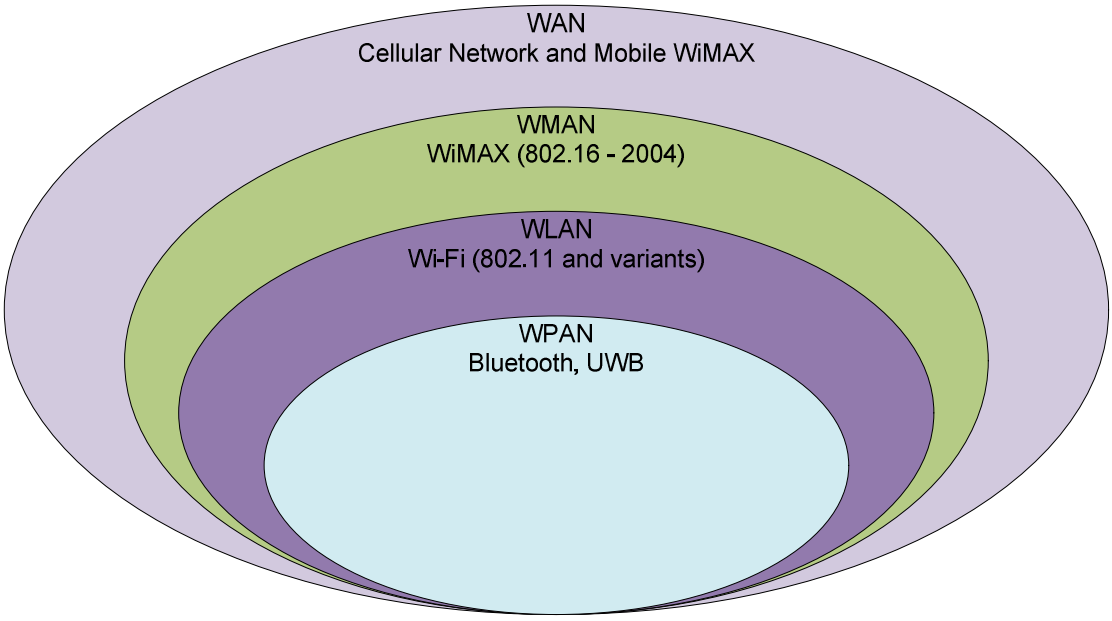

Figure 2 Different Types of Wireless data transmission technologies (Nuaymi, 2007)

2.1 GENESIS

WiMAX is created by the WiMAX Forum which is formed in 1998 and it is based on IEEE 802.16 standard completed in December 2001. It provides high bit-rate data over the air interface in a variety of ways from Point to Point (P2P) links to mesh mode. It is also called WirelessMAN (Metropolitan Area Networking). It is also believed to solve the Last Mile problem.

IEEE 802.16-2001 is the first standard of the family, published in 2002 and provides network access to buildings through exterior antennas communicating with a radio base station using point to multipoint (PMP) infrastructure design and operating between 10 and 66 GHz with an average bandwidth of 70 Mbps and a peak rate up to 268 Mbps. Because of having some problems with existing European counterpart standard such as HiperMAN and limited to line-of-sight (LOS) propagation, it was followed by many amendments.

The first amendment was IEEE 802.16c which was published aiming to certify interoperability between existing local multipoint distribution service LOS solutions working in the 10-66 GHz range. However, its maximum coverage area couldn't exceed 5 km. Afterward, IEEE 802.16b, also called WirelessHUMAN (Wireless high-speed unlicensed metropolitan area network) followed. It's primarily published for quality of service (QoS) features. It widened 802.16-2001 to operate under license-exempt regulation in the 5-6 GHz range.

The most well-known amendment is the 802.16a published in April 2003. The main objective was to standardize the lower-frequency multi channel multipoint distribution service (MMDS) solutions in licensed and unlicensed range of 2-11 GHz. Because of working lower frequencies 802.16a has the advantage of being able to offer non-line-of-sight (NLOS) communication and a coverage area up to 50 km with a bit rate up to 75 Mbps, using an OFDM (orthogonal frequency division multiplexing)-based physical layer. Moreover, it facilitated to communicate in mesh network.

IEEE 802.16-2004 which is an active standard was followed by different projects addressed different issues. In December 2005, the IEEE group completed and published IEEE 802.16e-2005 as an amendment to IEEE 802.16-2004 adding mobility support, which is referred as Mobile WiMAX and as an example for Wide Area Network (WAN).

2.2 Main Features and Advantages

WiMAX offers a wide-range set of features with a lot of flexibility in terms of deployment options. The Physical Layer (PHY) and MAC-Layer has been improved in order to deploy broadband wireless networks all over the word by the IEEE 802.16 Working Group. The main features and advantages of WiMAX compared to other broadband wireless networks are presented briefly in separate sections namely, WiMAX Physical Layer and WiMAX MAC-Layer as depicted in Figure 3.

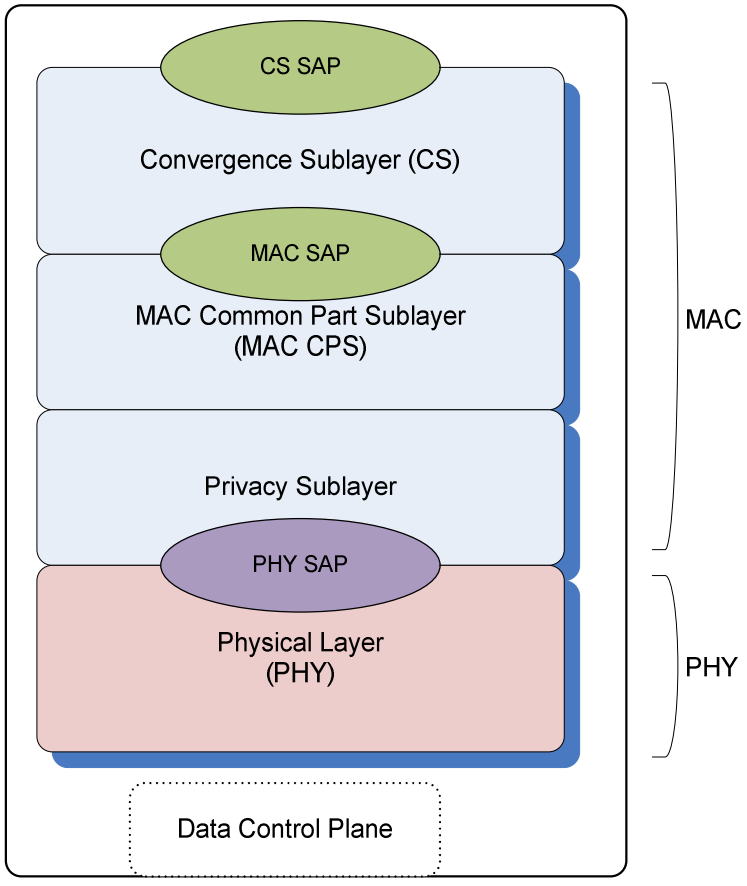

Figure 3 Protocol Layer of WiMAX (based on)

2.2.1 WiMAX Physical Layer

2.2.1.1 OFDM

One of the significant improvements of the WiMAX physical layer, used in fixed-WiMAX is the Orthogonal Frequency Division Multiplexing (OFDM) which can provide high speed Non-Line of Sight (NLOS) and multicarrier modulation scheme, where the high-bit-rate data stream is divided into several lower bit-rate streams and each stream is modulated on separate carriers. By means of OFDM, inter-symbol interference (ISI) can be avoided by increasing the symbol rate enough (Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed, 2007).

Fixed WiMAX which is based on IEEE 802.16-2004 uses a 256 FFT-based OFDM physical layer. On the other hand, mobile WiMAX which is based on IEEE 802.16e-2005 standard uses (Orthogonal Frequency Diversity Multiple Access) OFDMA-based physical layer which facilitates the use of frequency diversity and multiuser diversity to improve system capacity. Flexibility of the size of Fast Fourier Transform (FFT) which may vary from 128 bits to 2,048 bits depending on the available channel bandwidth plays an important role for scalability.

2.2.1.2 Advanced antenna techniques

Some features of WiMAX such as space time coding and spatial multiplexing allow us to use advanced antenna techniques for instance spatial diversity antennas, simple diversity antennas and beam-streaming antennas. Deploying these multiple antenna techniques at both receiver and transmitter often refers MIMO (multiple input multiple output) which improves the overall system capacity by increasing data throughput link range without any additional bandwidth or transmit power. Furthermore, under very good signal conditions, using multiple antennas and spatial multiplexing, higher data rates could be achieved.

2.2.1.3 Adaptive modulation and coding (AMC)

Different modulation schemes are supported by the WiMAX such as BPSK and QPSK for the down-link and up-link communications (Syed Ahson, Mohammad Ilyas, 2008). In order to maximize throughput in a time varying channel, AMC is used where there is a

need of use of the highest modulation and coding scheme that can be supported by the signal-to-noise and interference ratio at receiver in order to supply the highest possible data rate (Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed, 2007).

2.2.1.4 TDD AND FDD

Both, Time Division Duplex (TDD) and Frequency Division Duplex (FDD) are supported by WiMAX standard. For the low cost implementations half-duplex FDD is also supported. TDD which uses a single channel for down-link and up-link in a different time slots is very efficient especially for IP-based and asymmetrical systems and it requires less additional components than FDD does and which means reduction in the deployment cost.

2.2.2 WiMAX MAC-LAYER

The Media Access Control (MAC) Layer is responsible for controlling the traffic over physical layer by way of being an interface between higher layers and physical layer. MAC service data units (MSDUs) are taken and arranged into MAC protocol data units (MPDU) and transmitted over the air by MAC layer and for the received transmissions the reverse of this process is followed. As shown in Figure 4, MAC layer consists of three main sublayers to be precise, Convergence Sublayer (CS) which is the top sublayer of the MAC layer, Common Part Sublayer (CPS) and Privacy Sublayer which provides authentication, key management and encryption and it will be focused on deeply in Security Sublayer section.

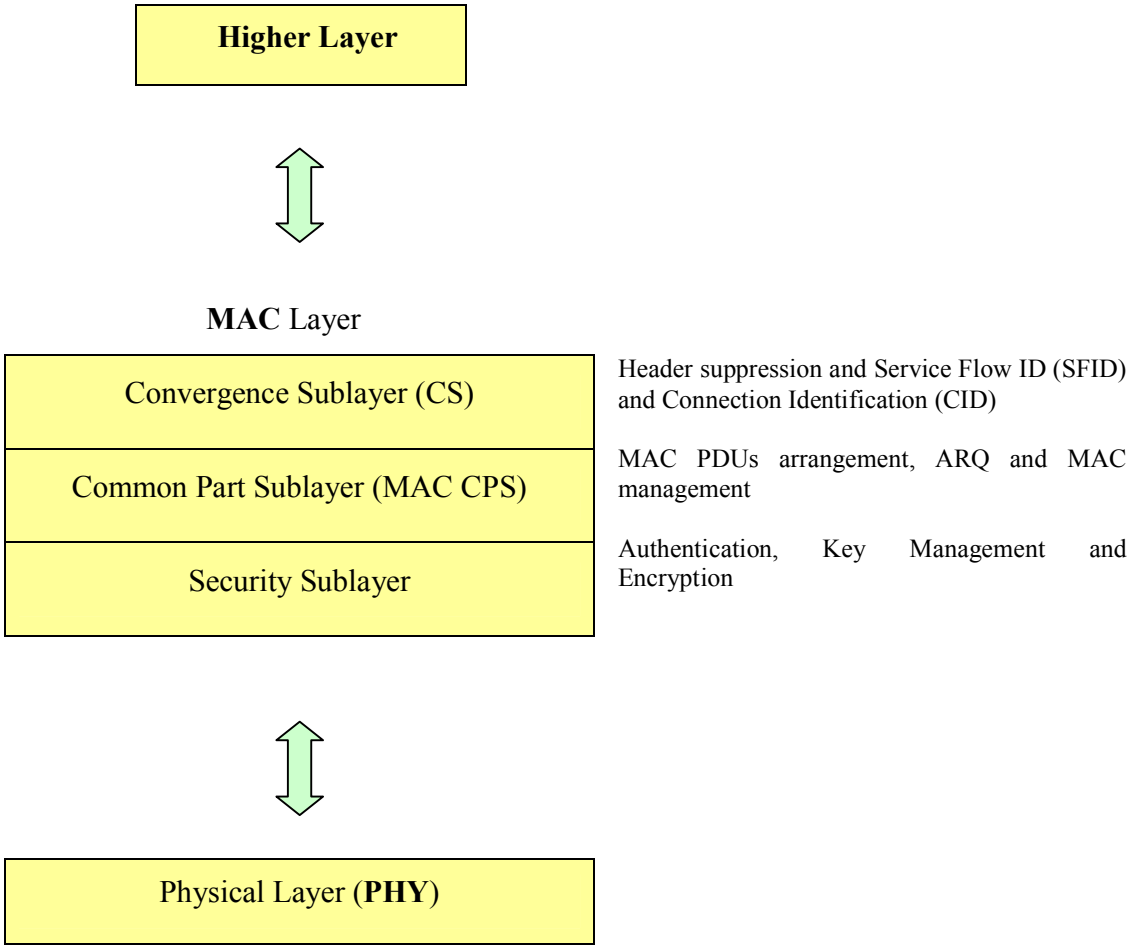

Figure 4 WiMAX MAC Layer

Convergence Sublayer facilitates the receiving PDUs from higher layers and transmission to the CPS where the standard MAC layer procedure takes place such as bandwidth allocation, connection establishment, management, packing and fragmentation. By means of using CS in MAC layer, a reduction in higher layer overheads is achieved (Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed, 2007).

