UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

UNIFIED SECURITY FRAMEWORKS FOR INTEGRATED WIMAX AND OPTICAL BROADBAND ACCESS NETWORKS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

WEN GU
Norman, Oklahoma
2011

UNIFIED SECURITY FRAMEWORKS FOR INTEGRATED WIMAX AND OPTICAL BROADBAND ACCESS NETWORKS

A DISSERTATION APPROVED FOR THE
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

BY

Dr. Pramode K. Verma, Chair

Dr. Stamatios V. Kartalopoulos, Co - Chair

Dr. Samuel Cheng

Dr. James J. Sluss, Jr.

Dr. William O. Ray

To my Mom & Dad

Acknowledgements

I would like to thank my advisors, Dr. Pramode Verma and Dr. Stamatios Kartalopoulos, for their guidance, help, and support throughout my studies and research in graduate school. I would like to thank the members of my doctoral committee, Dr. Samuel Cheng, Dr. James Sluss, and Dr. William Ray, for their advice and suggestions to improve this dissertation.

I would also like to thank my friends, Xianbo Chen, Di Jin, and Huanhuan Yang, for their help and encouragement during my life in Tulsa.

Lastly I would like to thank my parents for their constant love and support.

Table of Contents

List of Tables

List of Figures

Abstract

This dissertation proposes the integration of optical and Mobile Worldwide Interoperability for Microwave Access (WiMAX) broadband access networks in order to combine the strengths of optical and wireless technologies and converge them seamlessly. To protect the access network security, this dissertation has developed the design of unified security frameworks for the proposed integrated optical and WiMAX broadband access networks.

Ethernet Passive Optical Networks (EPONs) offers a popular broadband access solution, providing high bandwidth and long transmission range to meet users' fast evolving needs. WiMAX provides a wireless broadband solution and it supports mobility. This dissertation proposes a WiMAX over EPON network architecture to provide optical bandwidth for the WiMAX base station (BS). The dissertation also presents a unified security framework for the proposed WiMAX over EPON architecture using public key infrastructure (PKI) and extensible authentication protocol (EAP). The security framework could achieve efficient system management, enhance the system security, and realize unified key management. Furthermore, the dissertation introduces three handover scenarios in the WiMAX over EPON network and describes the corresponding handover schemes based on a pre-authentication method and the communication framework of the ranging step. The proposed handover mechanisms can simplify and accelerate the handover process, compared to the standard WiMAX handover scheme, while keeping the handover procedure secure.

Free Space Optics (FSO) provides a relatively flexible optical wireless solution to provide gigabit bandwidth to areas where fiber is costly or hard to deploy. This dissertation also proposes an integrated Mobile WiMAX and FSO broadband access network and presents a unified EAP-based security framework. The dissertation then evaluates and compares the performance of EAP-Transport Layer Security (EAP-TLS) and EAP-Tunneled Transport layer Security (EAP-TTLS) for the FSO-WiMAX network, and also evaluates the impact of the point-to-point FSO link. Measurements show that, compared to EAP-TLS, EAP-TTLS provides a more flexible, efficient, and secure way to protect the integrated FSO-WiMAX access network. Experiments conducted as part of investigation demonstrate that the point-to-point FSO link does not degrade the performance of EAP authentication in the integrated network.

Chapter 1 Introduction

Abstract: This chapter introduces emerging broadband access technologies including passive optical networks (PONs), free space optics (FSO), and Worldwide Interoperability for Microwave Access (WiMAX). It then gives an overview of network security and access security. Further it presents the motivation for integrated broadband solutions and the need for unified security frameworks. The chapter concludes by presenting the contribution and organization of this dissertation.

1.1 Overview of Emerging Broadband Access Technologies

Since its explosive expansion in the late 20th century, the Internet has become an integral part of people's daily lives and revolutionized the concept of communication and entertainment. An access network refers to the segment of a communication network that connects subscribers to the Internet service provider (ISP). Dial-up access was the earliest and most popular Internet access method during the 1980s and 1990s [1]. The dial-up user connects the computer with an attached modem to an ordinary telephone line and dials into an ISP node to establish Internet connection. Although the dial-up access service is simple and ubiquitous, the full use of a telephone line is required, and the maximum data transfer rate is limited to 56 Kbps, which is slow and causes up to 400 ms latency [2].

In the early 2000s, broadband Internet access technologies started to become available to Internet subscribers and offered wide penetration all over the world (Figures 1.1 and 1.2). The definition of the term “broadband” varies areas around the world and has evolved over time, ranging from 64 Kbps to 2.0 Mbps [3]. The United States Federal Communications Commission (FCC) defines broadband service as data transmission speeds exceeding 200 Kbps in at least one direction: downstream (from the Internet to the user’s computer) or upstream (from the user’s computer to the Internet) [4]. According to the FCC, compared to dial-up connection, broadband access is always on and provides higher data rate and higher quality Internet service with less delay than does the dial up service.

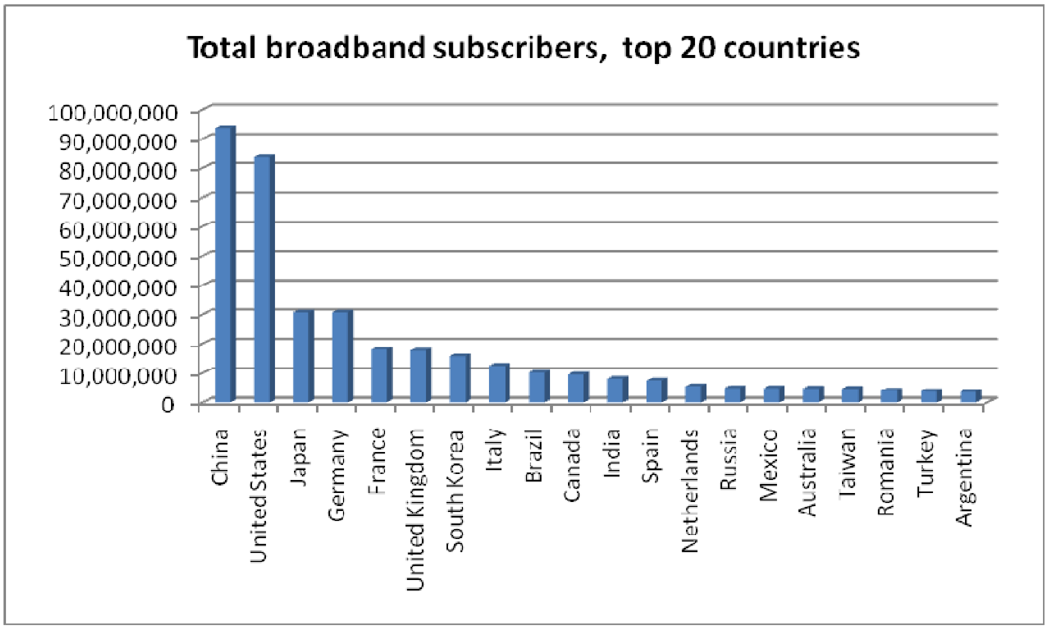


Figure 1.1 Broadband subscribers worldwide [5]

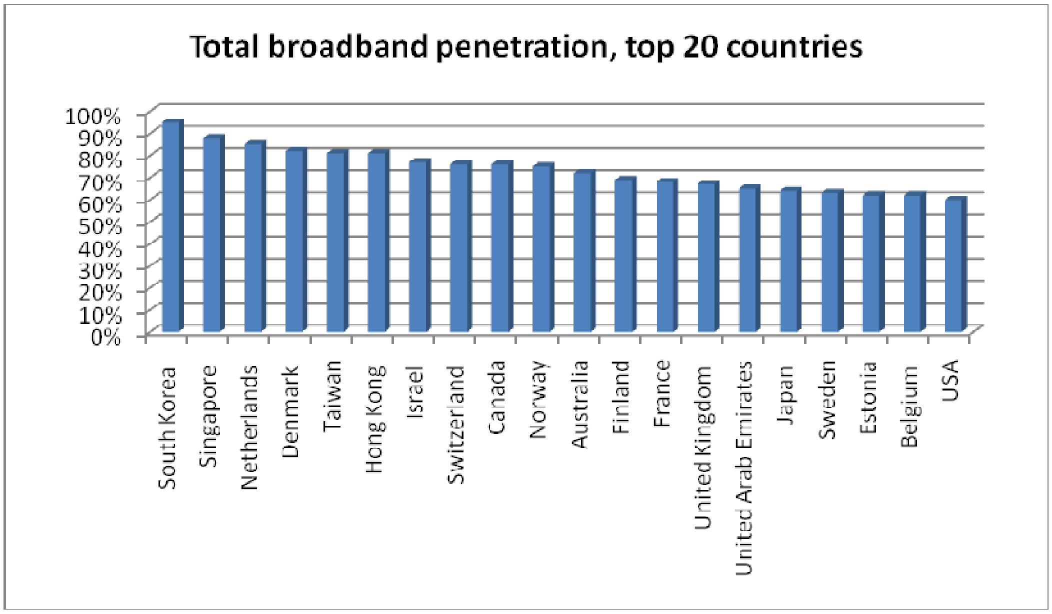


Figure 1.2 Broadband penetration worldwide [6]

Over the last two decades, broadband access technologies have experienced tremendous changes. Digital Subscriber Line (DSL) and cable modem are the two primary broadband access solutions available during the early stage of the broadband development. Compared to the dial-up service, DSL and cable modem provide much higher transmission speed. DSL transmits data traffic over the traditional copper telephone lines, and the most popular Asymmetric DSL (ADSL) offers 384 Kbps to 9Mbps download bandwidth [7]. The cable modem connection delivers data over the existing cable television infrastructure and provides data rates in the range of several megabits per second. However, as the development of large bandwidth-consuming applications, such as, online video conferencing, online gaming, and video streaming since the beginning of this century, DSL and cable modem are constrained by the bandwidth they provide, typically under 10 Mbps, and transmission distance limited to a few kilometers.

Apart from wired solutions, wireless broadband access technologies also play an important part in the consumer market. Wi-Fi defined by IEEE 802.11 [8] is so far the most popular wireless access solution worldwide. It offers up to 54 Mbps shared bandwidth and covers distances less than 100 meters. Wireless stations (such as PCs, laptops, and PDAs) embedded with Wi-Fi cards or devices are connected to access points (APs) that connect to DSL, cable, or Ethernet for broadband connectivity. Wi-Fi hotspots are usually provided at homes, offices, coffee shops, hotels, and airports for short range broadband access services. The concept of municipal Wi-Fi [9] has been introduced recently to cover a whole city or town with wireless broadband access by deploying a wireless mesh network using the Wi-Fi technology in the municipal areas.

In recent years, new broadband access solutions have been explored to provide bigger bandwidth, wider coverage, and better mobility. Such emerging broadband access technologies include passive optical networks (PONs), free space optics (FSO), and Worldwide Interoperability for Microwave Access (WiMAX).

PON provides over 60 Mbps bandwidth for each user and a reach of more than 20 kilometers. PON typically adopts point-to-multipoint topology and consists of an optical line terminal (OLT) that lies in the central office (CO), a passive optical splitter, and optical network units (ONUs) that lie at the subscriber side as shown in Figure 1.3. Two of the most popular PON standards are Ethernet PON (EPON), defined by IEEE 802.3ah [10], and Gigabit PON (GPON), defined by ITU-T G.984 [11]. EPON applies Ethernet technology to the PON network, and data is carried in a modified Ethernet frame while GPON uses GPON encapsulation method (GEM) [12], which encapsulates both asynchronous transfer mode (ATM) cells [13] and packetized data like Internet Protocol (IP) and Ethernet.