WiMAX defines 48 bits IEEE 802 MAC address for each Subscriber Station (SS) and it is used for mutual authentication between BS and SS. On the other hand, BS has another address namely 48-bit Base Station ID (BSID) different than its MAC address. Figure 5 illustrates the MAC PDU, MAC PDU Header format for Header Type 0 which is the generic MAC header format and Header Type 1 which is without payload and called bandwidth request header respectively.

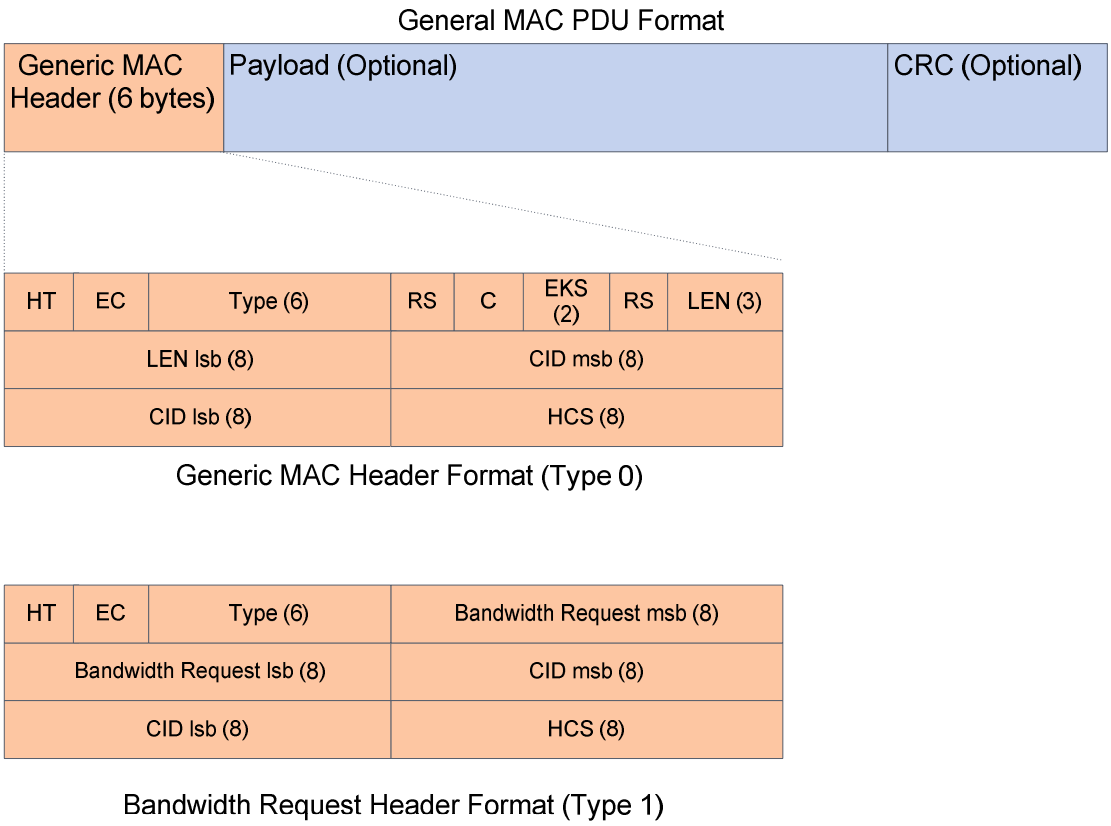

Figure 5 Generic MAC PDU and Header Formats

The WiMAX MAC layer has a connection oriented architecture where downlink and uplink connections controlled by the serving BS and Each connection is identified by CID (Connection Identifier). Moreover, in order to provide intended promising feature i.e. supporting very high bit rates, special variable-length MPDUs have been designed by WiMAX Forum.

2.2.2.1 ARQ AND H-ARQ

WiMAX supports Automatic Repeat reQuest (ARQ) at the link layer to ensure reliable connection. These kinds of connections need each transmitted packet to be acknowledged by the receiver. Furthermore, hybrid-ARQ (H-ARQ) and its main variants, Incremental Redundancy and Chase Combining are also supported by WiMAX. H-ARQ combines the features of ARQ and an error control code such as Forward Error Correction (FEC) and allows that the messages that are received with errors are sent with the combination of

subsequent retransmissions aiming an improvement in reliability. ARQ mechanism flows as illustrated in Figure 6.

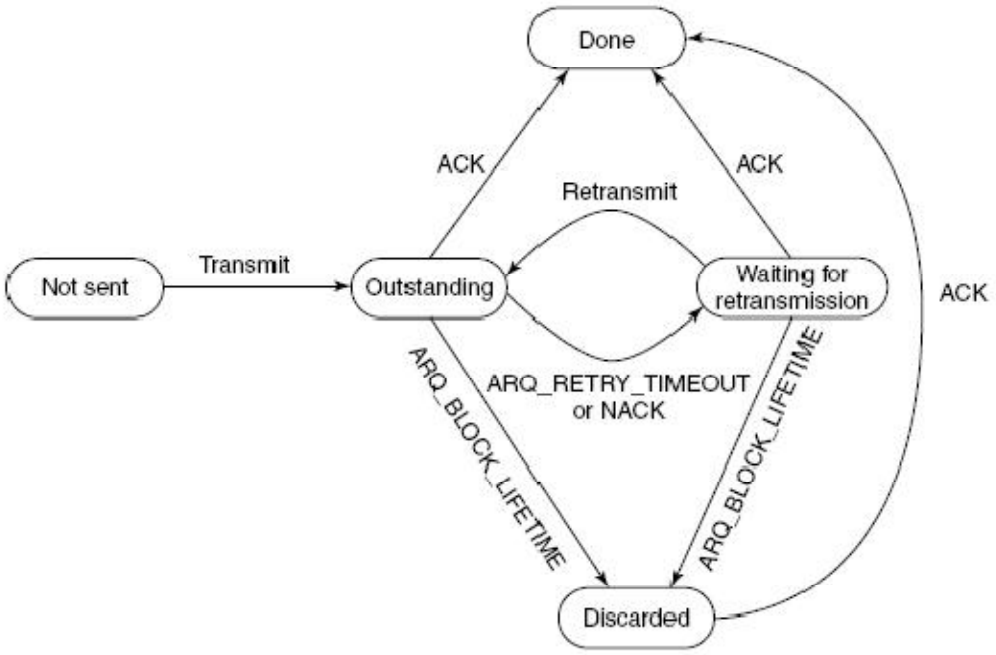

Figure 6 ARQ Scheme in WiMAX (Syed Ahson, Mohammad Ilyas, 2008)

2.2.2.2 QoS (Quality-of-Service)

QoS requirements that can vary for each connection for instance data rate, jitter, and packet error rate are handled with various instrument of WiMAX. Scheduling Service is the one of them. WiMAX defines five different scheduling services to be able to meet QoS requirements for. These are the real-time polling service, the non-real-time polling service, the best-effort service, the extended real-time polling service (Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed, 2007).

Service flow is another crucial part of WiMAX QoS architecture which the packets crossing over the MAC layer are associated with and it is used to order and schedule the transmissions in other words a service flow identifies QoS parameters for the MAC PDUs. Different service flows are set into service flow classes which enables the service provider to control the management of QoS for all application i.e. VoIP, e-mail, in general multimedia services.

WiMAX MAC is designed to provide multiple connections to a large number of users and each connection has its own QoS requirement. The QoS parameters might include traffic priority, maximum traffic rate, maximum burst rate, ARQ type, maximum delay and service data unit type and size.

2.2.2.3 MOBILITY

Mobility is the most important challenge for the wireless communications as the subscriber station or mobile devices move even at the vehicular speed through a large scale area where foreseeing the route of the mobile device is not so easy. For the session initiation, Subscriber station sends signals through the network when it moves. These signals are stored at the centralized databases. Therefore, the roaming is handled by using these databases causing a trade of between consuming radio resource and transmitting location updating signals (Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed, 2007).

Another issue apart from roaming is the handoff. As the SS moves from one base station called serving BS to another called target BS which provides stronger signals and better QoS, it is necessary to maintain the ongoing sessions without any interruption. Otherwise, the handover latency increases causing the worse service quality and because of the limitation of resource and power of MSs, the time elapsed for handover process becomes crucial. The handoff process involves the detecting and the making decision when to handoff (Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed, 2007). There are two types of handoff that is Hard Handoff and Soft Handoff. Hard handoff is that SS ends its radio links with the serving BS before establishing a connection with the target BS. Soft Handoff is the making a connection with the target BS before ending the connection between serving BS. It is clear that soft handoff is quite faster than hard handoff.

IEEE 802.16e – 2005 (Mobile WiMAX) whose major aim is to introduce mobility allows mobile constraint devices to save power by turning off parts of the SS in a controlled manner in the situation where SS is not sending or receiving data. It supports robust seamless handovers for full mobility applications for example VoIP (voice over IP). In

addition, it has a built-in support to save the battery life. Furthermore, three handoff methods are supported by WiMAX; Hard Handover, which is mandatory, should be implemented initially. Moreover, Fast Base Station Switching (FBSS) and Macro Diversity Handover (MDHO) are the optional soft handover methods for SSs and BSs which are supported by IEEE 802.16e – 2005 standard. These two methods allow an SS to establish connection with more than one BS. However, in FBSS, SS communicates only with one BS which is called anchor BS whereas in MDHO an MS can communicate with all base stations in its diversity set.

2.2.2.4 SECURITY

WiMAX Security is handled at the Security sublayer in WiMAX MAC layer. Being aware of the threats and the vulnerabilities in Wi-Fi technology over the years, IEEE 802.16e – 2005 provides more reliable, trusted wireless communication to the mobile WiMAX users with additional security protocols especially for mobility which is necessary for the WiMAX market success.

For instance, for the data encryption, instead of using DES (Data Encryption Standard) or triple DES, WiMAX uses AES (Advanced Encryption Standard) which is believed to be stronger and easier to implement than DES which provides data privacy. In addition, it supports the flexible authentication architecture based on EAP (Extensible Authentication Protocol) and it has a robust key-management protocol PKMv2. The Privacy key-management protocol (PKMv2) is used to transfer all credentials from BS to MS securely by reauthorizing and refreshing the keys periodically. Moreover, the integrity of the messages that is sent through air is controlled by message digest methods such as CMAC (cipher-based message authentication code) and HMAC (hash message authentication code). And for the security vulnerabilities and the QoS considerations, WiMAX supports the fast handoffs by way of pre-authentication method which is used by MS with a specific BS.

2.3 WiMAX NETWORK ARCHITECTURE

In order to provide mobility, security and IP connectivity to WiMAX subscribers, WiMAX network architecture contains a number of protocols and consists of three main

components namely; (Mobile) Subscriber Station (M)SS, Access Service Network (ASN) and Connectivity Service Network (CSN) (see Figure 7). The network architecture will refer to the Point to Multi Point (P2MP) network architecture for the rest of the section rather than Mesh mode which is an optional network model for WiMAX technology.

The main function of the ASN is to provide radio access connection to SSs by using one or more BSs and ASN Gateways (ASN-GW). Moreover, handover control inside the BS and radio resource control and mobility related functions, MS discovery, location management, paging, and location management are supported by the ASNs. ASN-GW also fulfils admission control by caching the subscriber credentials and the encryption keys (Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed, 2007).

CSN provides IP connectivity allocating IP address to the MSs. AAA server in CSN provides authentication, authorization and accounting (AAA) and it will be focused on more in WiMAX Security section. In addition to this, the roaming between Network Access Providers (NAP) is supported by the inter-CSN tunnelling. Moreover, subscriber billing and WiMAX services such as location-based services, peer-to-peer (P2P) connection are the other functionalities of the CSN.

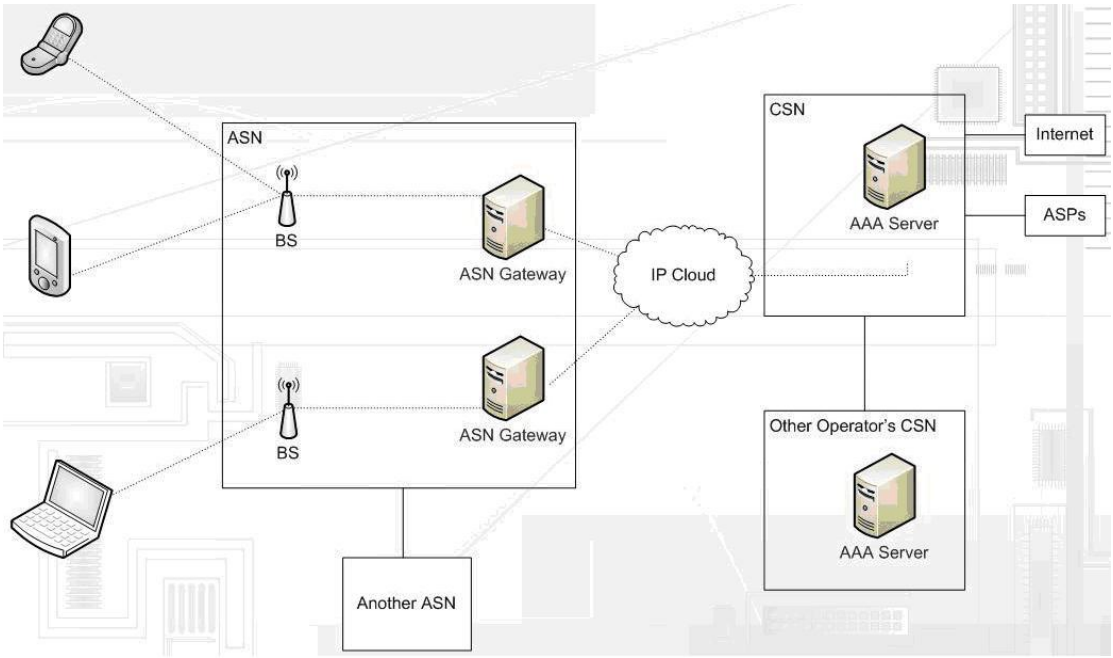

Figure 7 Mobile WiMAX Network Reference Model

CHAPTER 3

3 WiMAX SECURITY

3.1 OVERVIEW OF WiMAX SECURITY

Being promising technology, mobile WiMAX (IEEE 802.16e - 2005) needs to be considered carefully in order to achieve great market success. Many weakness and inefficiencies of WiMAX has been identified for the IEEE 802.16 – 2004 over the years. Although some security flaws of IEEE 802.16 – 2004 is no longer a threat thanks to 802.16e - 2005 amendment, mobile WiMAX still has to be improved especially against security concerns.

The security of WiMAX is based on encapsulation protocol and PKMv2 (Privacy Key Management Protocol version 2) which provides authentication, authorization and secure distribution of keying data from BS to MS and operates as a security sublayer in Medium Access Control layer. PKMv2 provides better confidentiality, integrity, and privacy than PKMv1 which is used in Wi-Fi networking technology.

Both PKM versions establish a shared secret key called Authorization Key (AK) which will be used to derive Key Encryption Key (KEK). Afterwards, KEK is used to exchange Traffic Encryption Key (TEK) established in BS and then to be used to encrypt messages sent between MS and BS. PKMv2 can use either EAP-based (Extensible Authentication Protocol) or RSA-based authentication schemes.

There are different kinds of EAP methods such as EAP-TLS, which is commonly used and capable of providing mutual authentication between BSs and MSs, EAP-SIM and EAP-AKA. Although EAP has a flexible authentication architecture and robust key management protocol, still it has some drawbacks. One important disadvantage of EAP is

that EAP framework causes a long delay especially during the re-authentication procedure. Thus, it may cause loss of quality of service while roaming.

RSA-based authentication uses X.509 digital certificate which has been issued by MS manufacturer in order to provide mutual authentication between MS and BS. However, requiring an important amount of memory to save the certificates is the bottleneck of it as the mobile devices may have limited space. There also exist other PKI (Public Key Infrastructure) algorithms, which are faster than RSA algorithm, such as ECC (Elliptic Curve Cryptography) which could be a solution for the problems regarding speed and latency in authentication phases.

There are some other proposed authentication schemes for the mobile-WiMAX which are believed as secure as EAP-TLS with significant reduction in latency while re-authentication in the phase of handover. One method is the Proactive Key Distribution (PKD) which reduces the number of messages that is sent between MS and BS in order to authenticate each other. In other words, some of steps of EAP-TLS are achieved before roaming.

Another security issue, privacy is achieved with robust cryptographic encryption methods i.e. Advance Encryption Standard (AES) and Triple Data Encryption Standard (3DES). Regarding their cryptographic aspects such as key sizes, both are more robust than DES which is used in Wi-Fi networking technology.

The integrity is provided by using message digest algorithms; MD5-based HMAC or AES-based CMAC.

While providing speed for the authentication, the thing that should also be thought is security of the system. In the next section, some vulnerability of the mobile-WiMAX and the attacks against them are described.

3.1.1 *Existing Security Vulnerabilities and Known Attacks against WiMAX networks*

The known attacks against WiMAX newtworks can be summerised as follows:

- Handover vulnerability: As the mobility becomes a reality for the Mobile WiMAX networks, new attacks appear in the process of re-entering the network while handoff. A critical example is that PKMv2 (Privacy key management) authentication scheme which is used for IEEE 802.16e – 2005 standard is omitted while re-entering which may cause forgery attacks to the SSs by copying the identity of BSs (Fuqiang Liu and Lei Lu, 2006).

- Initial network entry vulnerability: In the initialization process between SS and the BS the SS Basic Capabilities (SBC) carries vital information during initial network entry and not having any security measures to keep their safety is an open gate to attackers. Even the existing message authentication schemes and encryption algorithms in IEEE 802.16e – 2005 which are HMAC/CMAC and AES-CCM are applied after initial network entry which means a malicious user may use that information to attack the system (Carl Eklund, Roger B. Marks and Kenneth L. Stanwood, 2002).

- Key space vulnerability: Insufficient space for distinguishing successive AKs (authentication key) and TEKs (traffic encryption key), 4-bit and 2-bit respectively (Fuqiang Liu and Lei Lu, 2006). The attack which arises due to lack of key space is Replay Attack in which case the space separated for the TEK keys runs out quickly in other word TEK identifier needs to wrap from 3 to 0 on every fourth key (Syed Ahson, Mohammad Ilyas, 2008).

- Initialization vector vulnerability: IV (initialization vector) is XORed with the contents of PHY synchronization field with the most recent one. Thus, it is easy to predict IV as PHY synchronization field will be repetitive and predictable (Fuqiang Liu and Lei Lu, 2006) exposing the characteristics of the IV then using the known-plaintext attacks might be used by the attackers.

- Ranging response vulnerability: RNG-RSP is the ranging response message from BS to SS in order to reply the RNG-REQ message that is sent from SSs to BSs to enter the WiMAX network. For the purpose of this, RNG-RSP carries crucial information such as SS request transmission time, power, frequency, and burst profile information (Carl Eklund, Roger B. Marks and Kenneth L. Stanwood, 2002). Following that, RNG-RSP message which BS uses in order to distinguish the SSs are sent from BS to SS. The vulnerability also occurs when these messages aren't encrypted while transmission such as in IEEE 802.16 – 2004 standard. Thus, attackers easily can modify the ranging messages to attack the system in order to interrupt the network activities and cause DoS (Denial of Service) attacks (Carl Eklund, Roger B. Marks and Kenneth L. Stanwood, 2002).

3.2 SECURITY SUBLAYER

The security sublayer allows secure communications over broadband wireless network by using cryptographic transforms to MPDUs carried between MS and BS. BS has an important role in providing protection against the services thefts by securing service flows. Figure 8 shows the protocol stack of the security sublayer with the recommended scope.

There are two protocols in the security architecture of WiMAX;

- Encapsulation protocol in order to secure data across the seamless network: This protocol defines the supported cryptographic suites such as authentication algorithms and data encryption methods and the rules for applying those algorithms to a MAC PDU payload (IEEE Std 802.16, 2004). However, not encrypting MAC management messages is the main reason for the initial network entry vulnerability.
- A key management protocol such as PKMv1 and PKMv2 provides secure distribution of the keying materials from BS to MS. PKM will be analysed in the following sections deeply.

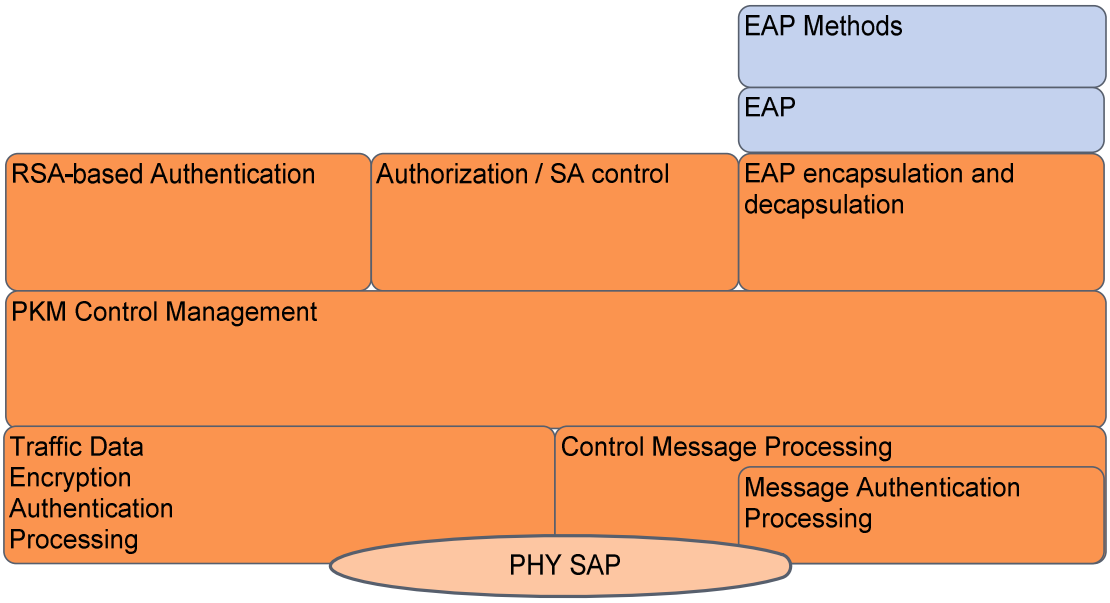

Figure 8 Security Sublayer Protocol Stack with recommended scope

3.2.1 KEY MANAGEMENT PROTOCOL

In order to provide mutual authentication or unilateral authentication, and re-authentication/reauthorization and refreshing Traffic Encryption Keys (TEK), key management protocol has three optional authentication methods.

- Extensible Authentication Protocol (EAP) [IETF RFC 3748]
- X.509 digital certificates together with RSA public key algorithm [IETF RFC 3280]
- RSA authentication followed by EAP authentication

Mainly, a shared secret key called Authentication Key (AK) is issued between MS and BS which is then used in order to exchange the TEKs securely. In the client-server model between MS and BS, BS authenticates the MS during the initial authorization process by checking X.509 digital certificate of MS which is issued by the manufacturer of the MS. Digital certificates in each MS contain the MSs MAC addresses and public keys. When MS is sending AK request to BS, it also send its digital certificate in order to allow BS to verify MSs Certificate and to encrypt the AKs with MSs Public key. Having the TEKs MS is authorized to access the services by BS.

Furthermore, it is clear unilateral authentication could be a source for the attacks such as rogue MS or BS, for this reason, mutual authentication which is provided by the PKMv2 is the essential part of PKMv2 to avoid these sorts of attacks.

In the following sections, PKMv1 of IEEE 802.16 – 2004 and PKMv2 which is announced in the 802.16e amendment will be analysed and discussed intensely. Moreover, the pros and cons of the both key management scheme will be presented. However, in PKMv1 subscriber station (SS) will be the client whereas in PKMv2 mobile station (MS) will be the client in the client-server model with BS.

CHAPTER 4

4 PKMv1

Security Association (SA) is the set of security information shared by BS and SS in order to communicate securely across the IEEE 802.16e – 2005 networks. SAs are identified by the Security Association ID (SAID) and the exact content of the SAs depends on the SAs cryptographic suite which is employed within SSs. The standard defines three kinds of SA;

- Primary SA: During the SS initialization process, primary SAs are established by each SS.
- Static SA: supplied within BS.
- Dynamic SA: established and eliminated in response to the initiation and termination of service flows.

In addition to these, WiMAX also uses two different types of SAs, data and authorization SAs. Data SAs protect transmission between SSs and A BS, whereas Authorization SAs is used by a BS to configure data SAs for each SS. The contents of each type of SAs are shown in Table 1and Table 2.

The content of the Data SAs
16 bit SAID that uniquely identifies the data SAs
Encryption Cipher to protect data exchange, DES Cipher Block Chaining (CBC) mode
Two TEKs (One for current in use and the other for in case of key expiration)
Two 2-bit TEK identifiers
TEK lifetime (the default lifetime is half a day but it can vary from 30 min to 7 days)
Initialization Vector (IV) for each TEK
Data SA type identifier

Table 1 The content of the data SAs

The content of the Authorization SAs
X.509 certificate
Authorization key (160-bit)
4-bit Authorization key ID
Authorization Key lifetime (The default value is 7 days and varies from 1 day to 70 days)
Key Encryption Key (KEK)
Downlink and Uplink Hash-based Message Authentication Code (HMAC) keys
The list of authorized data SAs

Table 2 The content of the authorization SAs

Static and Primary SAs may be shared by multiple SSs. PKM allows SS to request a SAs keying material from its BS. SAs keying materials has a limited lifetime and it needs to be fresh. As a result, SS has the responsibility for requesting new keying material from BS before it expires at the BS. If SS doesn't receive the new keying material SS will need to perform network entry.