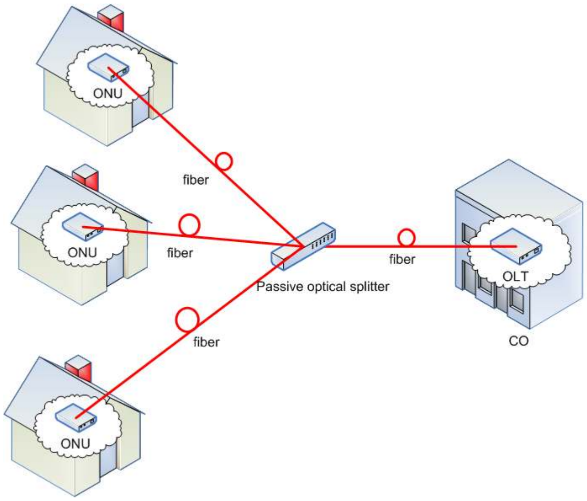


Figure 1.3 Passive optical networks (PONs)

FSO provides a high-speed, cost-efficient alternative optical broadband access solution. A basic point-to-point FSO system consists of two FSO transceivers and a line-of-sight (LOS) optical link between them as shown in Figure 1.4. FSO systems operate in the infrared (IR) wavelength spectrum which is also the range used by fiber optical transmission systems. Therefore, although transmitted in the air, FSO belongs to optical communication. FSO technology offers a data rate up to 2.5 Gbps and reaches distances ranging from less than 100 m up to several kilometers in clear weather conditions [14]. However, FSO communication is affected by attenuation caused by atmospheric effects [14] and is restricted by physical obstructions. FSO mesh networks have been explored to improve traffic management and link protection [15, 16].

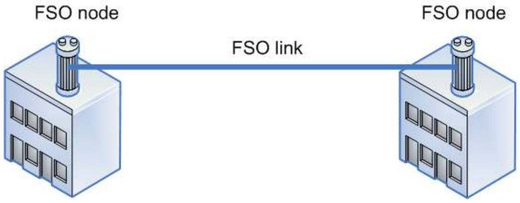


Figure 1.4 Point-to-point free space optic (FSO) system

WiMAX, based on IEEE 802.16 – 2004 [17], defines a fixed broadband wireless metropolitan area network which covers a radius of 50 km (31 miles) and provides up to 75 Mbps bandwidth. Although the maximum transmission distance and bandwidth cannot be achieved at the same time due to the distortion over distances, a WiMAX network is able to reach far beyond the limits of DSL while providing DSL-like speed. Mobile WiMAX, based on IEEE 802.16e – 2005 [18], adds functions and features to the original standard to support mobility. Therefore, WiMAX could provide broadband connections to both fixed locations, e.g., residential areas and business districts, and mobile handsets or moving highway vehicles and trains equipped with WiMAX end devices (as shown in Figure 1.5). In late 2007, mobile WiMAX was included in the International Mobile Telecommunications-2000 (IMT-2000) specification [19] defined by the International Telecommunication Union (ITU) [20], which is known as the third generation (3G). Compared to Mobile WiMAX, Wi-Fi suffers from limited transmission ranges and from security issues, while the 3G cellular data services provide a lower bandwidth at a relatively high price.

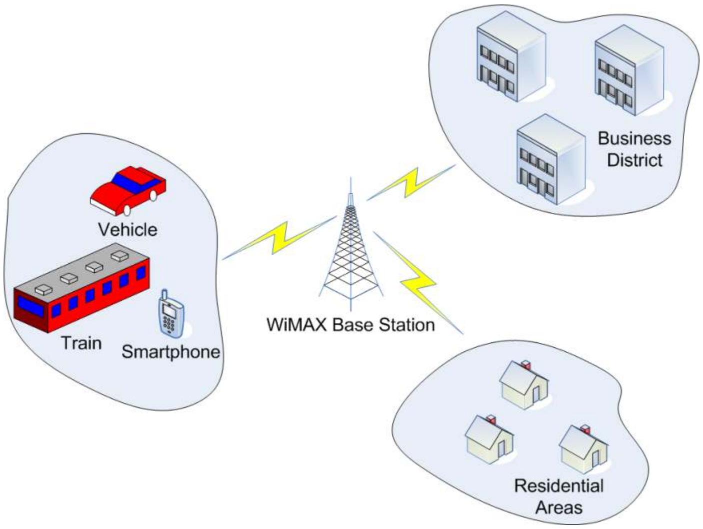


Figure 1.5 WiMAX applications (adopted from [21])

The fourth generation (4G), referred to as IMT-Advanced [19], defined by the ITU Radiocommunication Sector (ITU-R) [22], is currently under development. According to the requirements by the ITU-R, the 4G technology needs to realize target peak data rates of up to approximately 100 Mbps for high mobility such as mobile access, and up to approximately 1 Gbps for low mobility such as nomadic/local wireless access [23]. A new generation of WiMAX, defined by IEEE 802.16m [24], is now under standardization and is expected to satisfy 4G requirements. The 4G technology competing with 802.16m is Long Term Evolution-Advanced (LTE-Advanced) [25], based on Universal Mobile Telecommunications System (UMTS) [26]/ 3G cellular system, developed by the

3rd Generation Partnership Project (3GPP) [27]. Concerning the future of 4G mobile broadband development, WiMAX and LTE-Advanced will likely both exist and evolve to meet different market needs [28].

1.2 Why Access Security

1.2.1 Network Security Overview

The fast growth of broadband access penetration as well as the ongoing 4G mobile broadband development world-wide is creating a ubiquitous environment, and Internet access is provided anytime, anywhere with substantial data rates, which encourage people to rely heavily on the Internet. More and more activities that required travel are now carried out indoors through the Internet, such as online shopping, online banking, and online conferencing. Huge amounts of sensitive data, including personal information, corporate files, and political and military data, are flowing across the Internet, posing various security risks. Therefore, as the world becomes tightly interconnected by the Internet, network security is becoming a more and more important issue.

Three classes of network security functionality are defined in [29] as shown in Figure 1.6: link-by-link, point-to-point, and end-to-end security. Link-by-link security is the security protection implemented between adjacent nodes, which relate to a single physical transmission link. Point-to-point security function is implemented between intermediate nodes of a telecommunication network. It is usually applied by peer network gateways to realize security protection for the user data transmitted between the points. End-to-end security refers to the security functions implemented within the end points of a communication system.

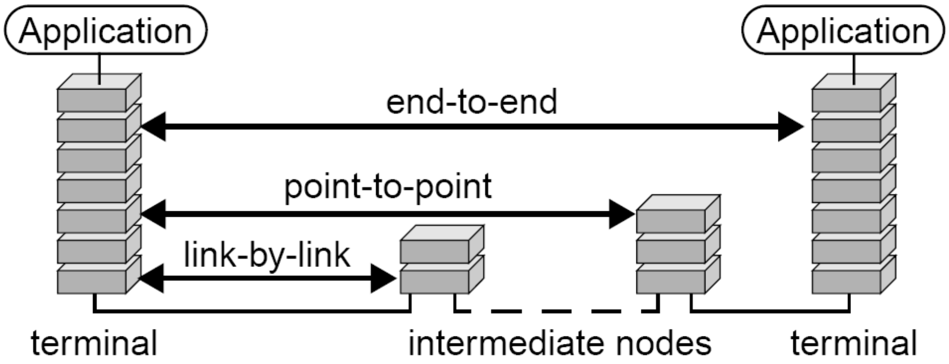


Figure 1.6 Classification of network security functions

From the perspective of the network layered model, link-by-link refers to the lower layer security, such as the data link layer. Point-to-point security usually refers to the IP layer security protocol. Virtual private network (VPN) implemented using IP Security (IPsec) is a good example. End-to-end security corresponds to higher layer security functions, including application layer and transport layer security, both of which are running above the Transmission Control Protocol/Internet Protocol (TCP/IP) infrastructure. Table 1.1 shows the common security protocols in different network layers.

Table 1.1 Common security protocols in different network layers

Layer	Protocol	Security Protocol
Application layer	Simple Mail Transfer Protocol (SMTP)	Pretty Good Privacy (PGP)
	Hypertext Transfer Protocol (HTTP)	HTTP Digest Authentication
Transport layer	Transmission Control Protocol (TCP)	Transport Layer Security (TLS)
Internet layer	Internet Protocol (IP)	Internet Protocol Security (IPsec)
Link layer	IEEE 802.11 (Wi-Fi)	Wi-Fi Protected Access (WPA)/WPA2

1.2.2 Need for Access Security

Access network security, which protects the data path between the subscriber and the ISP, uses link-by-link security but sometimes both link-by-link security and point-to-point security, if more than one network node is involved. Although end-to-end security might also be used in the access network, because it is implemented spanning both the backbone and access network and is not specifically for the access segment, the access network security usually only refers to the lower layer protection.

Compared to the backbone network, the access network is deployed mostly in populous urban areas. Even in rural areas, it is advisable to install broadband networks in locations with a relatively high density of people. Therefore, the intruder has relatively close and easy physical access to the access network, which makes the access network vulnerable to various security threats. The following is a list of three common security attacks.

- Eavesdropping

For wired access networks, the intruder could tap the cable or fiber to implement eavesdropping. For wireless access networks with an inherently broadcast nature, the attacker could easily acquire the wireless signal without being detected.

- Theft of service

A malicious subscriber may alter his identification information or the link layer address to masquerade as an authorized user to connect to the Internet. Therefore, that legal user will be charged for the stolen broadband service.

- Denial of service

In PON networks, because all the broadband subscribers connecting to the same central office share the network resources and bandwidth, the malicious user could overload the network to disrupt the services provided to other subscribers.

To ensure the privacy of the broadband subscribers as well as the normal regulation of the access network, encryption and authentication are two basic and necessary security mechanisms.

- Encryption

A strong encryption method at the link layer is used to ensure both the confidentiality and integrity of the user data. Although higher layer data encryption might be implemented in the access network providing a certain level of security, because the link layer header is still left unencrypted, lower layer encryption is needed to prevent traffic analysis.

- Authentication

There are two levels of authentication: device authentication and user authentication. Device authentication is used to validate the identity of the end device installed on the user side, such as the cable modem and ONU. User authentication is implemented to authenticate the subscriber who is using the end device. User authentication is usually performed following the device authentication. In some circumstances, mutual authentication is necessary where the identity of the ISP also needs to be verified. For example, for a WiMAX network, the end user needs to make sure that the base station he is connecting to is legitimate.

1.3 Motivation for Integrated Broadband Solutions

Among the emerging broadband access technologies, PON provides substantial bandwidth and long transmission distances compared to traditional broadband methods. However, for rural areas with low population density where people are dispersed throughout a very large region, it would be very costly to deploy the fiber network to reach every end user. Second, it is hard to deploy fiber in areas with complex mountainous terrain or to a cluster of small islands. Third, PON lacks mobility. Compared to PON, FSO offers a relatively flexible optical wireless solution to provide up to gigabit bandwidth to areas where fiber is costly or hard to deploy. But an FSO network is restricted by environmental factors and does not provide full mobility.

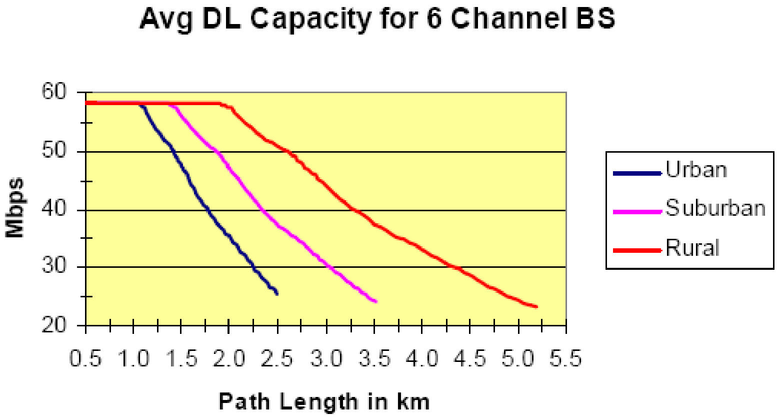


Figure 1.7 Six-channel base station downlink capacity versus range in the 3.5 GHz band[30]

Compared to the optical access network, WiMAX provides a promising wireless broadband solution, which supports mobility and is easier and cheaper to deploy in different types of terrain. Theoretically, WiMAX covers a radius of 50 km (31 miles) and provides up to 75 Mbps bandwidth. However, that doesn’t mean that 50 km and 75 Mbps can be achieved at the same time. Figure 1.7 illustrates a testing result taken from a WiMAX Forum white paper [30] showing a 6-channel base station downlink capacity versus transmission distance in the 3.5 GHz band. A long transmission range and high data rate cannot be achieved at the same time. Longer distances will significantly reduce the bit rates. Therefore, for mobile broadband deployment in rural areas, which are far away from the backbone network, a WiMAX base station needs backhaul bandwidth supply to reach wider coverage.

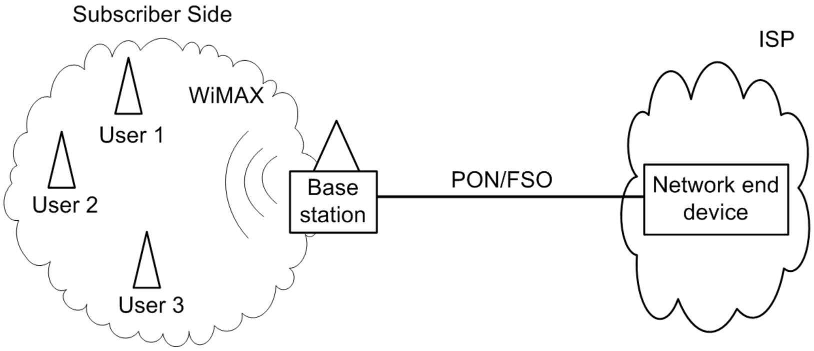


Figure 1.8 Integrated optical and WiMAX broadband access network model

In recent years, integrated optical and WiMAX broadband access networks have been explored to combine the strengths of optical and wireless technologies and converge them seamlessly. As shown in Figure 1.8, the integrated access network uses an optical network to provide huge bandwidth backhaul and a wireless front-end to support mobility. The optical segment could be PON or FSO. In most cases, PON is adopted to provide optical backhaul with a reliable infrastructure and long transmission range. The FSO network provides an alternative optical backhaul solution when the integrated PON and WiMAX access network is not available. Such examples include areas with complex terrain where fiber network is unreachable, city downtown where fiber infrastructure is expensive and time-consuming to deploy, and natural disaster situations where fast temporary network recovery is needed. Compared to pure optical networks, the integrated network saves cost in installation and supports mobility. Compared to a pure WiMAX access network, the integrated network extends the coverage of the overall access networks.

1.4 Need for Unified Security Frameworks

One of the challenges associated with the integrated access network is security. Each broadband technology has its distinct physical characteristic and lower layer management system; therefore, different security frameworks are adopted for different types of access networks.

PON uses fiber infrastructure that belongs to wired transmission. So far, there is no security protocol defined in the EPON standard, and EPON vendors describe and implement their own security mechanisms. FSO works at the physical layer and is transparent to upper layer protocols. So the security framework is subject to the link layer protocol that runs over the FSO system. WiMAX uses radio frequency (RF), which is in the category of wireless communication. A privacy key management (PKM) protocol is defined as part of the security infrastructure by IEEE 802.16 standards [17, 18, 31].

The simple and straightforward security solution for integrated broadband access networks is to adopt both the optical and WiMAX security schemes.

However, the existence of two different security systems suggest that each end-user packet needs to go through encryption and decryption twice between the subscriber side and ISP, and the authenticity of the packet also needs to be verified twice. That fact introduces delay and management cost to the integrated system. Therefore, a security framework which can unify two security systems is needed.

There are three requirements that the unified security framework needs to satisfy:

- Unified

Instead of simply connecting two different access technologies, certain functional integration needs to be achieved. The integrated security system should be able to realize unified control and management, which applies to both the optical and WiMAX networks.

- Secure

The primary requirement is that the integration cannot bring any additional security flaws and vulnerabilities to the integrated access network, and the original security level of either optical and WiMAX segment should be maintained. On the basis of that, the security flaws with each broadband system itself need to be solved by the integrated security framework to enhance the security level.

- Efficient

The unified security framework should bring minimum redundancy and complexity to the integrated access network. Double encryption should be eliminated, and efficient key management protocols need to be adopted to save both cost and time.

1.5 Contribution of the Dissertation

In this dissertation, an integrated WiMAX and optical architecture named WiMAX over EPON that can achieve efficient and unified network management is proposed. In this model, each WiMAX media access control (MAC) protocol data unit (PDU) is encapsulated directly into one EPON Ethernet frame and all the WiMAX MAC management functions are moved from the optical network unit – base station (ONU-BS) to the OLT. Then a unified security framework adopting public key infrastructure (PKI) [32] and extensible authentication protocol (EAP) [33] in the WiMAX over the EPON network is proposed. This protocol could simplify key management and enhance the system security.

Based on the WiMAX over EPON network, the dissertation presents the handover scenarios and corresponding handover schemes. A pre-authentication method for authorization key (AK) pre-distribution and the communication framework of the ranging process are used to realize mutual authentication to accelerate the handover procedure as compared to the standard Mobile WiMAX handover process defined in IEEE 802.16 – 2009.

For areas where fiber deployment is not available, an integrated Mobile WiMAX and FSO access network architecture is presented. Mobile WiMAX is used as the front-end wireless access solution, supported by high capacity FSO at the back end. To efficiently secure both the Mobile WiMAX and FSO access links, the dissertation proposes a unified security framework based on EAP. The performance of two of the most popular EAP methods is evaluated when implemented in the integrated access network: EAP - Transport Layer Security (EAP-TLS) [34] and EAP - tunneled transport layer security (EAP-TTLS) [35]. Furthermore, the dissertation evaluates how the FSO link impacts the performance of EAP-based authentication in the integrated access network. The measurement shows that compared to EAP-TLS, EAP-TTLS provides a more time-saving, flexible, and secure way to protect the integrated Mobile WiMAX and FSO access network. Also the point-to-point FSO link does not degrade the performance of the EAP authentication.

1.6 Organization of the Dissertation

This dissertation is organized as follows. Chapter 2 introduces the background of emerging broadband access technologies including EPON, FSO, and WiMAX. Chapter 3 presents the current security schemes for EPON, FSO, and WiMAX. Chapter 4 proposes the WiMAX over EPON network reference model and Layer-2 and Layer-3 architectures. Chapter 5 describes the proposed unified security framework for WiMAX over EPON and gives related security analysis. Chapter 6 presents the handover scenarios and handover mechanisms for WiMAX over EPON access networks. Chapter 7 proposes the integrated Mobile WiMAX and FSO access network architecture and unified security framework as well as the security analysis. Chapter 8 describes the performance evaluation of EAP-TLS and EAP-TTLS for the integrated Mobile WiMAX and FSO access networks. Chapter 9 concludes the dissertation and provides ideas for future work.

Chapter 2 Emerging Broadband Access Technologies

Abstract: This chapter first introduces this evolution of passive optical networks and presents the network architecture and operation principles of EPON. Then it gives an overview of FSO technology. Further, it presents the network architecture and handover process of WiMAX.

2.1 Ethernet Passive Optical Network (EPON)

2.1.1 Passive Optical Network Evolution

The first passive optical network standard was established in the early ‘90s and was based on ATM which is named APON. It is defined by ITU-T G.983 and was mainly developed in Germany. The typical data rate of APON is in the range of 54 Mbps to 155 Mbps, but as the growing demand of bandwidth from the Internet subscribers exploded, APON was replaced by broadband PON (BPON) which supports 622 Mbps.

As the rapid increase in IP-based applications and the volume of data traffic came along, BPON again could not satisfy the bandwidth demand. At the same time, Ethernet began to prevail and gradually dominate the local area network (LAN). EPON defined by IEEE 802.3ah was completed in 2004 as part of Ethernet in the first mile project [36]. Each EPON OLT provides 1 Gbps bandwidth shared by 16 ONUs, and each ONU can get 62.5 Mbps. The competing technology with EPON is Gigabit PON (GPON), defined by ITU-T G.984. GPON supports 2.488 Gbps in the downstream direction and is shared by 32 or more

ONUs, and each ONU gets approximately 80 Mbps. Both EPON and GPON could reach more than 20 km from the OLT to the ONU. EPON is adopted mostly in Asia while GPON is popular in North America and Europe. The evolution map of PON is shown in Figure 2.1 [37].

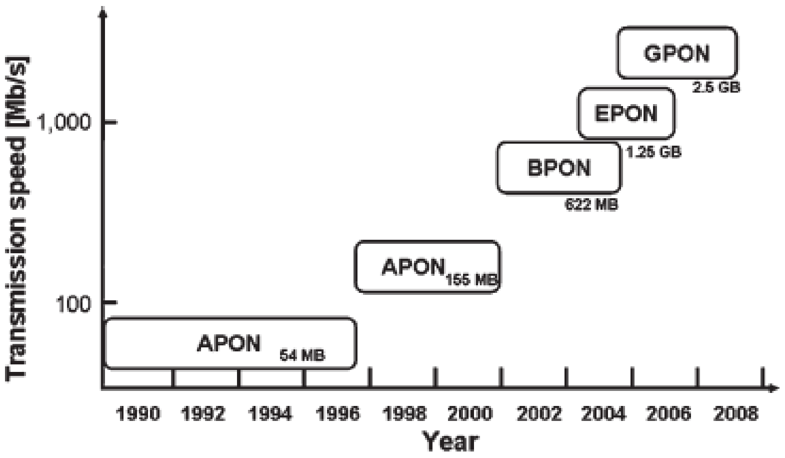


Figure 2.1 Evolution of passive optical networks [37]

In early 2006, the EPON working group also began to work on 10 Gigabit EPON, known as 10G-EPON and now is standardized by IEEE 802.3av [38]. 10G-EPON offers bandwidth capacity over 600 Mbps for each ONU. PONs discussed so far are called time division multiplexing (TDM)-PONs which utilize TDM technology [13]. Another PON technology called wavelength division multiplexing (WDM)-PON [39] is also an active research subject using WDM technology [40]. With the latter technology, a dedicated wavelength is running from the OLT to the ONU, which can give each ONU more than 1 Gbps bandwidth; this bandwidth is then provided to a number of end users [41].

Similarly, PON solutions have been proposed that are capable of delivering elastic bandwidth on demand to end users and to a huge end-user population [42, 43].

2.1.2 EPON Architecture and Operation Principles

2.1.2.1 EPON Reference Model

The layered model for EPON is shown in Figure 2.2. IEEE 802.3ah defines the media access control (MAC) sublayer of the data link layer and the physical layer. The MAC layer consists of the Multipoint MAC Control (MPMC) sublayer and MAC sublayer.

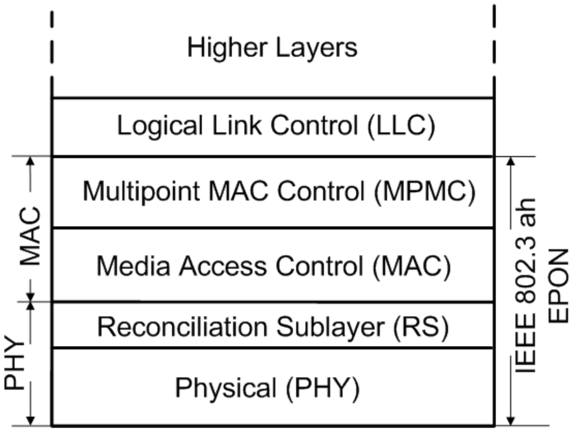

Higher Layers
Logical Link Control (LLC)
Multipoint MAC Control (MPMC)
Media Access Control (MAC)
Reconciliation Sublayer (RS)
Physical (PHY)
MAC
PHY
IEEE 802.3 ah
EPON

Figure 2.2 IEEE 802.3ah reference model

- MPMC sublayer

This sublayer provides the control and manipulation operations for the MAC sublayer. In EPON, the multipoint control protocol (MPCP) [10] is used to reconcile the P2MP topology into the Ethernet framework.

- MAC sublayer

This sublayer provides data encapsulation and medium access management. Data encapsulation function includes framing, addressing, and error detection. Media access management includes media allocation and contention resolution.

- Reconciliation sublayer (RS)

A reconciliation sublayer (RS) is included in the physical layer to interconnect the MAC layer and the physical layer. The RS is used to enable multiple MAC instances to interface with a single physical layer and make the underlying P2MP network appear as a collection of point-to-point links to the higher protocol layers.

2.1.2.2 EPON Frame Structure

As shown in Figure 2.3, the main structure of an EPON Ethernet data frame is the same as a regular Ethernet IEEE 802.3 frame. When the MAC layer frame passes the reconciliation sublayer, a Logical Link Identifier (LLID) is placed at the beginning of each data frame, replacing 2 octets of the preamble to uniquely identify the MAC address of each ONU.