4.1 AUTHORIZATION VIA RSA AUTHORIZATION PROTOCOL IN PKMV1

PKMv1 provides one way RSA-based authentication where only BS authenticates SS. This means SS does not authenticate the BS, thus a rogue BS can create and send AUTH RSP messages to the SS in order to fulfil forgery attacks. PKMv1 Authorization flow via RSA authentication protocol is illustrated in Figure 9.

SS **BS**

Authentication Information Message (Auth_Info)

→

- The message contains SS manufactured X.509 certificate issued by SS's manufacturer, however BS may choose to ignore it

Authorization Request (Auth_REQ)

→

Auth_REQ is sent to request AK and SAID from SS, and it contains;

- A manufacturer issued X.509 certificate
- A list of cryptographic suites and descriptions of cryptographic algorithms, such as data Encryption and Message Authentication Algorithms
- SS's basic CID which is the first Primary SAID assigned by BS during initial ranging

Authentication Reply Message (Auth_RSP)

←

After getting Auth_REQ message, BS validates the identity of SS and determines the encryption algorithms and supported protocols. The remaining is just to activate AK for SS by sending Auth_RSP message which contains;

- AK encrypted with SS's public key
- 4-bit key sequence number (SeqNo) used to separate successive AK generations
- A key lifetime
- SAID lists and properties of SAs

Figure 9 Authorization in PKMv1

Other messages that might be transmitted between SS and BS are;

- An Authorization Reject (Auth Reject) message is sent from BS to SS in response to a Key Request.
- In the case of an unsolicited indication or a response to a message from one of the SSs, Authorization Invalid (Auth Invalid) message is sent by the BS to SS. When SS sends a Key Request message to BS, if BS doesn't recognise it as an authorized SS which means SS doesn't have a valid AK or if BS can't confirm the validation of HMAC of Key Request, BS sends Auth Invalid message to that particular SS.

An SS needs to refresh AK without interruption by resending Auth_REQ to the BS without sending any Authorization Information to the BS under the control of Authorization State Machines. AK lifetime which AK expires is predefined in BS system configuration parameter. BS sends Authorization Reply message to SS with the remaining AK lifetime at the time the Authorization Reply message is sent. If the SS doesn't reauthorize before current AK expires, it is quite possible that BS can't recognize the SS as an authorized SS and can remove all TEKs associated with that SS from its keying table.

BS uses AKs for the following reasons;

1. Verifying the message digest of the Key Request messages from SS
2. Calculating the message digests that is written in to Key Reply, Key Reject and TEK invalid messages
3. Encrypting TEK messages prior to sending it to SS

SS uses HMAC_KEY_U which is derived from most recent AKs of SS in order to insert the message digest into Key Request messages. Moreover, SS is capable of using HMAC_KEY_D derived from most recent AKs to authenticate Key Reply, Key Request, and TEK Reject messages. In addition, KEK which also derived from its most recent AK is used to decrypt an encrypted TEK in a key Reply message. Lastly, AK Key Sequence Number is used to decide on which set of keying material defined by the BS will be used.

4.2 CRYPTOGRAPHIC METHODS IN PKMV1

4.2.1 DATA ENCRYPTION METHODS

IEEE 802.16 – 2004 defines two different data encryption methods to encrypt MAC PDU; Data Encryption Standard (DES) CBC mode and Advanced Encryption Standard (AES) CCM mode. For the rest of this section these algorithms will be defined briefly and mentioned about their strengths and vulnerabilities against some attacks.

DES in CBC mode is a symmetric key block cipher with the key size of 64-bits. The operations used in DES are transpositions, XOR, linear transformations, substitutions and modular arithmetic multiplications. DES processes 64-bit plaintext blocks and produces 64-bit cipher text block (see Figure 10) using K with 56-bits key size.

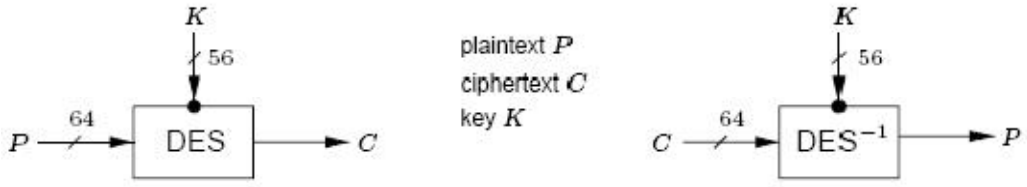

Figure 10 DES Input and Output (A.J. Menezes, Paul van Oorschot and Scott A. Vanston, 2001)

DES process consists of 16 rounds and 8 S-boxes which substitutes 6-bit to 4-bit. In each round K_i subkeys are generated and 64-bits plaintext is divided into 32-bits two block, L_0 and R_0. Moreover, in each round the next 32-bit outputs L_i and R_i are calculated for $1 \leq i \leq 16$, as follows;

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, *where* $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$ *and E and P are the fixed expansion permutation mapping from 32-bits to 48-bits* (A.J. Menezes, Paul van Oorschot and Scott A. Vanston, 2001).

As all other symmetric key algorithms, the same key and the algorithm are used for both encryption and decryption; however, in the decryption procedure of DES, the subkeys Ki are used in reverse order. Figure 11 illustrates the process of the DES inner function f.

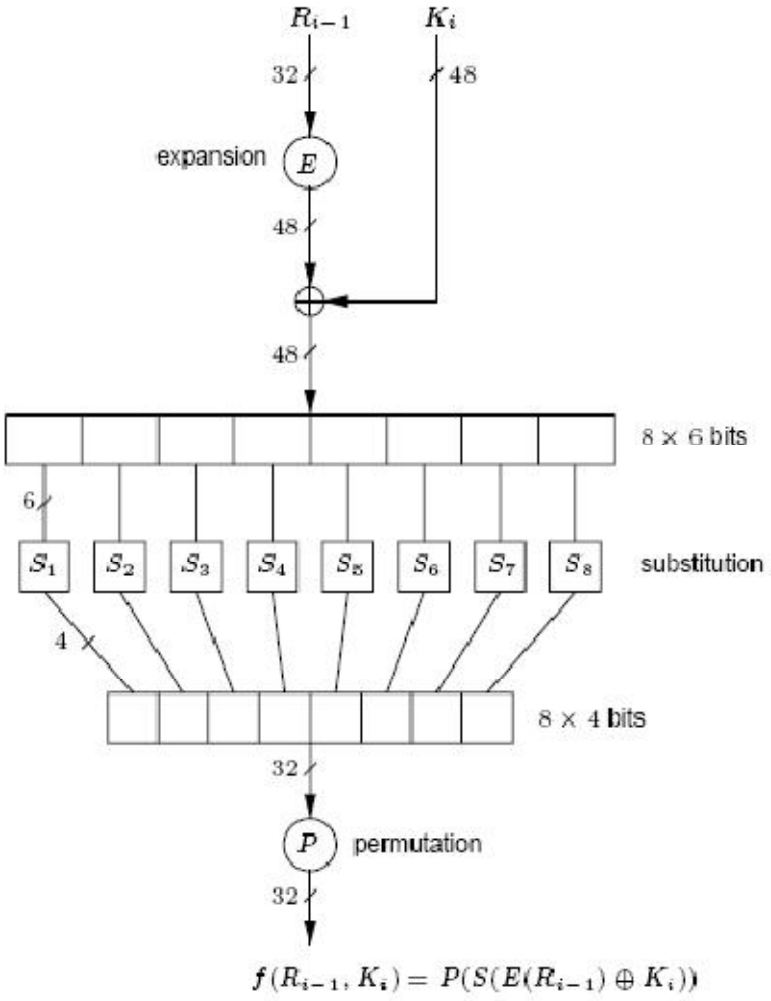

Figure 11 DES Inner Function

Generally, Cipher Block Chaining (CBC) mode is described as follow; each block of plaintext is XORed with the previous encrypted ciphertext block priory to being encrypted, however, in order to encrypt the first block of the plaintext an Initialization Vector (IV) must be used. In downlink, IV is calculated with the XOR of the IV parameter which is supplied in the TEK keying material and the content of the PHY synchronization field. Figure 12 demonstrates the CBC mode encryption and decryption where the CIPHK and CIPHK-1 represents DES and DES-1 respectively.

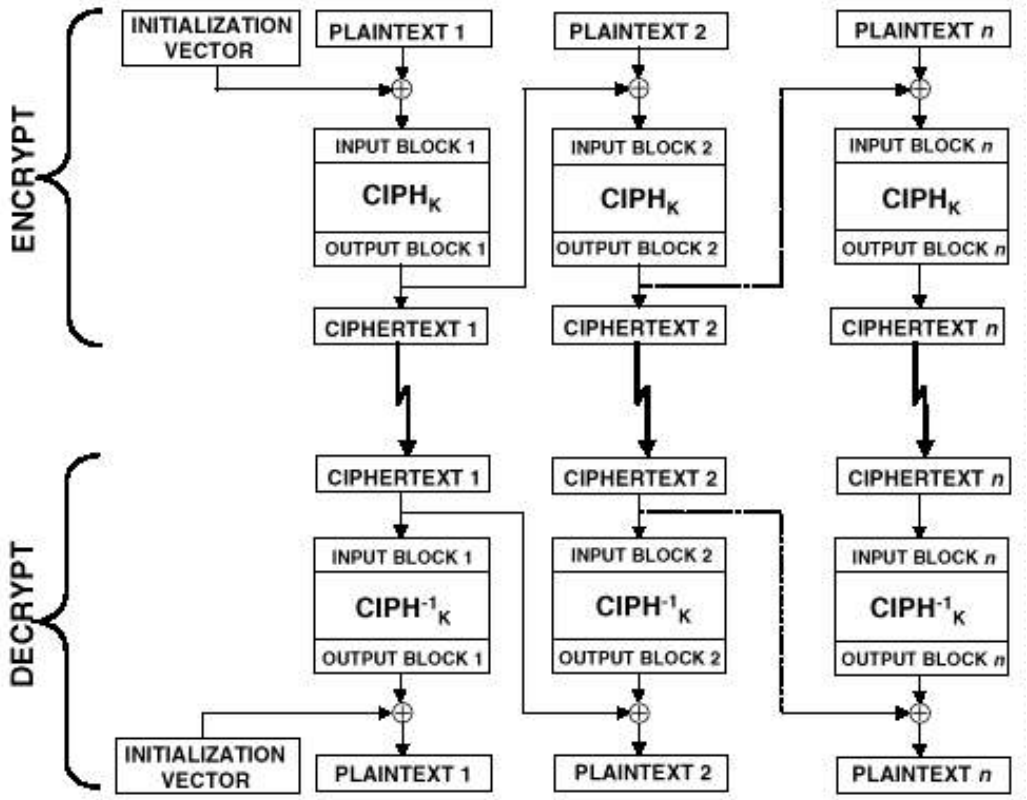

Figure 12 CBC Mode Encryption and Decryption

DES in CBC mode in IEEE 802.16 – 2004 is illustrated in Figure 12. Obviously, DES-CBC only encrypts the MAC Payload, but not MPDU Header or the CRC as seen in Figure 12 DES CBC Mode Encryption Process. Since the information that MPDU headers carry is so crucial, such as 2-bits TEK indicator which is XORed with the PHY synchronization field to calculate the Initialization Vector and as the PHY synchronization field is "repetitive and predictable" (David Johnston and Jesse Walker, 2004) MPDU initialization Vector can be calculated easily.

The standard provides three encryption methods for TEKs with key encryption keys (KEK); 3-DES, RSA and 128-bit AES.

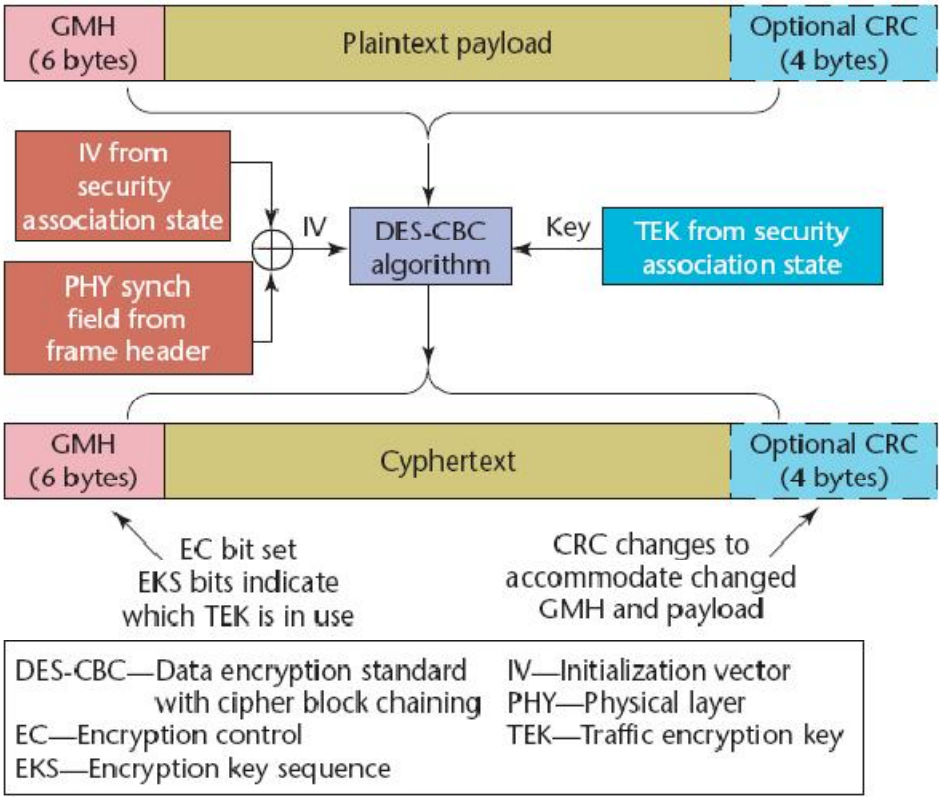

Figure 13 DES CBC Mode Encryption Process (David Johnston and Jesse Walker, 2004)

Another data encryption method is to use AES in Counter with CBC-MAC (CCM) mode. AES also called Rijndael was designed by Vincent Rijmen and Joan Daemen. Moreover, AES which was selected as the most suitable block cipher by the National Institute of Standards and Technology (NIST) became a widely used encryption algorithm. 128-bit block length and is used and 128, 192, and 256-bits key lengths are supported by AES. (The Internet Engineering Task Force) defines CCM as "a generic authenticated encryption block cipher mode". The CCM parameters defined by NIST CCM are; the number of octets in authentication field, the size of length field, and the length of additional authenticated data string.

4.2.2 Message Digest Method

Message digest also known as checksum, digest or hash value is a cryptographic hash function which transforms a message to a fixed-size string for the purpose of providing message authenticity. The standard IEEE 802.16 – 2004 calculates message digests using hash-based Message Authentication Coding (HMAC) with the Secure Hash Algorithm

(SHA-1). The downlink authentication key is HMAC_KEY_U and the uplink authentication key is HMAC_KEY_D. Both are derived from the AKs as described in the next section.

4.3 Key Derivations and Management in PKMv1

After successful authorization by RSA authorization in PKMv1 in other word BS authenticates SS and sends the Message 3 to SS which contains AK. It is aimed that AK is shared only between BS and SS. However, the more usage of the AK leads to get easier revealing too much information to the third parties. An example is that The AK is used to derive KEKs and the standard doesn't control the AKs generation. Afterward KEK is for generating TEKs in the PKM. The generation flow of PKMv1 is shown in Figure 14.

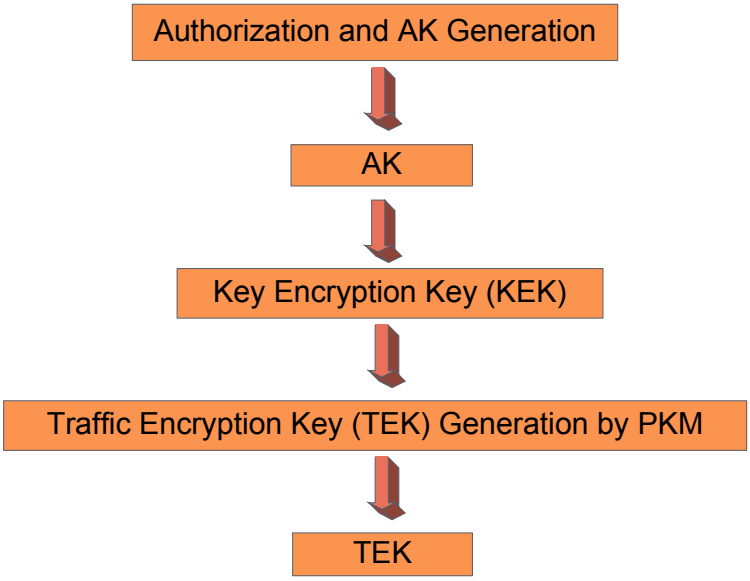

Figure 14 TEK Generation flow in PKMv1

AKs, TEKs and IVs are generated by BS which brings vulnerability for the keys and consequently for the BSs and SSs. Specifically, creating keys just from the one side which is BS might be crucial if the BS is compromised by the intruders as the rogue BS might send forge AKs in order to introduce itself as an uncompromised BS to the target SS. In addition, random or pseudo-random number generators may be used to generate AKs, TEKs and IVs. Using cryptographic methods described above, TEKs, KEKs and message

authentication keys are derived from 128-bit AK as follows;

KEK = Truncate (SHA1 (AK ¦K_PAD_KEK), 128]), Where K_PAD_KEK = 0x53 repeated 64 times and truncate(x,n) denotes the result of truncating x to its left most n bits

The derivation of HMAC Authentication Keys as folows;

HMAC_KEY_D = SHA1 (H_PAD_D ¦ AK)
HMAC_KEY_U = SHA1 (H_PAD_U ¦ AK)
HMAC_KEY_S = SHA1 (H_PAD_D ¦ Operator Shared Secret)

with

H_PAD_D = 0x3A repeated 64 times
H_PAD_U = 0x5C repeated 64 times

A Privacy and Key Management Protocol establishes a data SA between SS and BS. The message traffic includes two or three message exchanges among BS and SS, since the first message is optional for rekeying. The messages that are sent between BS and SS in PKM protocol are illustrated in Table 3 and the terms used in the PKM message exchange are described in Table 4.

Message 1: SS to BS: *SeqNo ¦ SAID ¦ HMAC(1)* (Optional)
Message 2: ***Key Request***
SS to BS: *SeqNo ¦ SAID ¦ HMAC(2)*
Message 3: ***Key Reply***
BS to SS: *SeqNo ¦ SAID ¦ OldTEK ¦ NewTEK ¦ HMAC(3)*
Where" ¦ " means bit-string concatenation

Table 3 PKM Protocol Message Exchange between BS and SS

Term	*Description*
Seq No	Sequence number of the AK used for exchange
SAID	The ID of the data SA
HMAC(1) and (2)	The HMAC-SHA1 digest of SeqNo and SAID, HMAC(1) for the downlink and HMAC(2) for the downlink
OldTEK	The previous-generation TEK's IV with remaining lifetime and TEK sequence number for the data SA which is indicated with 2-bits
NewTEK	The next TEK's IV with remaining lifetime and TEK sequence number which is 1 greater than the old one
HMAC(3)	The HMAC-SHA1 digest of SeqNo, SAID, OldTEK, NewTEK under AK's downlink HMAC key

Table 4 Terms used in PKM message exchange (based on (David Johnston and Jesse Walker, 2004))

Message 1 is optional and BS never uses it except rekeying a data SA or creating a new SA. HMAC(1) digest of SeqNo and SAID is used for the purpose of avoiding SS from the forgery attacks. However, Message 2 is used by SS in order to request SA parameters. There are two option for SS to take SAIDs; one from SAID lists or from a Message 1 with valid computation of HMAC(1) (David Johnston and Jesse Walker, 2004). By means of calculating HMAC(2), BS can avoid from the forgery attacks. In the case of HMAC(2) is valid and SAID belongs to one of the SS, BS configures the SA with targeted SS using Message 3. Finally, SS can detect forgeries via HMAC(3).

CHAPTER 5

5 PKMv2

Together with IEEE 802.16e – 2005, advance security features have been introduced such as the second version of Privacy and Key Management protocol (PKMv2). PKMv2 similar to PKMv1 aims to produce AK by means of enhanced security elements for instance RSA authentication scheme with Extensible Authentication Protocol (EAP), or just RSA and EAP authentication options which provide mutual authentication between BS and Mobile Station (MS) unlike PKMv1. Moreover, new key encryption method, AES with key wrap, has been introduced and AES in Counter (CTR) mode for Multicast and Broadcast Service (MBS) is just another improvement for the data encryption. Lastly, although the definition of pre-authentication mechanism and procedure hasn't been made as it is out of the scope of the standard, many pre-authentication methods have been proposed over the years in order to facilitate handover process and to support mobility for mobile WiMAX networks with the low latency.

In this section, these variations will be analyzed by highlighting important points and identifying the pros and cons of each of these innovations comparing to PKMv1.

5.1 KEY MANAGEMENT PROTOCOL

As highlighted in previous sections, PKM protocol supports both mutual authentication and unilateral authentication using either EAP, or RSA public key encryption algorithm or RSA authentication followed by EAP authentication or EAP-in-EAP mode and for the key exchange robust encryption algorithms are used. The common aim of these authentication schemes is to establish a shared secret AK which is then used to secure

subsequent TEK exchanges between MS and BS. A unique manufacturer issued X.509 digital certificate in the case of RSA authentication and an operator-specified credential in the case of EAP-based authentication are presented by MS to BS so that BS can authenticate MS to access the network (IEEE Std 802.16e, 2006). Figure 15 gives an idea for the overall TEK generation flow and the main steps to produce it.

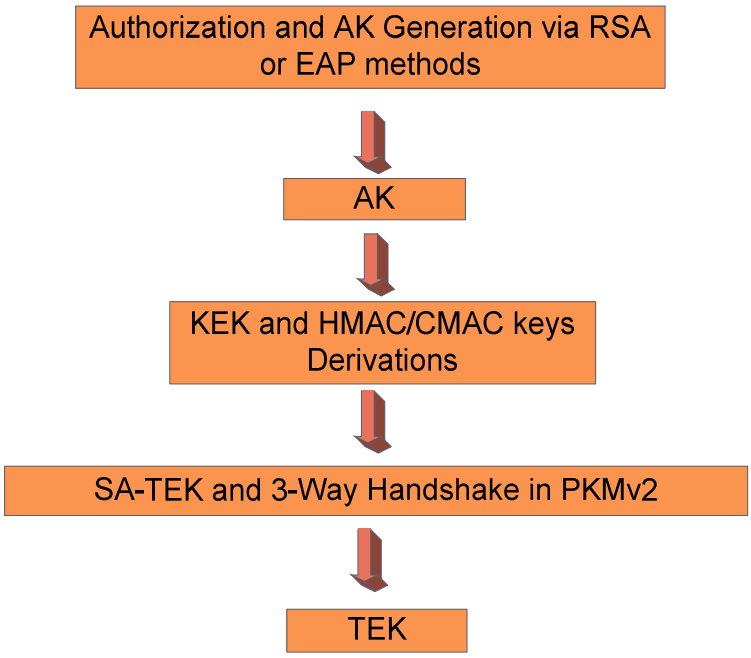

Figure 15 TEK Generation Flow in PKMv2

5.2 AUTHORIZATION AND AUTHENTICATION

PKMv2 authorization and authentication processes are illustrated in

Table 5 and the contents of the authentication authorization messages are explicitly defined in Table 6. Sending Auth_Info message which includes MS's X.509 certificate, MS starts the authorization process. By ways of this, MS can identify itself to the BS. Then, Auth_REQ message follows it requesting AK and SAID from BS. Upon receiving Auth_REQ message, BS checks the MS's certificate and, if it is valid, BS determines the encryption algorithms and supported protocols, generates AK and encrypts it with MS's public key using RSA algorithm and lastly sings the whole message using its own private key. This means only MS can decrypt the message and retrieve AK and SAID by using its

private key, in addition, MS now is capable of checking if the BS is the expected BS using the BS's public key. The message also includes MS_Random, BS_Random, BS_Signature and BS_Certificate which Auth_RSP in PKMv1 doesn't comprise. By way of these attributes, mutual authentication becomes a reality in PKMv2 as MS can identify the identity of the target BS. Consequently, a forgery attack from a rogue BS is avoided.

Message 1: ***Auth_Info***

MS to BS: CA_Certification of MS

Message 2: ***Auth_REQ***

MS to BS: {*MS_Random* ¦ *Cert_MS* ¦ *Capablilities* ¦ *Basic CID}*

Message 3: ***Auth_RSP***

BS to SS: {*MS_Random* ¦ *BS_Random* ¦ *Cert_MS* ¦ *Encrypted AK* ¦ *AK lifetime* ¦ *AK SeqNo* ¦ *SAID* ¦ *Cert_BS* ¦ *BS_Signature}*

Message 4: ***Key_REQ***

MS to BS: {*AK SeqNo* ¦ *SAID* ¦*MS_Nonce* ¦ *HMAC/CMAC*}

Message 5: ***Key_RSP***

BS to MS: {*AK SeqNo* ¦ *SAID* ¦ *OldTEK* ¦*New TEK* ¦*Nonce_MS* ¦ *HMAC/CMAC*}

Where" ¦" means bit-string concatenation

Table 5 PKMv2 Authorization and Authentication Processes

Attribute	**Content**
MS_Random and BS_Random	64-bit random number generated in MS and BS
Cert_MS	MS's X.509 Certificate including MS's public key
Capabilities	Requesting MS's security capabilities
Basic CID	Connection identifier (first static CID assigned to MS from BS during initialization process)
AK lifetime	The time that AK expires and MS needs to refresh the AK
AK_SeqNo	64-bit sequence number to distinguish successive AK generations

Table 6 Attributes in Authentication and Authorization Messages

5.3 TEK EXCHANGE OVERVIEW

TEK exchange for Point to Multipoint (PMP) topology is targeted rather than mesh topology in this section. Depending on their policy BS and MS may agree on "No authorization" in which case neither SA-TEK handshake nor Key request reply handshake is performed. On the other hand, after successful authentication and authorization, MS triggers TEK state machine for each SAID identified in the Authorization Reply or PKMv2 SA-TEK-RSP message for the data traffic encryptions. These TEK state machines are responsible for managing keying material which is associated with the respective SAIDs and needs to be refreshed periodically by the MS and its TEK state machines. Moreover, TEK state machines remain active in these cases;

1. The MS is authorized to operate in the security domain of BS which means MS has a valid AK.
2. The S is authorized to participate in that particular SA, in other word the BS keep refreshing the keying material.