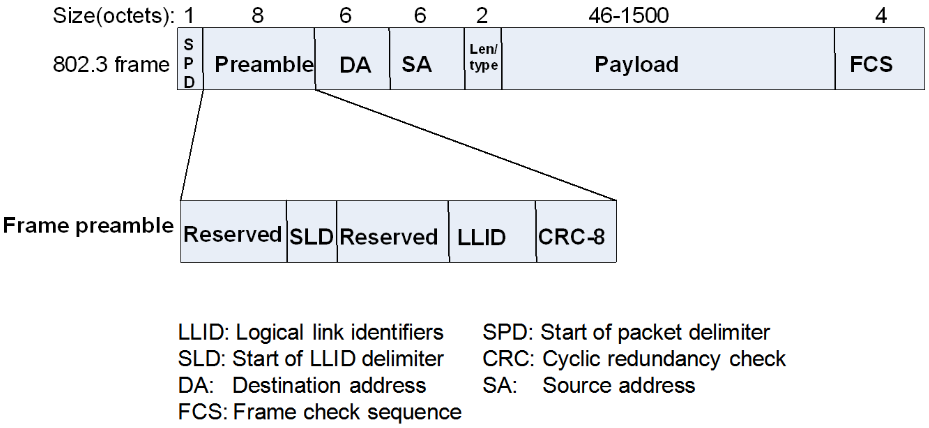


Figure 2.3 EPON frame structure (adopted from [44])

The structure of the EPON MPCP protocol data unit (MPCPDU) is shown in Figure 2.4. The opcode field is used to identify the type of the MAC control frame. The timestamp field values are used to synchronize MPCP clocks for the OLT and ONUs [44]. The opcode-specific fields are responsible for carrying specific MPCP functions, and the rest of the opcode-specific fields that are not used are padded with zeros. The size of the opcode-specific fields is 40 octets, which is a fixed length. Based on the MAC instance used to generate the specific MPCPDU, the corresponding LLID is derived by the RS and placed in the preamble of the MPCP control frame.

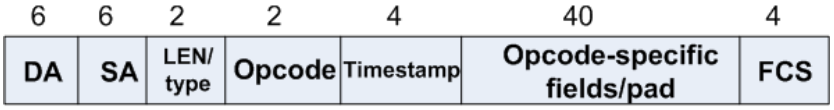


Figure 2.4 MPCPDU structure

2.1.2.3 Auto Discovery Process

MPCP defines two modes of operation: bandwidth assignment mode and auto discovery mode. The bandwidth assignment mode is used to arbitrate the transmission grant for each ONU. The auto discovery mode is used to discover newly activated ONUs and to learn the round-trip times and MAC addresses of these ONUs. The auto discovery operation including authentication and key management is shown as follows.

As shown in Figure 2.5, the auto discovery happens when an off-line ONU registers to the EPON network, and the procedure [10]. Four types of MPCP control messages are used during the auto discovery process: GATE, REGISTER_REQ, REGISTER, and REGISTER_ACK. First, the OLT advertises the discovery grant by periodically broadcasting a discovery GATE message containing the starting time and length of the discovery window. The LLID of this GATE message is set to broadcast since the MAC Control instance is mapped to all ONUs. Upon receipt of this message, the off-line ONU waits for a random time and then sends back a REGISTER_REQ message, which includes this ONU's MAC address and the number of maximum pending grants. The LLID field of the REGISTER_REQ message is still set to broadcast because the MAC Control instance is mapped to an undiscovered ONU.

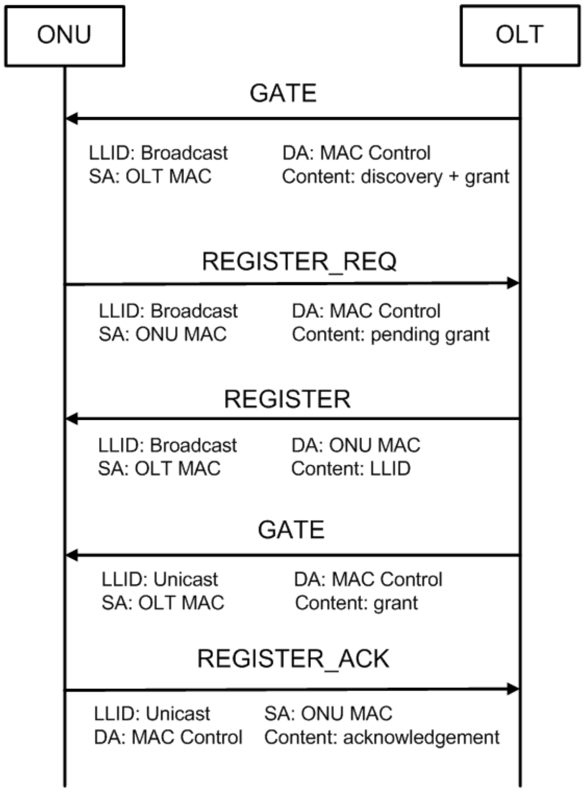


Figure 2.5 EPON auto discovery process

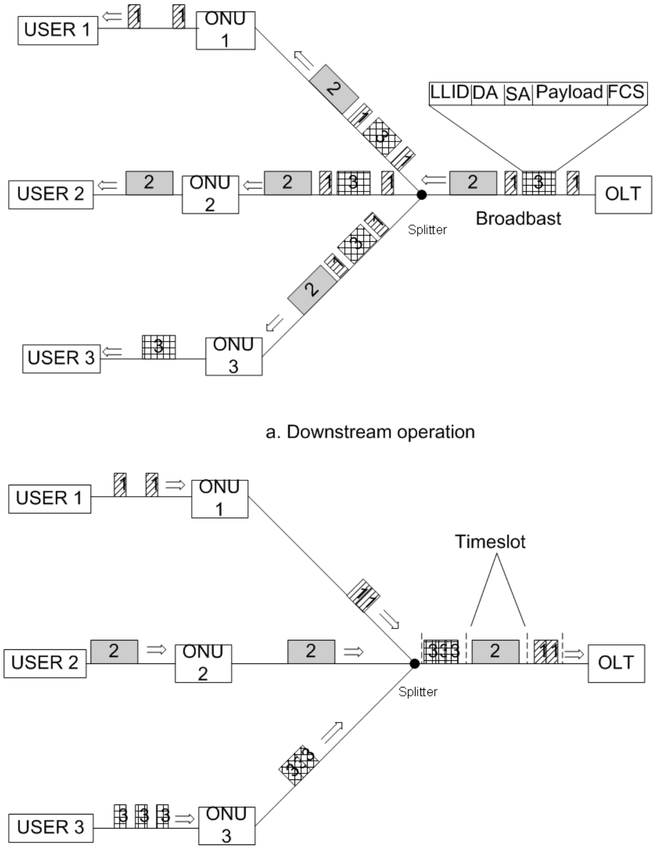
Upon receiving the REGISTER_REQ message, the OLT registers the ONU, allocates and assigns new port identity (LLID) and bonds the corresponding MAC to the LLID. Then the OLT sends a REGISTER message to the newly discovered ONU, containing the ONU's assigned LLID and the OLT’s required synchronization time. The LLID field of this REGISTER message is set to broadcast because the ONU has not received the new assigned LLID yet. After that, the OLT transmits a normal GATE message to grant transmission opportunity to the discovered ONU. This time, the LLID field of this GATE message is set to unicast corresponding to the newly registered ONU. Upon the receipt, the ONU returns a REGISTER_ACK to complete the auto discovery process. The LLID of the REGISTER_ACK is set to unicast mapping to the active ONU.

2.1.2.4 EPON Downstream and Upstream Operations

EPON uses tree topology and consists of an OLT which lies in the center office (CO) and ONUs located at the subscribers’ side. A passive optical splitter is used to split the optical signal to several identical signals. The splitting ratio determines the number of ONUs connected to the OLT.

As shown in Figure 2.6, in the downstream direction, the OLT broadcasts the Ethernet frames to ONUs. Each ONU filters the received frames according to the LLID and only accept frames that have the same LLID as the assigned one by the OLT. In the upstream direction, each ONU is allocated a time slot and only transmits packets during its own transmission window. The time slot is assigned to an ONU dynamically during the auto discovery process according to the number of users and service level agreement (SLA). Frames sent by ONUs in different time slots are time multiplexed and transmitted to the OLT.

Typically two wavelengths are used in EPON: 1490 nm for downstream and 1310 nm for upstream. Sometimes, 1550 nm is used for optional video overlay services. WDM technology is used to multiplex different wavelengths in a single fiber.



a. Downstream operation

b. Upstream operation

Figure 2.6 EPON downstream and upstream operation

2.2 Free Space Optics (FSO)

2.2.1 FSO Overview

FSO is a wireless communication technology that transmits modulated invisible light beams through the atmosphere between remote sites. A basic point-to-point FSO system consists of two FSO transceivers and a LOS optical link between them. FSO has the following advantages over fiber and RF communications:

- **License-free**

Commercially available FSO system works in the IR spectral range around 850 and 1550 nm [14] and no spectrum licensing is required.

- **High capacity**

LEDs and lasers are currently the primary signal sources for FSO. LEDs provide bandwidth typically limited to 155 Mbps while laser sources offer up to 2.5 Gbps speed [14].

- **Immunity to EMI**

FSO is immune from electromagnetic interference (EMI) which is a serious issue for RF communications. Because an FSO link is a narrow beam with line of sight, the chance for interference with other signals is extremely small. However, it may suffer from solar EMI, which with proper design can be minimized or eliminated.

- **Cost efficient and ease of deployment**

Deployment of underground wired network is not needed for FSO, which saves much money and time. An FSO node could be easily installed on the rooftop, by a window or on a high tower, and it can be deployed quickly according to subscribers' needs.

- **Protocol transparent**

FSO works at the physical layer and is transparent to any link layer protocols. Therefore, it can adopt Ethernet, ATM, and SONET.

FSO faces several challenges. First, FSO communication is affected by attenuation due to atmospheric effects [14]. The main atmospheric impairments are dense fog and heavy snow both of which can hinder the passage of light through a combination of absorption, scattering, and refraction [45, 46]. Therefore, an FSO network is preferred in areas where fog and snow are rare. A backup RF link may be used in parallel with the laser beam [16]. RF links provide less bandwidth but are much more reliable and are not affected as much by fog and snow. Scintillation is another atmospheric effect caused by heated air rising from heated matter and air.

Second, because of the LOS requirement, FSO transmission is restricted by physical obstructions and topology. Multi-beam systems (spatial diversity) could be used to address temporary obstructions and provide high availability. Third, simple movement of an FSO node causes misalignment. Studies in mobile FSO technology [47-50] have been performed to maintain LOS connection during the movement of the mobile FSO node. However, mobile FSO technology has high requirements for optical alignment and tracking equipment, optical alignment and auto-tracking technology is needed. Therefore, mobile FSO is suitable for relatively low speed moving object due to its LOS characteristic. An RF access network is still the optimum choice for the front end to reach mobile subscribers.

2.2.2 FSO Network Topology

As shown in Figure 2.7, the most basic and common FSO network topology is point-to-point, which is simple, cost effective, and easy to deploy. However, a point-to-point FSO system does not provide protection and has limited connectivity and capacity.

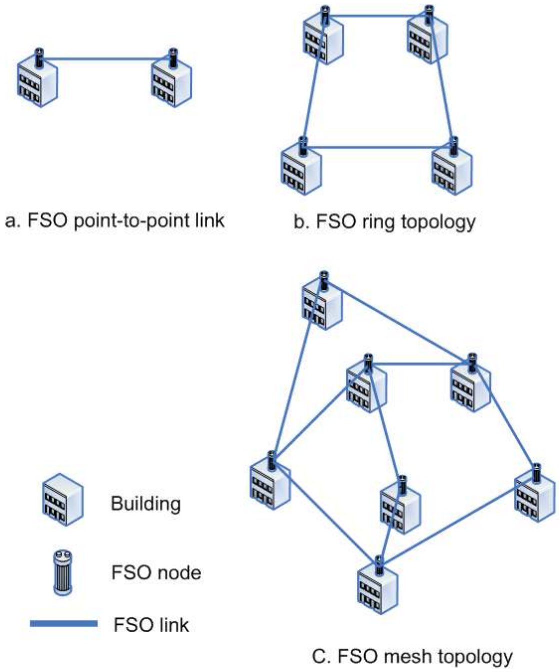


Figure 2.7 FSO link topology

FSO networks with ring and mesh topologies, as shown in Figure 2.7b and 2.7c, respectively, interconnect multiple locations over larger areas and provide better link and service protection and offer better traffic management and load balancing than point-to-point FSO networks. Compared to the ring topology, although the mesh topology adds to the management complexity and increases deployment cost, FSO networks with mesh topology offers better routing, enhanced protection and more traffic capacity [15, 16].