Depending on their ciphersuites of SAs, TEKs and KEKs might be 64-bit or 128-bit. For instance, for the ciphersuites employing DES-CBC mode the TEK is encrypted by 3-DES and for the cipher suite employing 128-bit encryption method such as AES-CCM mode, the TEK is encrypted with a 128-bit key derived from AK.

5.4 RSA-BASED AUTHENTICATION

RSA-based authentication scheme yields Primary Authorization Key (pre-PAK) which is sent by BS and shared between MS and BS in order to generate 160-bit PAK. PAK is then used to generate AK. PAK and AK generation flow proceeds as shown in Figure 16 and calculations are made as follows;

PAK = Dot16KDF (pre-PAK, MS MAC Address ¦ BSID ¦ "PAK", 160)

AK = Dot16KDF (PAK, MS MAC Address ¦ BSID ¦ PAK ¦ "AK", 160)

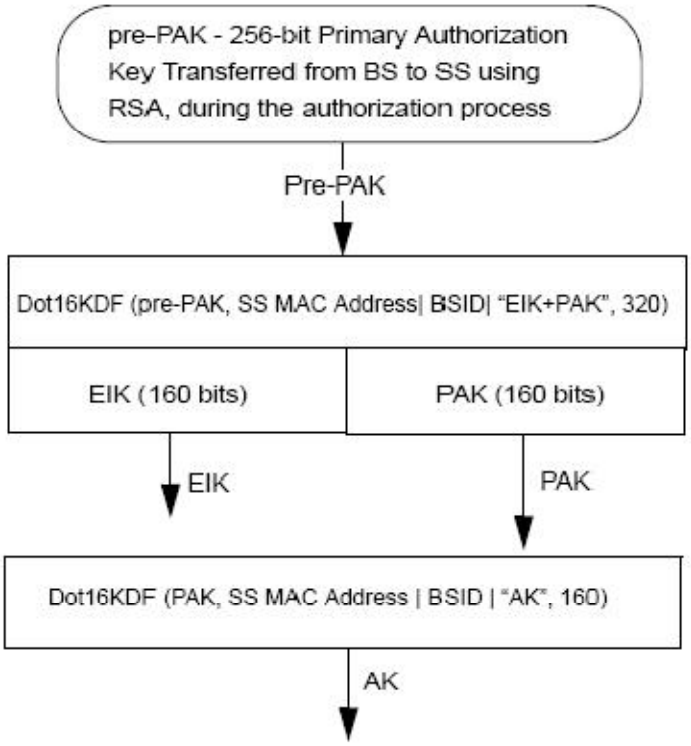

Figure 16 AK derivation from PAK in RSA-based authentication

In PKMv2 RSA-based authentication scheme, the security flaw, unilateral authentication in which BS authenticates MS but MS can't distinguish a legitimate BS from rogue one, provides mutual authentication. Therefore, it is so difficult for an attacker to impersonate a BS.

5.5 EAP AUTHENTICATION

Extensible authentication protocol (EAP) is capable of gathering different authentication methods providing flexibility to the networks to be secured. For this purpose, there are a number of mandatory and optional requirements for EAP methods defined in RFC 4017. The mandatory requirements are as the following;

- EAP method should be capable of generating keys which are used to encrypt authentication messages.
- EAP method should support mutual authentication.
- EAP method should protect itself from the attacks such as eavesdropping, man in the middle and dictionary attacks.

Depending on the type of the network, wired or wireless, the EAP method that needs to be deployed in these networks differentiates. For instance, EAP Transport Level Security (EAP-TLS) and EAP tunnelled TLS (EAP-TTLS) is a certificate-based EAP methods which uses public key certification and provides mutual authentication. Second EAP method is the passport-based EAP authentication method such as Lightweight Extensible Authentication protocol (LEAP) and EAP Subscriber Identity Modules (EAP-SIM) which can be used in smartcard-like devices. In the rest of this section, how EAP works in PKMv2 in mobile WiMAX networks and possible attacks against EAP-based authentication schemes.

If the RSA-based authorization has been used before EAP or EAP authentication has been taken place during EAP-in-EAP mode, the EAP messages might be protected using 160-bit EAP Integrity Key (EIK) which is derived from pre-PAK. Figure 17 illustrates the AK generation by using MSK and pre-PAK which comes from a successful RSA authorization between MS and BS. The product of the EAP exchange between BS and Authentication Authorization Accounting (AAA) server is the 512-bit Master Session Key (MSK). MSK is transferred from AAA to the MS through the authenticator (BS). At this moment, MS and the BS have the same MSK which is then used to generate the PMK truncating it to 160-bit at the both sides. Finally, 160-bit AK derivation takes place through Dot16KDF algorithm.

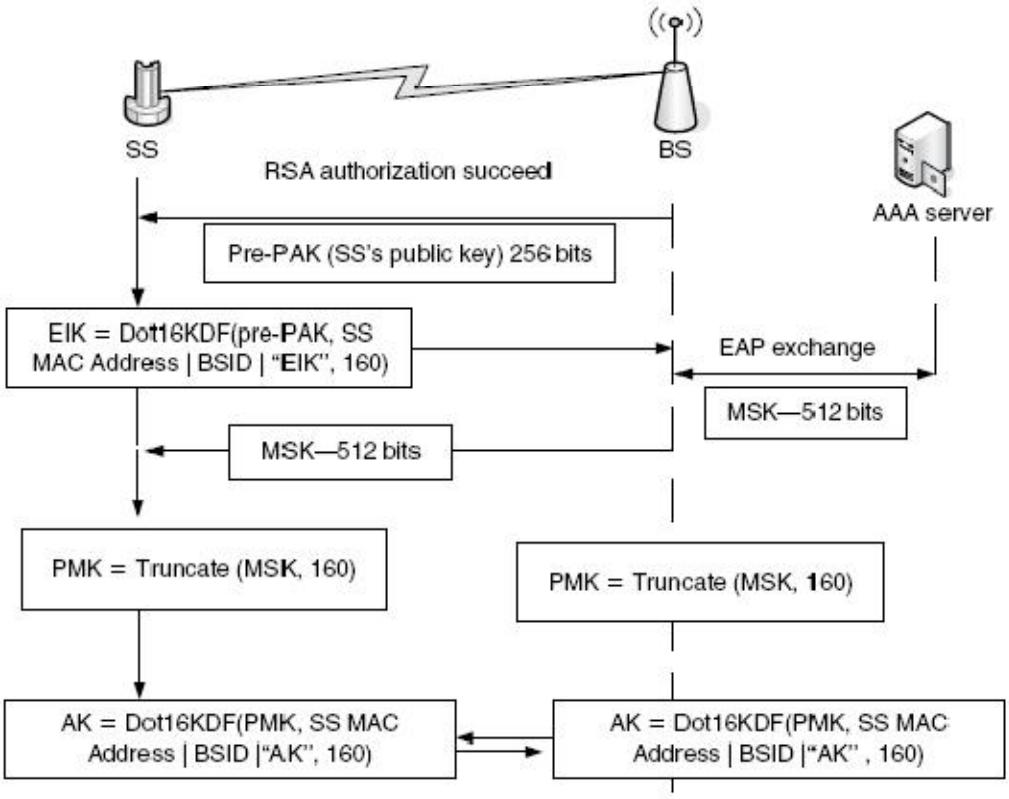

Figure 17 AK Derivation in EAP authorization (Syed Ahson, Mohammad Ilyas, 2008)

Depending on the negotiated authentication policy, following EAP-based authorization EAP-in-EAP mode can be performed. In this case, achieving a successful first EAP, second EAP is triggered by the MS. Once the second EAP is completed, AK is derived in both MS and BS.

One of the possible attacks against EAP methods is the Man in the Middle Attack in which an intruder intercepts all messages transferring between MS and BS and relays them to the victims so that they believe they are communicating privately. On the other hand, by means of EAP-in-EAP mode, the man in the middle attack can be avoided if the first and the second EAP method posses the required criterions. The other potential attacks to EAP methods; Dictionary attacks especially against password-based EAP methods, Denial of Service (DoS) attacks using spoofed authentication response messages (replay attack).

Some other issues with the EAP methods occur during handoff process in the mobile WiMAX networks. In the case of handoff, the mobile subscriber needs to re-authenticate with the target BS while roaming from one BS to another in which case a forged BS might introduce itself to the MS as a legitimate BS. Moreover, if visited network and the home network for MS don't use the similar EAP authentication methods, the authentication procedure becomes more complex.

5.6 SA-TEK 3-WAY HANDSHAKE

After constructing AK with one of the three authentication methods and deriving KEK with the algorithms mentioned in the previous sections, SA-TEK 3-way handshake takes place for the reason of requesting SA parameters. SA-TEK 3-way handshake consists of there messages, namely, SA-TEK- Challenge message, Request message, and Response message. These messages and their contents are presented as depicted in Table 7.

Message 1: ***SA-TEK-Challenge Message***
BS to MS: *BS_Random ¦ SeqNo ¦ AKID ¦ HMAC or CMAC*
Message 2: ***SA-TEK- Request Message***
MS to BS: *MS_Random ¦ BS_Random ¦ SeqNo ¦ AKID ¦MS_Capabilities ¦ Negotiation Parameters ¦ Config Setting ¦ HMAC or CMAC*
Message 3: ***SA-TEK- Response message***
BS to MS: *MS_Random ¦ BS_Random ¦ SeqNo ¦ AKID ¦SA-TEK Update ¦ FrmNum ¦ SADisc ¦ Negotiation Parameters ¦ PKM Config Setting ¦ HMAC or CMAC*
Where" ¦" means bit-string concatenation

Table 7 SA-TEK 3-way Handshake Messages

Message 1 carries the BS_Random which is generated in BS and protects BS from forgery attacks when BS checks the value in the next message that MS sent to it. After receiving SA-TEK-Request message, BS checks the values; AKID, HMAC/CMAC and the BS_Random, in the case of invalid values, the message are ignored otherwise BS checks the security MS_Capabilities. Afterward, BS prepares the third message and sends it to the MS. Following the successful validation of the HMAC/CMAC values, TEKs and the parameters associated with them is installed by MS.

5.7 PRE-AUTHENTICATION

One of the main objectives of the mobile WiMAX is to be able to provide mobile communication without any interference and interrupts, and at the same time to be able to protect the MS from service thefts. In other word, providing mobile communication to the mobile subscribers anywhere and anytime, without sacrificing any special feature of it is their key target. However, since IEEE 802.16e – 2005 doesn't specify the pre-authentication procedure exactly and the authentication methods to be used while roaming from one BS to other, the handover latency and the interruptions while re-authenticating might affect service quality and consequently its market success. The handover process is explained as a block diagram in Appendix.

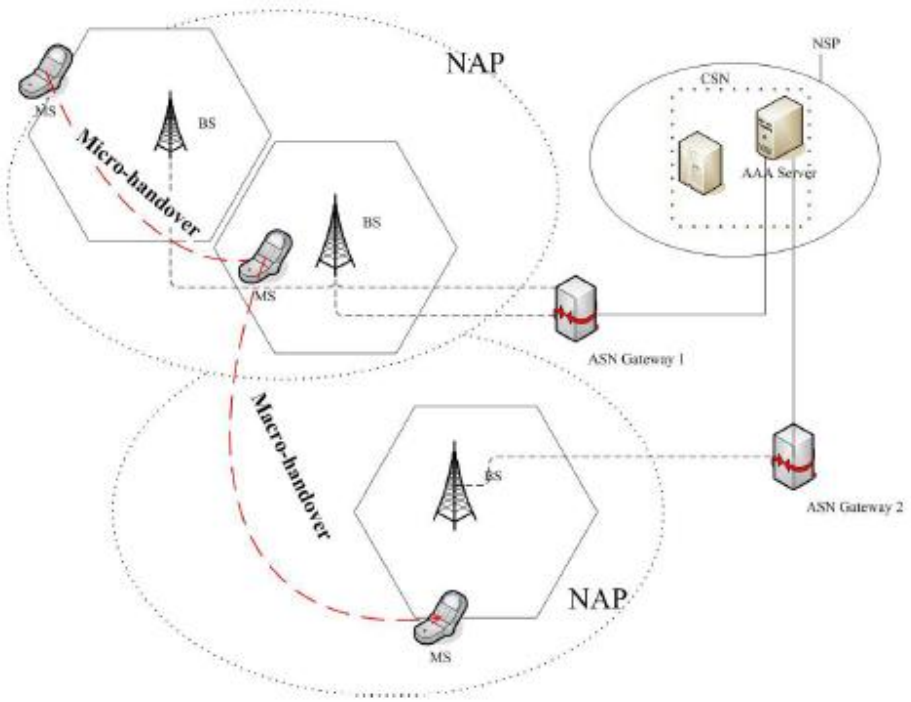

Figure 18 Macro and Micro Handover models in 802.16/WiMAX networks

Figure 18 illustrates Macro and Micro Handover models in WiMAX networks. Micro handover is the process of moving of an MS from one BS to another BS in the same Access Service Network (ASN). On the other hand, Macro handover takes place when a MS roams from one ASN to another ASN, and the problem it causes is more important

than the one in Micro handover. Here is the complete EAP-TLS authentication flow as seen in Figure 19 where the number of steps is 13.

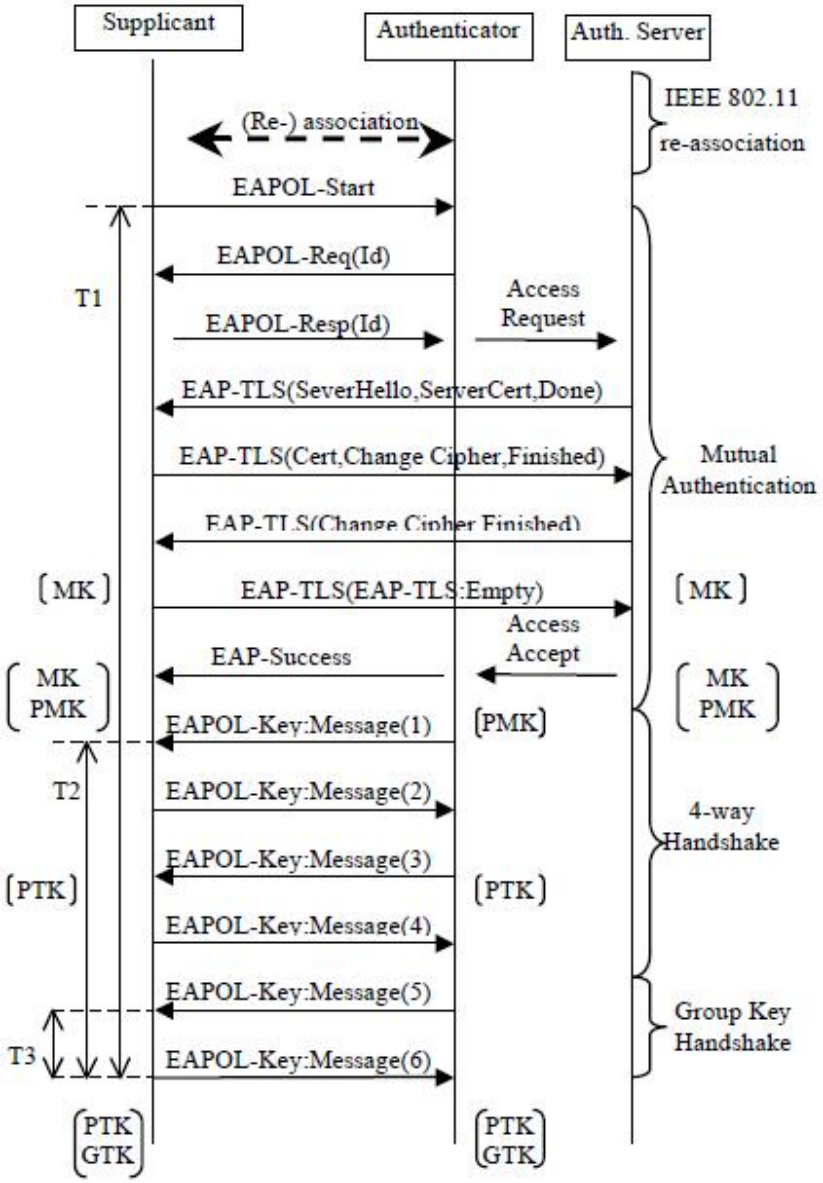

Figure 19 Complete EAP/TLS authentication process (Mohammed Kassab, Abdel Belghith, Jean Marie and Sahbi Sassi, 2005)

For this reason, the slowness of the EAP which is a reality causes an important amount of time consuming while re-authentication. A number of possible solutions have been

studied through the years such as Wireless Public Key Infrastructure (WPKI) for mobile WiMAX networks (see (Hung-Min Sun, Yue-Hsun Lin, Shuai-Min Chen and Yi-Chung Shen, 2007) and Pre-authentication method proposed by (Mohammed Kassab, Abdel Belghith, Jean Marie and Sahbi Sassi, 2005) for 802.11 infrastructure networks.

5.8 KEY DERIVATION AND ENCRYPTION

PKMv2 defines what keys are presented in the system and how the keys are generated. As there are two authentication schemes and two keys yielding from these methods, derivations of AKs are different. RSA-based authentication generates pre-PAK and EAP-based authentication produces the MSK as explained in previous sections. Figure 20Figure 20 illustrates the key generation process overview in PKMv2.

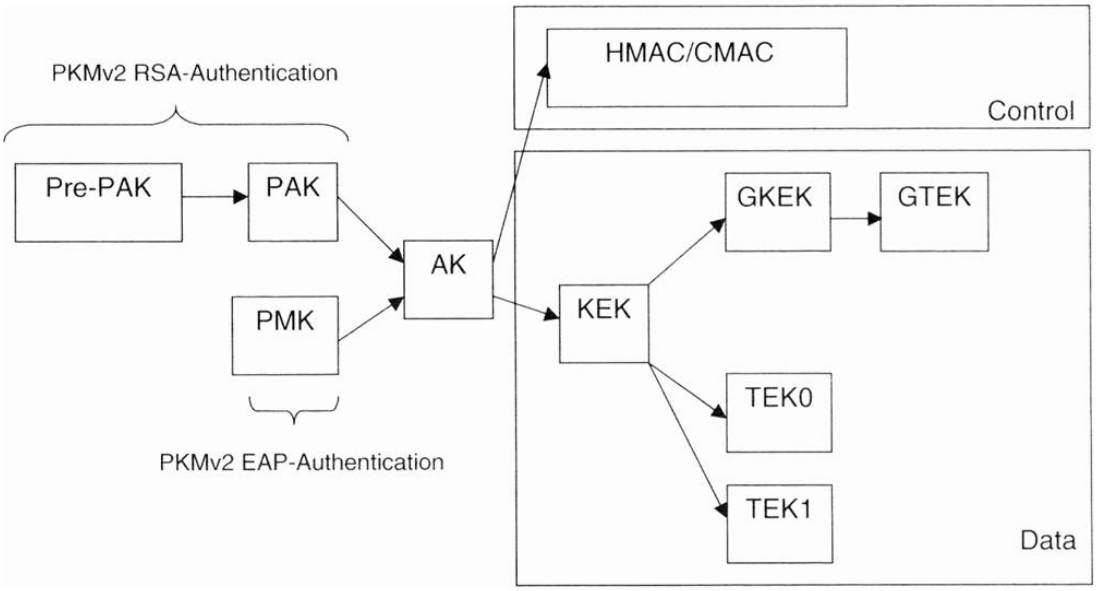

Figure 20 Key Generation Process in PKMv2 (Nuaymi, 2007)

The key derivations are made depending on Dot16KDF algorithm which is a CTR mode construction. If the HMAC/CMAC setting in the MAC is set to CMAC, then the algorithm is defined as follows in (IEEE Std 802.16e, 2006).

```
Dot16KDF (key, astring, keylength)
{
        result = null;
        Kin = Truncate (key,128);
        for (i=0; i<=int ((keylength - 1) / 128) ; i++)
                {
                result = result ¦ CMAC (Kin , i ¦ astring ¦ keylength );
                }
        return Truncate (result, keylength);
}
```

In the case of setting it to the HMAC, the algorithm is defined as;

```
Dot16KDF (key, astring, keylength)
{
        result = null;
        Kin = Truncate (key,160);
        for (i=0; i<=int ((keylength - 1) / 160) ; i++)

                {
                result = result ¦ SHA-1 (i ¦ astring ¦ keylength ¦ Kin );
                }
        return Truncate (result, keylength);
}
```

Another key encryption algorithm for the TEK-128 is AES Key Wrap which the BS encrypts TEK-128 value in Key Reply messages with in order to protect integrity of the keying material. AES Key Wrap defined by the NIST in 2001 consists of two primitives; a block cipher (AES) and a cryptographic hash function (SHA) which means the algorithm provides confidentiality and integrity protection to the keying material and the key itself. Figure 21 depicts the AES Key Wrap encryption motion.

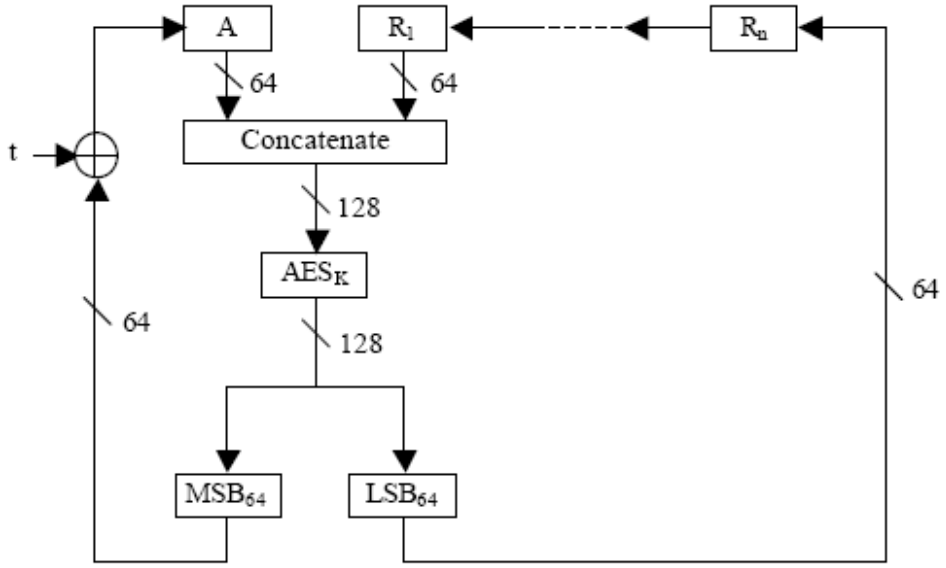

Figure 21 AES Key Wrap

Furthermore, Figure 22 outlines the unicast key hierarchy in PKMv2 beginning from AK and separated into two parts according to HMAC/CMAC hash algorithms.

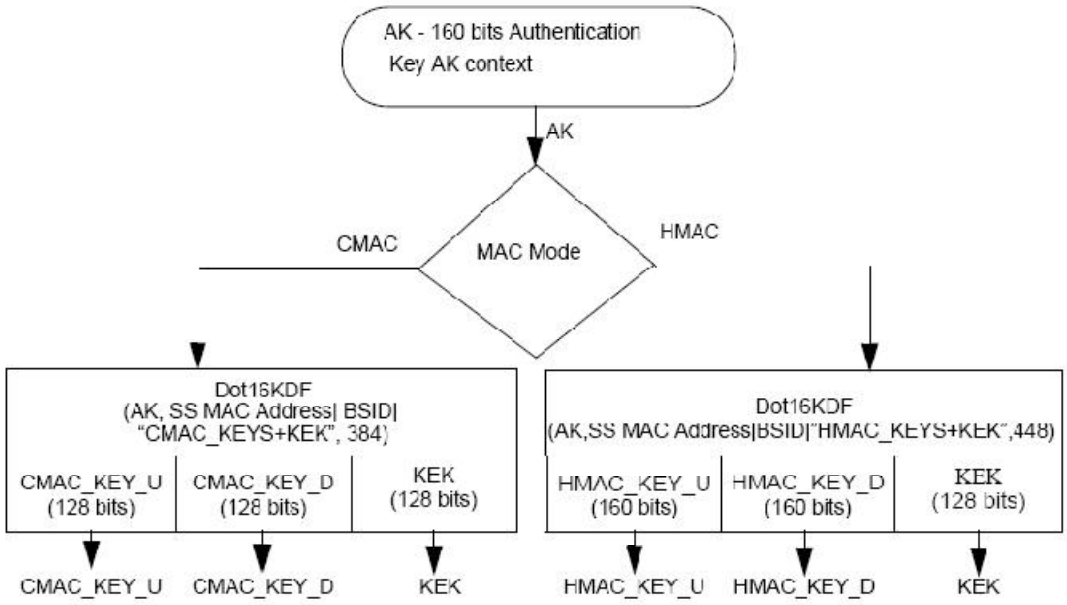

Figure 22 HMAC/CMAC/KEK derivation from AK in PKMv2 (IEEE Std 802.16e, 2006)

CHAPTER 6

6 CONCLUSION AND FUTURE WORK

In growing wireless networks such as mobile WiMAX, security demands play an important role. However, providing secure communication is not a straightforward issue comparing to the wired networks. Therefore, in this thesis, IEEE 802.16e – 2005 / mobile WiMAX is handled. Although, some issues of the previous standard have been solved by means of "e" amendment, but some is still a threat for the systems. In addition, not only the weaknesses are considered as a threat but also the processes which are lack of definitions in the standard. In this thesis, these sorts of issues are studied specially in chapters 3, 4 and 5.