2.3 Worldwide Interoperability for Microwave Access (WiMAX)

2.3.1 WiMAX Overview

Fixed WiMAX is defined by IEEE 802.16 – 2004 [17], and Mobile WiMAX is defined by IEEE 802.16e – 2005 [18]. The most current IEEE 802.16 – 2009 standard [31] is a revision of IEEE 802.16 – 2004. It also consolidates material from IEEE 802.16e – 2005 and other previous 802.16 standards. Both licensed and unlicensed spectrums are available for WiMAX: licensed bands in the 2-11 GHz and 10-66 GHz range, and license-exempt bands in the 2-11 GHz range [17]. Each WiMAX subscriber station (SS) has a 48-bit universal MAC address. Each base station (BS) has a MAC address as well as a base station ID (BSID), which is used for operator identification.

Two modes are supported in IEEE 802.16: the point-to-multipoint (PMP) mode in which the SS only communicates with the BS and the mesh mode in which the SS can talk directly to other SSs. This dissertation will consider only the PMP mode in the integrated access networks. In 802.16 -2004, SS is used to represent the end user, while in 802.16e – 2005, mobile station (MS) is used. In this dissertation, those two terms are used interchangeably.

The reference model defined in IEEE 802.16 is shown in Figure 2.8. The WiMAX MAC layer consists of a service-specific convergence sublayer (CS), MAC common part sublayer (CPS), and a security sublayer. The CS accepts higher layer PDUs such as ATM and IP. Multiple CS specifications are provided for interfacing with various protocols. Based on their classification and quality of service (QoS) parameters, these PDUs are classified and mapped into MAC service data units (SDUs). At the MAC CPS, the core MAC functions are provided, including system access, bandwidth allocation, connection establishment, and connection maintenance. The MAC SDUs are mapped and classified to particular MAC connections, and MAC PDUs are constructed. The security sublayer provides data encryption and authentication services.

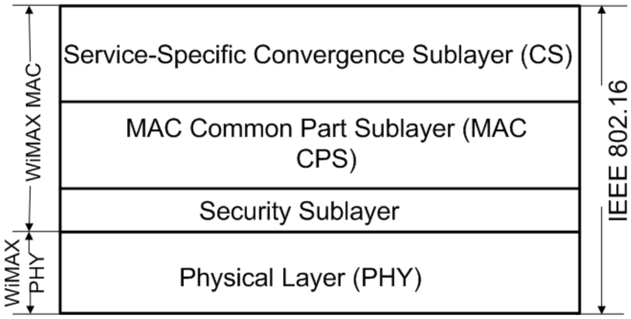

Service-Specific Convergence Sublayer (CS)
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
Physical Layer (PHY)
WiMAX MAC
WiMAX PHY
IEEE 802.16

Figure 2.8 IEEE 802.16 reference model

The WiMAX MAC frame structure consists of generic MAC header (GMH), payload and cyclic redundancy check (CRC) as shown in Figure 2.9. The fixed-length GMH contains the MAC management information. The length of the payload is variable, allowing the MAC to tunnel various higher-layer traffic types. The maximum length is 2046 bytes, which is indicated by the 11-bit length field in GMH. The CRC is used for error detection. More details regarding the frame structure and function are presented in the 802.16 standard [31].

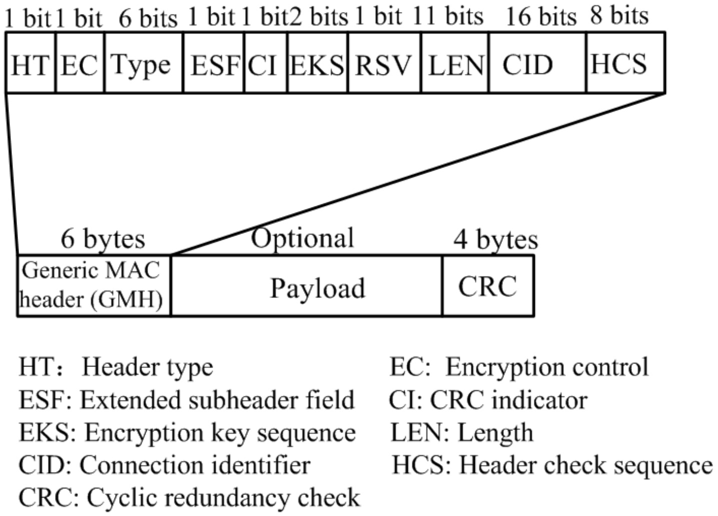
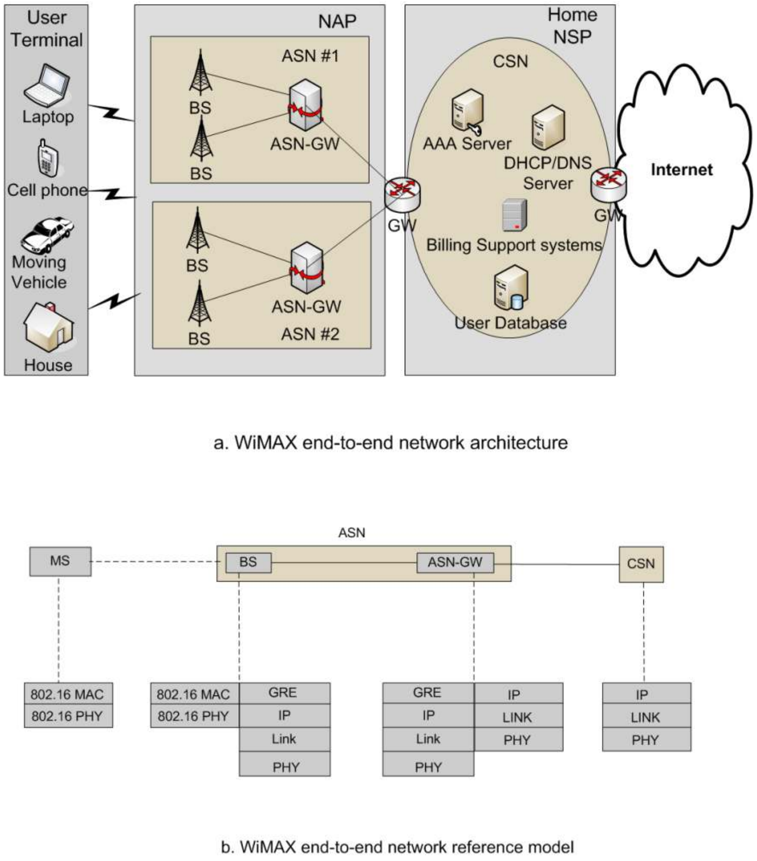


Figure 2.9 WiMAX MAC PDU structure

2.3.2 WiMAX Network Architecture

IEEE 802.16 standard focuses mainly on the specifications of the MAC and physical layers. To ensure the inter-vendor inter-networking interoperability for roaming, multi-vendor access networks and inter-company billing [51], the WiMAX Forum [52] formed the Networking Working Group (NWG) to create the end-to-end higher layer networking specifications for fixed, nomadic, portable and mobile WiMAX systems beyond what is defined in the scope of IEEE 802.16.

The IP-based, end-to-end WiMAX network architecture, described by the NWG network, and the corresponding layered model, defined by the WiMAX Forum network architecture specification [53], are shown in Figure 2.10. The network architecture consists of user terminal, access service network (ASN) owned by the network access provider (NAP), and connectivity service network (CSN) owned by the network service provider (NSP) [51]. The user terminal could be fixed WiMAX terminals like houses installed with the WiMAX antennas, portable WiMAX terminals such as laptops and cell phones embedded with WiMAX chipsets, or mobile WiMAX terminals such as moving vehicles equipped with WiMAX customer-premises equipment (CPE) devices.



a. WiMAX end-to-end network architecture

b. WiMAX end-to-end network reference model

Figure 2.10 WiMAX end-to-end network architecture and layered model

The ASN provides radio access connection to the WiMAX subscribers and relays functionality for establishing Layer-3 connectivity with a WiMAX MS. An

ASN comprises a BS and ASN gateway (ASN-GW). The BS implements WiMAX PHY and MAC functions defined in the IEEE 802.16 standard [17, 18]. The ASN-GW provides control and management functions for the BS and interfaces to the CSN. The ASN-GW also plays the role of the authenticator during the EAP authorization process [54]. Between the BS and ASN-GW, a generic routing encapsulation (GRE) [55] (IP-in-IP) tunnel is established to transport the upper layer traffic. The CSN is defined as a set of network functions that provide IP connectivity services to the WiMAX subscribers.

The CSN includes functions such as authentication, authorization, and accounting (AAA) services, QoS management, DHCP/DNS services, and WiMAX subscriber billing [56]. In roaming conditions, the subscriber might connect to the home NSP via visited NSPs with whom the home NSP has roaming agreements.

2.3.3 Mobile WiMAX Handover

The handover (HO) process in Mobile WiMAX networks is an essential element in supporting mobility and user roaming. The HO happens when the MS changes from one BS to another to obtain a higher signal QoS [31]. IEEE 802.16e – 2005 defines three modes of handover: a standard hard handover and two types of soft handovers: macro diversity handover (MDHO) and fast BS switching (FBSS). The hard handover is mandatory while MDHO and FBSS are optional. This dissertation only considers the standard hard handover process, which is the basis for the proposed handover schemes. Descriptions of MDHO and FBSS are detailed in [18, 31].

The standard handover procedure consists of the following nine stages [31] as shown in Figure 2.11:

A. Network topology advertisement

In this stage, the serving BS broadcasts the network topology information to the MS using the MOB_NBR-ADV (neighbor advertisement) message at a periodic interval. Channel information of neighboring BSs that are normally carried by each BS's own DCD (downlink channel descriptor) and UCD (uplink channel descriptor) are provided in MOB_NBR-ADV.

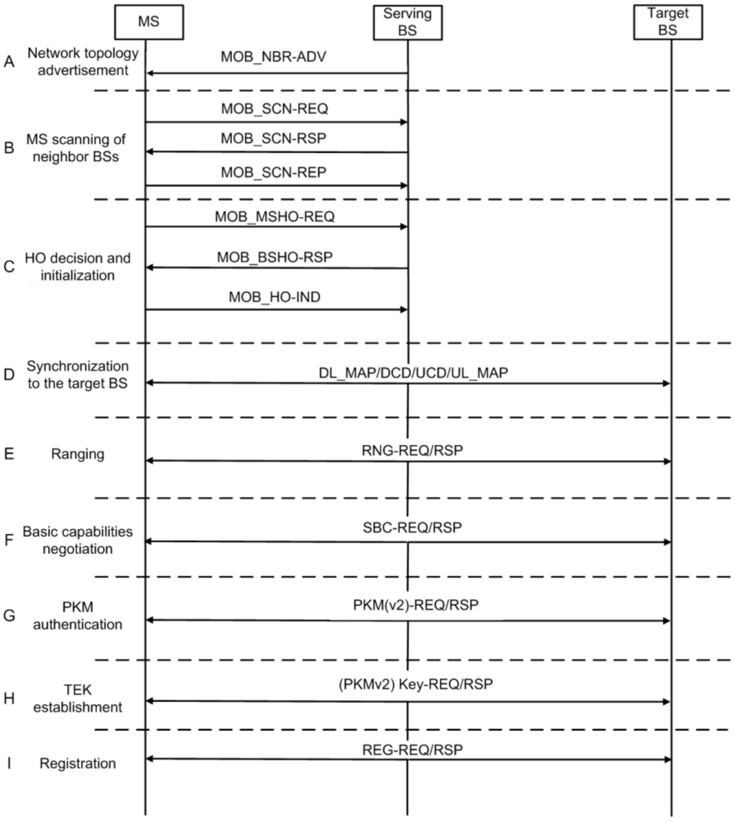


Figure 2.11 Standard WiMAX handover procedure

B. MS scanning of neighbor BSs

The MS sends a MOB_SCN-REQ (scanning interval allocation request) message to request scanning intervals, thus seeking available BSs and determining the target BS. The serving BS replies with a MOB_SCN-RSP (scanning interval allocation response) message to allocate the scanning intervals for the MS. The MS then scans all recommended BSs and reports the scanning result in the MOB_SCN-REP (scanning result report) message, which is sent to the serving BS.