Firstly, in Chapter 2, in order to figure out how WiMAX works and what specifications it has and how worthy this study is, a number of features including pros and cons are researched. This research allows us to notice two main advantages of WiMAX. One is the using OFDM in which case the high speed Non-Line of Sight and multicarrier modulation method enables WiMAX to provide high-bit-data-rate communication with less Inter-symbol interference. Moreover, by using the advantage of being able to use FDD and TDD, it becomes cost-effective solution. In addition, higher data rates could be achieved with advance antenna system that it deploys at receiver and transmitter. Of course, the most impressive one is the supporting mobility, despite of having issues with it such as re-authentication during handover.

In Chapter 3, a comprehensive WiMAX security is studied and introduced in detail, security vulnerabilities of the mobile WiMAX networks are described and the possible malicious usages of them are identified giving the reasons. Mainly, some of the security features of the WiMAX such as the authentication methods, key distribution methods and encryption algorithms are mentioned roughly. Following the introduction to the WiMAX Security, known existing system flaws and the ways that attacker may use are defined in separate paragraphs. According to this study, handover vulnerability which is also analyzed in Chapter 5, initial network entry, initialization vector (IV) vulnerability, and ranging response vulnerability are the most important security deficiencies of the mobile WiMAX networking technology.

Chapter 4 explains PKMv1 with a considerable amount of details which is used in the previous standard IEEE 802.16 – 2004. As it can be foreseen, PKMv1 has more security weaknesses than PKMv2, for the reason of this, the success of the Wi-Fi networking couldn't exceed the average. Most important one is the not being capable of providing mutual authentication and some other is related to (re)-keying material security in which the distribution of key encryption keys (KEK) and traffic encryption keys (TEK) needs to be focused on while authorization and authentication processes.

Finally, Chapter 5 clarifies the differences between PKMv1 and PKMv2. More specifically, comparing the authentication schemes, PKMv2 with four different authentication scheme option namely, RSA-based, RSA-based followed by EAP, EAP-based, and EAP-in-EAP authentication scheme, provides better confidentiality. Moreover, having two different data encryption methods i.e. AES in CTR mode and AES in CBC mode is believed to provide better privacy than PKMv1. In addition to these, using nonce in the key exchange and key distribution mechanism protects MS from replay attacks which differentiate PKMv2 from PKMv1. Lastly, some contribution is made in the pre-authentication subsection regarding with robust and fast handovers while re-authentication. As a result, mobile WiMAX provides robust user authentication with mutual authentication, data privacy with strong data encryption algorithms and data integrity using HMAC/CMAC digests. However, in order to fulfil their aim, mobile

WiMAX security has to be worked on further in particular, interoperability between different networking technologies for which new EAP methods could be a solution, mobility and ultimately efficient micro and macro handover process securities.

7 APPENDIX

7.1 HANDOVER BLOCK DIAGRAM

The first figure shows the handover process at the time MS decides to handoff but as seen from the MS , the second figure is as seen from the serving BS where target BS is selected from.

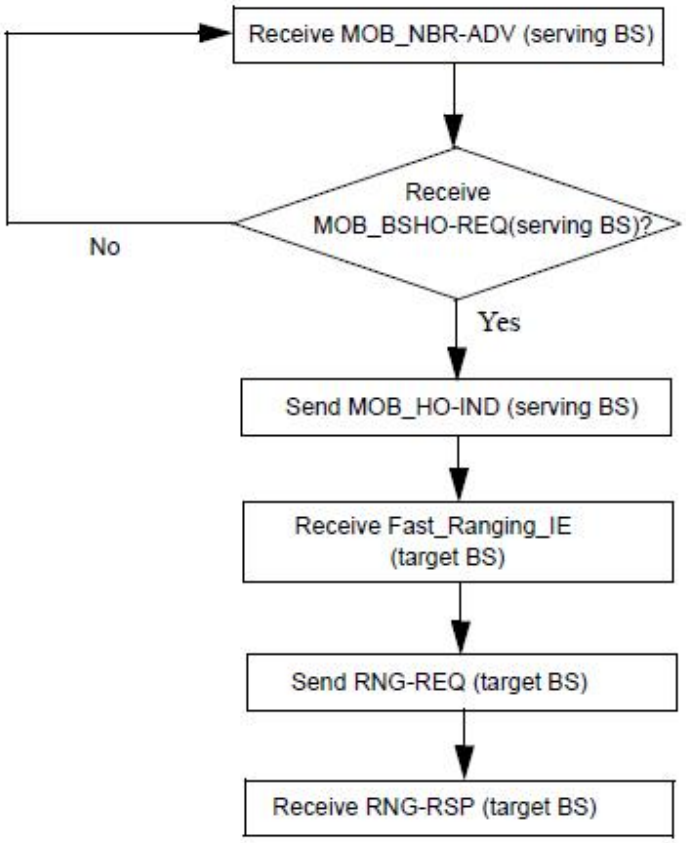

Figure 23 MS initiated Handover Process as seen by MS (IEEE Std 802.16e, 2006).

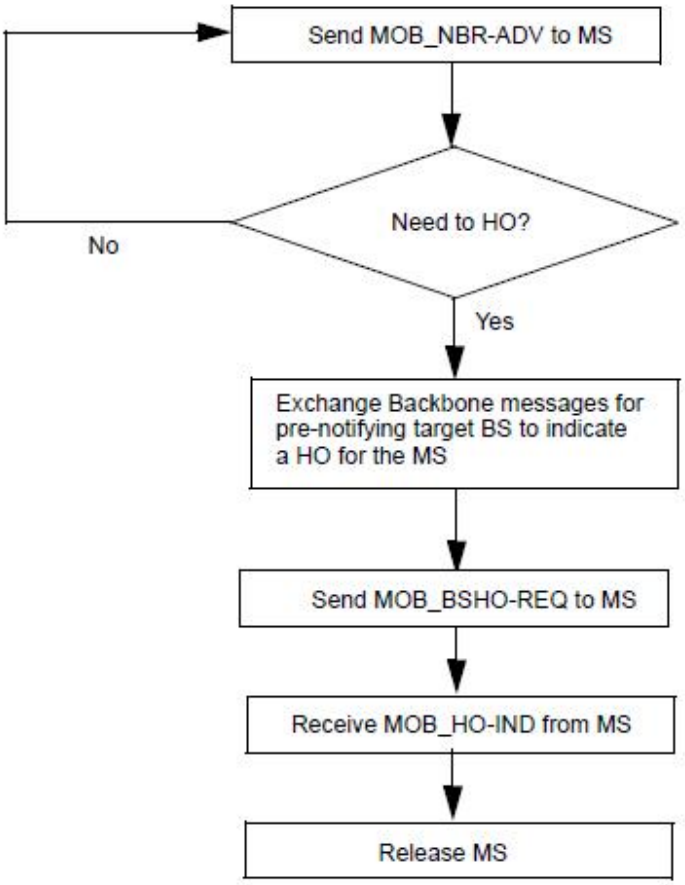

Figure 24 MS initiated Handover Process as seen by serving BS where final target BS is selected by serving BS (IEEE Std 802.16e, 2006).

7.2 ABBREVIATIONS

ABBREVIATION	DEFINITION
AAA	Authentication Authorization Accounting
AKA	Authentication Key Agreement
ANS	Access Network Service
AP	Access Point
AS	Authentication Server
BPSK	Binary Phase Shift Keying
BS	Base Station
BWA	Broadband Wireless Access
CBC	Cipher Block Chain
DES	Data Encryption Standard
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
IKEv2	Internet Key Exchange Protocol version 2
MANET	Mobile Ad hoc Networks
MBS	Multicast and Broadcast Service
MPDU	MAC Protocol Data Unit
MS	Mobile Station
MSDU	MAC Service Data Unit
MSK	Master Session Key
NIST	National Institute of Standards and Technology
PKD	Proactive Key Distribution
PKMv1 and PKMv2	Privacy Key Management Protocol version 1 and version 2
PMK	Pair-wise Master Key
QPSK	Quadrature Phase Shift Keying
RSA	R.Rivest, A.Shamir, L.Adleman
SS	Subscriber Station
TLS	Transport Layer Security
WIMAX	World Wide Interoperability for Microwave Access
WPKI	Wireless Public Key Infrastructure
WTLS	Wireless Transport Layer Security
XOR	Exclusive – or

Table 8 Abbreviations

7.3 GLOSSARY

NLOS: A Service where a small antenna on your computer connects to the tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to Wi-Fi).

LOS: A Service where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz.

TDD: Time Division Duplexing is the system in which theuplink and the downlink use the same frequency but in a different time slots.

FDD: Frequency Division Duplexing is the system in which the uplink and the downlink channels are allocated on different frequencies. For both channels, a fixed duration frame is used. By means of FDD, the usage of both full-duplex SSs and half-duplex SSs can be used simultaneously.

MAN IN THE MIDDLE (MITM) ATTACK: An intruder intercepts all messages transferring between MS and BS and relays them to the victims so that they believe they are communicating privately.

8 BIBLIOGRAPHY

(NIST), N. I. (2008). Retrieved June 2008, from Computer Security Division: Security Technology Group: Cryptographic Standards and Guidelines Cryptographic Toolkit AES-Key Wrap: http://csrc.nist.gov/groups/ST/toolkit/documents/kms/key-wrap.pdf

A.J. Menezes, Paul van Oorschot and Scott A. Vanston. (2001). *Handbook of Applied Mathematics, Fifth Edition.* Taylor&Francis Ltd.

Arunes Mishra, Min Ho Shin, Nick L. etroni, Jr., T.Charles Clancy, and William A.Arbaugh. (2004). Proactive Key Distribution using Neighbour Graphs. *IEEE Wireless Communications* .

Barbeau, M. (2005). WiMAX/802.16 Threat Analysis. *The Association for Computing Machinery (ACM)* .

Carl Eklund, Roger B. Marks and Kenneth L. Stanwood. (2002). IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access. *IEEE Communication Magazine* , 98-107.

Choi, T. S. (2007). An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions. (pp. 88-97). Springer-Verlag Berlin Heidelberg, LNCS 4658.

Crytpome.org. (2008). Retrieved August 2008, from http://cryptome.org/bcm/bcm-f2.jpg

David Johnston and Jesse Walker. (2004). Overview of IEEE 802.16 Security. *IEEE Computer Society* , 40-48.

Forum, M. T. (2006). Technical Standards for Wireless Broadband – WIMAX, MTSBF 001.

Fuqiang Liu and Lei Lu. (2006). A WPKI-based Security Mechanism for IEEE 802.16e. *IEEE Communications Society/School of Electronics and Information Engineering Tongji University* .

Hung-Min Sun, Yue-Hsun Lin, Shuai-Min Chen and Yi-Chung Shen. (2007). Secure and Fast Handover Scheme Based on Pre-Authentication method for 802.16/WIMAX Infrastructure Networks. *IEEE* .

IEEE Std 802.16. (2004). *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems* . New York, USA: IEEE.

IEEE Std 802.16e. (2006). *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2* . New York, USA: IEEE.

Jeffrey Andrews, Arunabha Ghosh and Rias Muhammed. (2007). *Fundamentals of WiMAX.* Prentice Hall.

Junbeom Hur, Chanil Park, Youngjoo Shin, and Hyunsoo Yoon. (2006). An Efficient Proactive Key Distribution Scheme for Fast Handoff in IEEE 802.11 Wireless Networks. *Korea Advanced Institute of Science and Technology (KAIST)* .

Katrin Hoeper and Guang Gong. (2007). Pre-authentication and Authentication Models in Ad Hoc Networks, Wireless Network Security. *Springer Series on Signals and Communication Technology* .

Leonardi Maccari, Matteo Paoli and Romano Fantacci. (2007). Security analysis of IEEE 802.16. *IEEE* .

Matthews, M. (2006). Security Issues in Privacy and Key Management Protocols of IEEE 802.16. USA: Department of Computer Science and Engineering University of South Carolina.

Meyer, E. (2006, 01 15). *WiMax vs WiFi*. Retrieved August 2008, from http://www.techwarelabs.com/articles/other/wimax_wifi/images/wimax-diagram.gif

Mohammed Kassab, Abdel Belghith, Jean Marie and Sahbi Sassi. (2005). Fast Pre-authentication Based on Proactive Key Distribution or 802.11 Infrastructure. *The Association for Computing Machinery (ACM)* .

Moran, M. (2008). Thesis Proposal: A fast Authentication Scheme for Secure Handovers in IEEE 802.16 Networks. Computing and Electronic System University of Essex.

Nuaymi, L. (2007). *WiMAX – Technology for Broadband wireless Access.* John Wiley & Sons, Ltd. England.

Ram Dantu, Gabriel Clothier and Anuj Atri. (2007). EAP Methods for wireless networks. *ScienceDirect Computer Standards & Interfaces* , 289-301.

Syed Ahson, Mohammad Ilyas. (2008). *WiMAX standard and Security.* CRC Press Taylor & Francis Group,LLC.

The Internet Engineering Task Force. (n.d.). Retrieved July 2008, from http://tools.ietf.org/html/rfc3610