C. HO decision and initialization

The HO decision can originate either at the MS by sending a MOB_MSHO-REQ (MS HO request) message or at the serving BS through a MOB_BSHO-REQ (BS HO request) message. In the handover process shown in Figure 2.11, I assume the HO is trigged by the MS. Within the MOB_MSHO-REQ message, the MS indicates one or more possible target BSs based on the evaluation from previous scanning results. Then the serving BS returns a MOB_BSHO-RSP (BS HO response) message as an acknowledgement. Finally, the MS sends a MOB_HO-IND (HO indication) message to indicate the release of the serving BS and that it is about to perform a handover.

D. Synchronization to the target BS

In this phrase, the MS synchronizes itself to the downlink (DL) transmission of the target BS and obtains the DL and uplink (UL) transmission parameters. The MS could already have received the target BSID, physical frequency, DCD and UCD from the MOB_NBR-ADV, which would shorten this process.

E. Ranging

The MS sends a RNG-REQ (ranging request) message to the target BS to acquire the correct timing offset and power adjustments. The MS's MAC address is also included in RNG-REQ to identify itself. A RNG-RSP (ranging response) message is transmitted by the BS in response to a received RNG-REQ. There is a HO Process Optimization type/length/value (TLV) field included in RNG-RSP, which is used to identify the network reentry steps that could be skipped during the current HO process because the target BS may obtain the MS information from the serving BS over the backbone network. This type of handover is named optimized HO. The possible omitted handover steps include basic capabilities negotiation, PKM authentication, traffic encryption key (TEK) establishment and registration.

F. Basic capabilities negotiation

After the completion of ranging, the MS and the BS use the SBC-REQ (SS basic capability request) and SBC-RSP (SS basic capability response) messages to associate their basic capabilities such as supported physical parameters and properties of the MS which are related to bandwidth allocation.

G. PKM authentication

This stage uses PKM-REQ (PKM request) and PKM-RSP (PKM response) messages to realize the MS's re-authentication to the WiMAX network. If PKM version 2 (PKMv2) defined in IEEE 802.16e – 2005 is enabled, then PKMv2-REQ and PKMv2-RSP messages are used. Depending on different modes, RSA-based authentication, or EAP-based authentication, or both need to be implemented in this step.

H. TEK establishment

During this phase, the MS sends a Key-REQ (key request) message to the BS to request new TEK and TEK-related parameters. TEK is created by the BS and sent using the Key-RSP (key response) message encrypted by the MS's public key. In PKMv2 mode, PKMv2 Key-REQ and PKMv2 Key-RSP messages are used.

I. Registration

Finally, the MS registers itself to the network using a REG-REQ (registration request) message. A REG-RSP (registration response) message is sent back by the BS in response to the received REG-REQ.

After registration, a few more steps, including establishment of IP connectivity and time of day, and operational parameters transfer [31] need to be implemented for the MS to establish connection to the mobile network. This dissertation considers registration as the last step of the handover.

2.4 Summary

This chapter has presented the evolution of passive optical networks. It has described the EPON reference model, MAC layer frame structure, auto discovery process, and operation principles. It has also introduced the characteristics of FSO technology, and the common topologies of FSO networks. Further it has presented an overview of WiMAX, including the reference model, network architecture and handover process.

Chapter 3 Current Security Schemes for Emerging Broadband Access Technologies

Abstract: This chapter introduces the contemporary security mechanisms used in EPON, FSO and WiMAX. It first presents the security characteristic in EPON networks and reviews the current security schemes adopted for EPON. Then the chapter gives a discussion on FSO security. Finally the chapter presents the privacy key management (PKM) protocols and security frameworks for WiMAX.

3.1 EPON Security

3.1.1 EPON Security Characteristics

As discussed in Chapter 2, EPON broadcasts downstream and unicasts upstream and LLID is used to identify the specific ONU. Due to its unique operation principles, EPON is vulnerable to the following security attacks.

- Eavesdropping

In downstream direction, since the data is broadcast to each ONU, a malicious ONU could disable the LLID filter function and implement eavesdropping on frames transmitted to other ONUs. In upstream direction, because upstream traffic is multiplexed and only OLT could see all the data, the transmission is relatively secure.

- Impersonation

During the auto discovery process, the OLT discovers ONUs and assigns them

LLIDs. If the intruder obtains the MAC address of a legal ONU, he could masquerade as that ONU and send the wrong registration information to the OLT, and then he can get a LLID without the OLT being aware.

- Denial of Service

In upstream direction, since each ONU shares the network resource and capacity and the OLT allocates the bandwidth to ONUs dynamically, a malicious ONU could generate a large amount of data traffic intentionally and thus deprive bandwidth from other ONUs.

Therefore, authentication of the ONU and user is needed to identify subscribers and prevent impersonation. Data encryption is needed to prevent eavesdropping. If encryption is applied at the MAC layer, only the payload will be encrypted and both DA and SA will be exposed to all users in the downstream direction, which leave the chance for impersonation. So encryption should be implemented at the reconciliation sublayer, which is below the MAC layer and only the preamble including LLID is left unencrypted.

3.1.2 EPON Security Mechanisms

In EPON's IEEE 802.3ah standard, no security protocol is defined. Vendors will describe and implement their own security mechanisms. Various security protocols, including IEEE 802.1x [57], Public Key Infrastructure (PKI) [58], symmetric cryptography and Diffie-Hellman key exchange method [32], have been proposed to realize authentication and key exchange in EPON networks.

For example in [59], the author adopts IEEE 802.1x and uses a Remote Authentication Dial In User Service (RADIUS) [60] server to authenticate the ONU. Another scheme [61] utilizes public key certificates to realize mutual authentication. Also, PKI is used in [61] and [62] to distribute secret encryption keys. Both [59] and [62] incorporate PKI keys into the MPCP messages. But the payload of the MPCP message is only 40 bytes, which is not enough to accommodate the PKI key, which is up to 1 Kb. Therefore, this method is not compatible with the IEEE 802.3ah standard.

Symmetric cryptography is adopted in [63]. A keyword pre-distributed to the OLT and ONU combining exchanged nonce are used to authenticate each other and generate the secret key. However, in this mechanism, the key derivation scheme is rather complex, and a nonce is sent in clear text potentially causing eavesdropping. The Diffie-Hellman key exchange method is proposed in [64] to derive the shared encryption key. But this scheme suffers from man-in-the-middle attack [32].

Among the above security proposals, the OLT is responsible for encryption key generation in [62], which makes the management of all the secret keys convenient. If the ONU generates the encryption key as presented in [61], it will be relatively more secure because the unicast upstream channel is used. In [63] and [64], both the OLT and the ONU contribute to the derivation of the session key to prevent the key’s transmission in the channel. However, the exchange of random numbers is left in the clear, which suffers from eavesdropping.

3.2 FSO Security

A FSO communication system is one of the most secure networking transmission technologies. RF-based wireless communication systems are more vulnerable to security attacks than wired networks, because RF generally spreads in all directions. The FSO systems operate in the IR wavelength spectrum, which is also the range used by fiber optical transmission systems. Therefore, although transmitted in the air, FSO belongs to optical communication and does not have the same security concern faced by wireless communications.

The FSO transmission has the following advantages, which make the tapping and eavesdropping of a FSO link very difficult. First, because the FSO signal is transmitted in a very narrow beam and because the FSO transceivers are located at an elevation above the ground level, the interception of the FSO link becomes rather difficult. Second, FSO nodes are usually installed on rooftops or behind office windows of tall buildings, both of which are restricted areas and could not be easily accessed by an intruder. Therefore, the interception of the optical beam at the customer premise where the system is installed would be very difficult [65]. Third, the FSO link requires LOS and works in a very narrow beam. Even if the FSO beam is intercepted, the connection will be interrupted, causing a decrease in the power of the received signal or no signal, which could be easily detected by the FSO management system. Therefore, FSO is considered more secure than both wireless and wireline transmissions.

However, there is one security weakness in FSO links caused by the divergence of the optical beam. Although the FSO link is a very narrow beam, after the beam travels several kilometers, the circular cross section could be a few meters in diameter. This is much larger than the aperture of the FSO receiver, which is several centimeters [16]. So there could be an overspill of the beam making it susceptible to eavesdropping at some point past the FSO node. Thus, to protect the FSO link, encryption of sensitive data at the higher layer is needed.

3.3 WiMAX Security

3.3.1 WiMAX Security Overview

In WiMAX networks, a PKM [17] protocol is defined to provide privacy, authentication and confidentiality across the WiMAX broadband wireless link between the MS and BS. The protocol stack for the security components of the PKM system are shown in Figure 3.1.

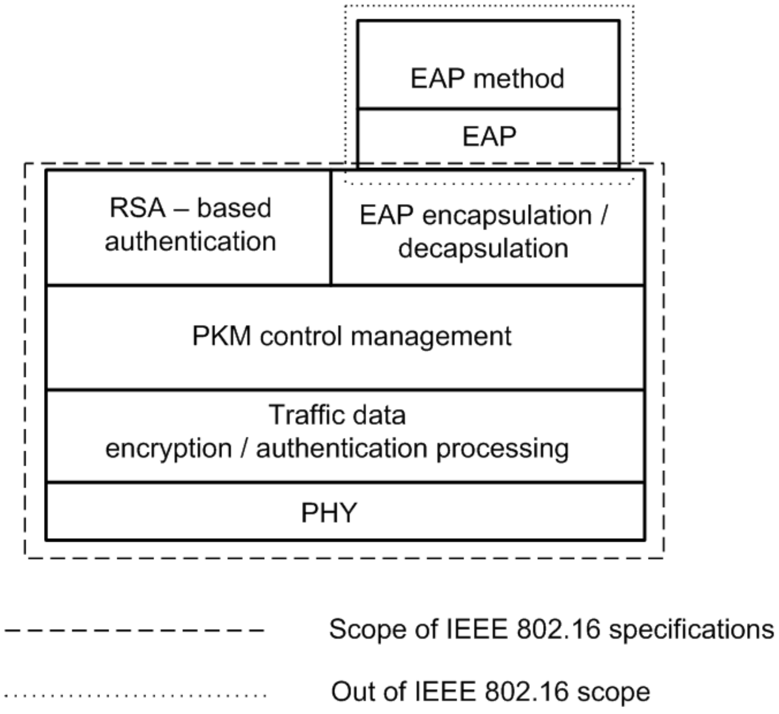

EAP method
EAP
RSA – based authentication
EAP encapsulation / decapsulation
PKM control management
Traffic data encryption / authentication processing
PHY
Scope of IEEE 802.16 specifications
Out of IEEE 802.16 scope

Figure 3.1 Security sublayer defined in IEEE 802.16 (adopted from [31])

The first version of PKM (PKMv1) was released in IEEE 802.16-2004, and X.509 digital certificate [32] and RSA [32] public-key encryption algorithm are used to realize authentication and key distribution. PKM is implemented at the security sublayer, which is at the bottom of the MAC layer and above the PHY layer [17].

The second version PKMv2 was released in IEEE 802.16e-2005 [18]. Apart from the RSA protocol, IEEE 802.16e also defines an EAP-based authentication [18]. EAP is implemented above the 802.16 layer, and the EAP information is carried by the PKMv2 management messages between the MS and BS.

3.3.2 Privacy Key Management (PKM)

3.3.2.1 PKM version 1

The PKM protocol uses X.509 certificates and RSA public-key scheme to establish a shared AK between the SS and BS. The AK is then used to secure subsequent exchanges of TEKs [17], which are used to encrypt user data.

Three messages are used to finish the authorization process as shown in Figure 3.2. The SS first sends an Authentication Information message containing the SS manufacturer’s X.509 certificate for the BS to verify the identity of the SS’s manufacturer. After that, the SS sends an Authorization Request message that includes the SS’s X.509 certificate, basic CID [31], and cryptographic capabilities indicated by a list of cryptographic suite identifiers. Upon receipt of the SS’s messages, the BS validates the SS’s identity, determines the cryptographic suit it shares with the SS, and generates an AK for the SS encrypted by the SS’s public key PUSS.

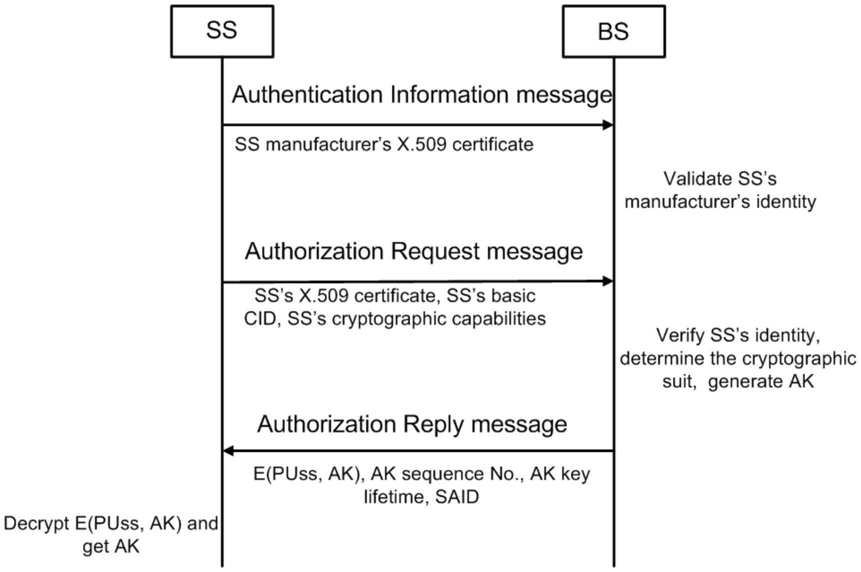

SS
BS
Authentication Information message
SS manufacturer's X.509 certificate
Validate SS's manufacturer's identity
Authorization Request message
SS's X.509 certificate, SS's basic CID, SS's cryptographic capabilities
Verify SS's identity, determine the cryptographic suit, generate AK
Authorization Reply message
E(PUss, AK), AK sequence No., AK key lifetime, SAID
Decrypt E(PUss, AK) and get AK

Figure 3.2 PKMv1 authorization

The third message, named Authorization Reply message, is then sent by the BS to the SS containing encrypted AK, 4-bit AK sequence number, AK key lifetime and security association identifier (SAID). The SS decrypts the message using its private key PRSS to obtain the AK. After the PKM authorization process completes, a traffic encryption key (TEK) [56] is generated by the BS which is used to encrypt the data traffic between the BS and SS. A key encryption key (KEK) [56] derived by the shared AK is used to encrypt the TEK. The BS then sends the TEK encrypted by the KEK to the SS. The SS decrypts the message to obtain the TEK.

3.3.2.2 PKM version 2

PKMv2 was released to enhance the security of PKMv1. PKMv2 introduces mutual authentication between the MS and BS to prevent forgery attacks and impersonation. The BS's X.509 certificate is incorporated in the Authorization Reply message for the SS to authenticate the identity of the BS. Further, 64-bit random numbers generated respectively by the BS and SS are exchanged during the authorization process to ensure key freshness. A pre-primary authorization key (pre-PAK) is generated by the BS and distributed to the SS. The AK is derived from the PAK, which is generated by the pre-PAK. PKMv2 3-way security association (SA)-TEK handshake is used after the authentication process to verify the security association between the MS and BS based on the AK.

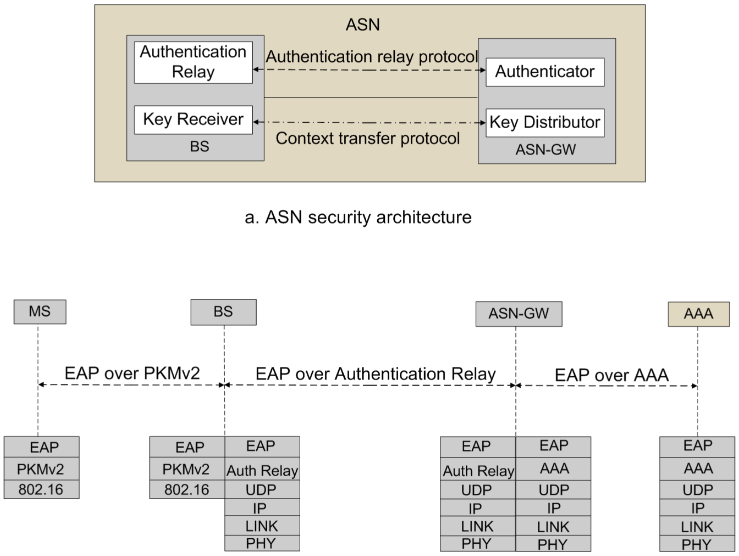
As described in the 802.16e standard, the PKMv2 system could use either RSA-based authentication, EAP-based authentication, or a sequence starting with RSA authentication and followed by EAP authentication.

3.3.3 WiMAX Security Framework Utilizing EAP

Although implementation is optional as defined in the 802.16e standard, the EAP authentication mechanism is very necessary for global roaming across WiMAX operator networks in which credential reuse, consistent use of AAA for accounting and billing are supported [51]. The RSA-based authentication is suitable for a fixed WiMAX network in which the MS is communicating with the same BS. But during the handover process in the mobile WiMAX network, in which the MS needs to change to different BSs from time to time, RSA-based authentication will bring much complexity to the security management system. On the other hand, EAP-based authentication, which happens between the MS and a backend server located at the CSN instead of the BS during the handover, brings much convenience and flexibility to the whole system. Therefore, compared to RSA-based authentication, EAP provides a viable and efficient authentication framework to support mobility and user roaming for mobile WiMAX networks. In the network architecture specified by the WiMAX Forum, EAP is used for authentication and authorization [53].

The implementation of EAP authentication requires an authentication server (AS) that stores user credentials, and an authenticator that acts as a pass-through device to pass the authentication messages from the subscriber to the AS. In mobile WiMAX networks, the backend AAA server in the CSN performs the AS function, and the ASN-GW implements the functions of the authenticator. The ASN security architecture [53] is shown in Figure 3.3a. The BS implements the authentication relay and key receiver functions while the ASN-GW contains the authenticator and key distributor functional entities. Authentication relay is a functional entity that relays EAP packets via an authentication relay protocol between the BS and ASN-GW. A key distributor is used to distribute the master session key (MSK) derived from the EAP process to the key receiver via a context transfer protocol [53]. Key receiver is the key holder for the AK and is responsible of generating other related 802.16e specified keys.

EAP has its own in-order delivery and retransmission mechanisms [66], and it could run directly on the link layer without relying on a network layer protocol such as IP. As shown in Figure 3.3b, between the MS and BS, EAP messages are encapsulated in the PKMv2 management messages and transported by the 802.16 protocol. Between the BS and ASN-GW, the EAP messages are relayed by the authentication relay protocol over the UDP/IP infrastructure [53]. Between the ASN-GW and the AAA server, EAP packets are forwarded over UDP/IP network by AAA protocols such as remote authentication dial in user service (RADIUS) [60].



a. ASN security architecture

b. Reference protocol stack during EAP process in WiMAX network

Figure 3.3 ASN security architecture and EAP authentication protocol stack

3.3.3.1 Layer-3 WiMAX Security Framework Based on Both RSA and EAP

In this framework, RSA authentication is implemented first and then followed by EAP authentication. The WiMAX PKMv2 procedure based on both RSA and EAP is shown in Figure 3.4.

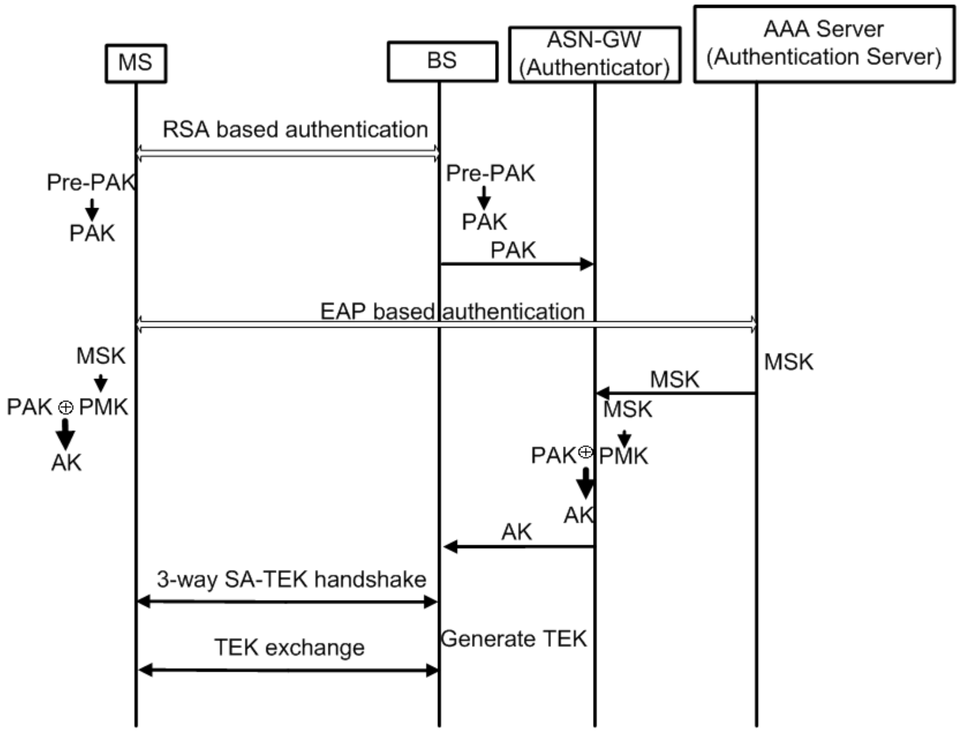


Figure 3.4 RSA and EAP based security framework for WiMAX networks

First, the RSA-based authentication process is implemented, deriving the pre-PAK to generate the PAK shared between the MS and BS. The PAK is then transferred from the BS to the ASN-GW for future use. Second, the EAP-based authentication takes place, generating a MSK in both the MS and AAA server. The MSK is then sent from the AAA server to the ASN-GW where a pairwise master key (PMK) is derived from the MSK. So far, both the MS and ASN-GW hold the PAK and PMK, which are subsequently used to derive the AK. Next, the ASN-GW transfers the AK to the BS. In the third step, the PKMv2 3-way SA-TEK handshake is performed between the MS and BS to verify the security association based on the AK. Finally, TEK exchange is implemented to transmit the generated TEK from the BS to the MS, completing the framework.

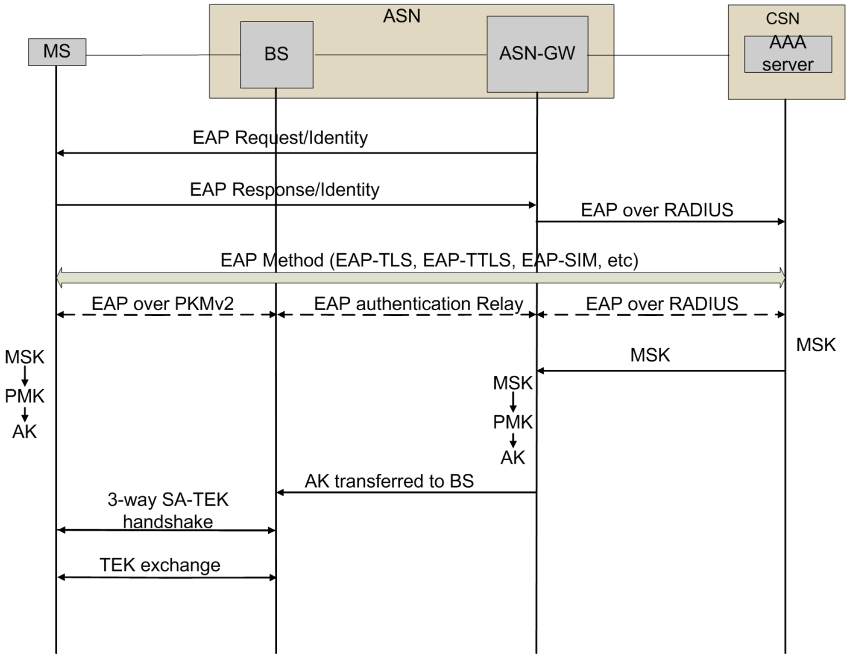


Figure 3.5 EAP-based security framework for mobile WiMAX networks

3.3.3.2 Layer-3 WiMAX Security Framework Based on EAP

The EAP-based WiMAX PKMv2 procedure is shown in Figure 3.5. First, the authenticator (ASN-GW) sends an EAP Request/Identity to the MS to trigger the EAP process. The MS responds with an EAP Response/Identity message that is passed to the AAA server. Then the EAP authentication is implemented between the MS and the AAA server. The particular credentials and EAP methods to be used are not specified in both 802.16e standard and WiMAX Forum released specifications. Various EAP methods such as EAP-Transport Layer Security

(EAP-TLS) [67], EAP for GSM Subscriber Identity (EAP-SIM) [68], and EAP for UMTS Authentication and Key Agreement (EAP-AKA) [69] are available choices. The EAP process derives a shared MSK between the MS and AAA server. The MSK is then transferred to the ASN-GW to generate a PMK used to derive the AK. Next, the ASN-GW forwards the AK to the BS over the context transfer protocol. The MS also derives the AK from the MSK. After that, 3-way SA-TEK handshake and TEK exchange are performed. At this point, the PKMv2 process completes.

3.4 Summary

This chapter has presented the security characteristics and mechanisms of EPON. It has also discussed the security aspects for FSO technology. Finally, the chapter has presented the security mechanisms used in WiMAX networks, including PKM protocols and EAP-based security frameworks.

Chapter 4 WiMAX over EPON Access Networks

Abstract: This chapter proposes a new WiMAX over EPON architecture which integrates WiMAX and EPON networks functionally. The chapter first gives an overview of integrated WiMAX and EPON networks and reviews current integration solutions. Then it proposes the WiMAX over EPON network including the reference model and layer-2 and 3 architectures. Finally, the chapter presents that this new integration solution could simplify the management system, saves costs, reduces latency and improves efficiency.

4.1 Integrated WiMAX and EPON Network Overview

The general architecture of the integrated access network is shown in Figure 4.1. The EPON network provides backhaul for WiMAX networks. A WiMAX BS is integrated with an ONU, called ONU-BS [70]. When the downstream data traffic from an OLT arrives at the ONU-BS, it is transformed into a WiMAX signal and transmitted to the SSs. In the upstream direction, the wireless signal from the SSs is transformed to an optical signal at the ONU-BS and is then transmitted to the OLT. Compared to pure EPON, this integrated access network provides mobility, is less costly, and reaches areas where fiber is hard to deploy. Compared to pure WiMAX network, subscribers even far away from the central office can access broadband bandwidth. The integration of EPON and WiMAX extends the coverage of the access network.

Such integrated architecture brings a higher possibility of interference between sectors served by different ONU-BSs especially in urban areas using the license-exempt spectrum. Various carriers need to collaborate to coordinate frequency usage and transmit times. Proper spectrum allocation by the service provider is required to reduce the interference among adjacent serving areas. In addition, advanced antenna technologies, dynamic frequency selection (DFS) [71], and robust network design and infrastructure placement are also helpful to minimize the interference [72].

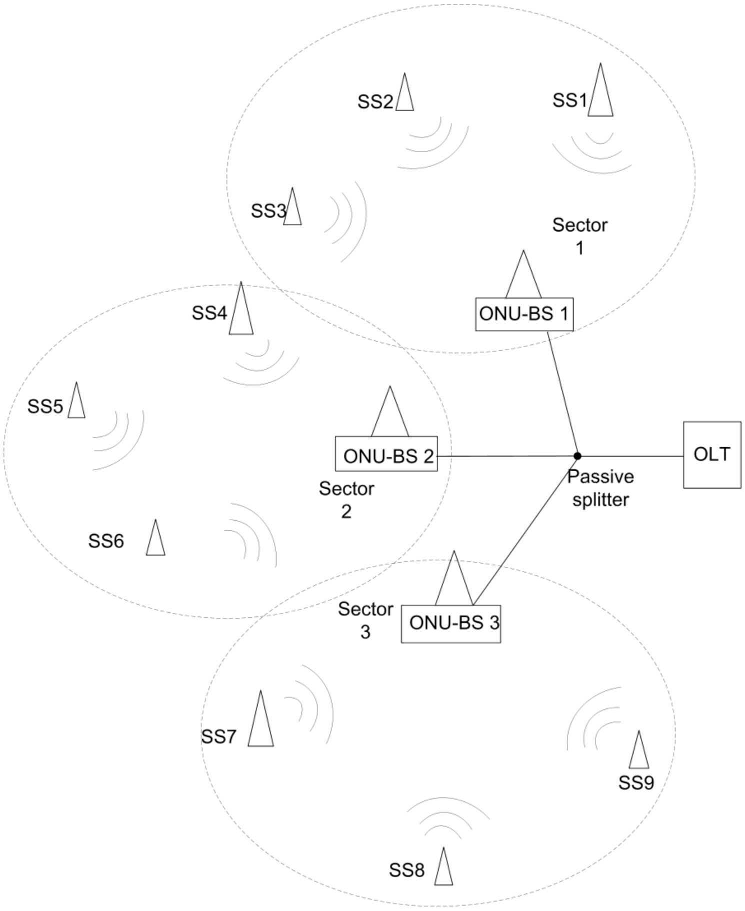


Figure 4.1 General integrated EPON and WiMAX access network architecture

Regarding the integration of ONU and BS, different architectures have been proposed [70, 73, 74]. This chapter presents a new integrated architecture named WiMAX over EPON that can achieve better efficiency and management than previously proposed architectures. In this model, each WiMAX MAC PDU is encapsulated directly into one EPON Ethernet frame and all the WiMAX MAC management functions are moved from the ONU-BS to the OLT.

4.2 Current Integrated EPON and WiMAX Architectures

Several authors have discussed integrated EPON and WiMAX architectures in contemporary literatures [70, 73, 74]. Authors of [70] discuss four types of integrated EPON and WiMAX architectures: Independent Architecture, Hybrid Architecture, Unified Connection-Oriented Architecture, and Microwave-over-fiber architecture.

Independent Architecture simply connects the ONU and BS through a common standardized interface like Ethernet, and EPON and WiMAX networks operate independently of each other. In this case, the architecture is easy to implement, but no functional integration is achieved. Also it would be costly to use two independent devices: EPON ONU and WiMAX BS.

A Hybrid Architecture integrates the ONU and BS in a single system box called ONU-BS. In this architecture, the ONU and BS are integrated in hardware and software. In hardware, there are three CPUs that can be further integrated into one CPU for better integration. CPU-1 runs EPON MAC protocol and communicates with the EPON network while CPU-3 implements WiMAX MAC protocol and communicates with the WiMAX network. CPU-2 is responsible for coordinating the behavior of the other two CPUs. In the upstream direction, the WiMAX data frame arriving at the ONU-BS is decrypted and de-encapsulated in CPU-3. Since EPON and WiMAX have different MAC management systems, the WiMAX MAC frame's control information is processed in CPU-2 to achieve the optimal bandwidth allocation and scheduling results. CPU-1 then constructs the EPON Ethernet frame according to CPU-2's processing, encrypts it and sends it to EPON network. In the downstream direction, the Ethernet frame is de-encapsulated in CPU-1 and the control information contained in the header is sent to CPU-2. According to the processing in CPU-2, CPU-3 constructs the WiMAX frame and sends it to WiMAX subscribers. This architecture integrates the ONU and BS to a single system which reduces the cost of equipment. It implements a control system which is expected to realize improved QoS and scheduling scheme. However, because three CPUs or one CPU that combines the functions of three CPUs are used, much processing time is needed in the ONU-BS. Also double encryption and decryption add delay and complexity to the system.

As shown in Figure 4.2, the Unified Connection-Oriented Architecture has almost the same layout as that of the Hybrid Architecture, except that instead of carrying the Ethernet frame, a WiMAX MAC PDU encapsulating multiple Ethernet frames is transmitted in the EPON network. A new convergence sublayer responsible for controlling and allocating the bandwidth in EPON is added below the Ethernet MAC layer. At the ONU-BS, the upstream WiMAX MAC PDUs from the SS are reconstructed into the Ethernet frames, and several of these Ethernet frames are then encapsulated into a new WiMAX MAC PDU. The EPON LLID is kept in front of the new WiMAX MAC PDU for addressing purposes. This architecture uses WiMAX's connection-oriented control protocol in EPON to achieve unified network control and management. However, like the Hybrid Architecture, this architecture suffers from the delay caused by the double encryption. Between the OLT and ONU-BS, to encrypt both the new WiMAX MAC PDUs and the Ethernet frames, two sets of keying material are needed, which makes it more complicated to manage and distribute keys. Further, in addition to keeping the preamble containing the LLID in the front, each new WiMAX MAC PDU needs to use a certain number of fields to accommodate multiple Ethernet headers and trailers. This frame structure will lower the throughput of the system.

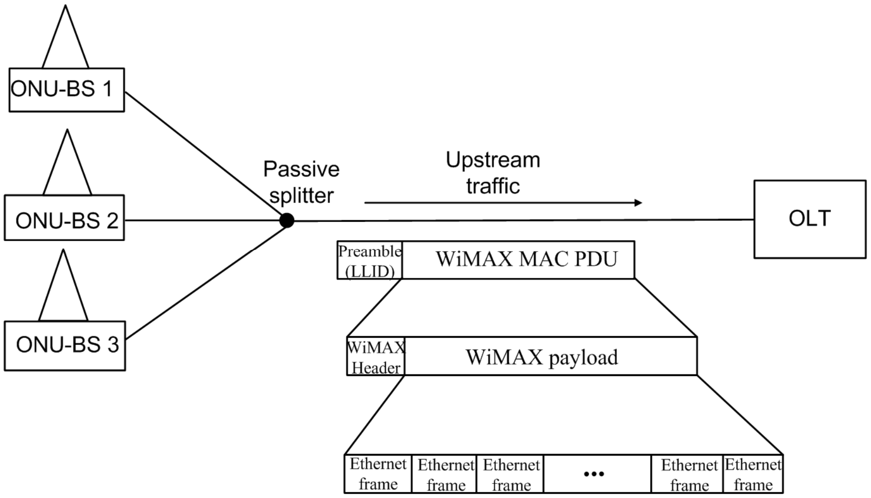


Figure 4.2 Unified Connection-Oriented Architecture (adopted from [70])

The fourth type is Microwave-over-fiber architecture in which the WiMAX signal modulates an optical carrier transmitted in optical fiber. Obviously, such an interconnection is open-ended, without any specific recognition of the characteristics of the PON environment.

Authors of [73] present the architecture of virtual ONU-BS (VOB) as shown in Figure 4.3. The ONU and BS are connected through a standard Ethernet interface, and a separate WiMAX-EPON bridge called WE-Bridge connects both the ONU and BS to coordinate joint resource allocation. The physical appearance of this architecture is similar to the Independent Architecture. The operation principle is much similar to the Hybrid Architecture except that the WE-Bridge implements the function of CPU-2. This architecture suffers from the same shortcomings as the Hybrid Architecture. Authors of [74] review current FiWi architectures and present integrated access networks with ring and star topologies. Because they are not consistent with current PON's tree topology, the dissertation will not discuss them here.

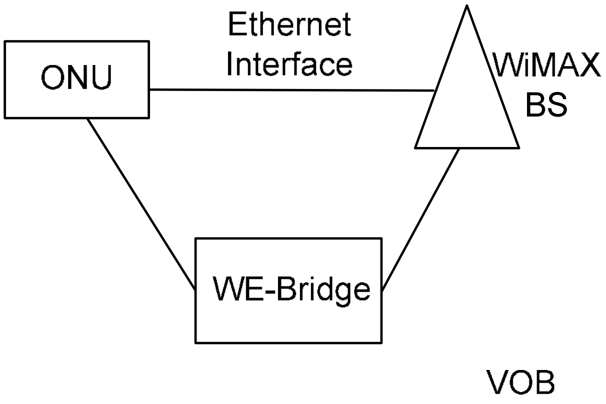


Figure 4.3 Virtual ONU-BS (VOB) (adopted from [73])

To sum up, both of the Hybrid and Unified Connection-Oriented Architectures implements double encryption, which adds processing delay in the ONU-BS. The Unified Connection-Oriented Architecture has a frame structure that lowers the system throughput and adds key management complexity. Plus, this architecture needs to modify the EPON standard. Therefore, an integrated architecture that can simplify the control and management inside the ONU-BS is needed to reduce the processing delay and utilize efficient security protocol to eliminate double encryption, without changing too much of both EPON and WiMAX standards.

4.3 Proposed WiMAX over EPON Network Architecture

The reference model for the proposed WiMAX over EPON architecture is shown in Figure 4.4. Part (a) is the reference model of WiMAX defined in IEEE 802.16 [17] and part (c) is the layered model of WiMAX over EPON. The physical layer of WiMAX is removed and the WiMAX MAC layer is placed on top of EPON (IEEE 802.3 ah) MAC layer [10], named WiMAX over EPON.

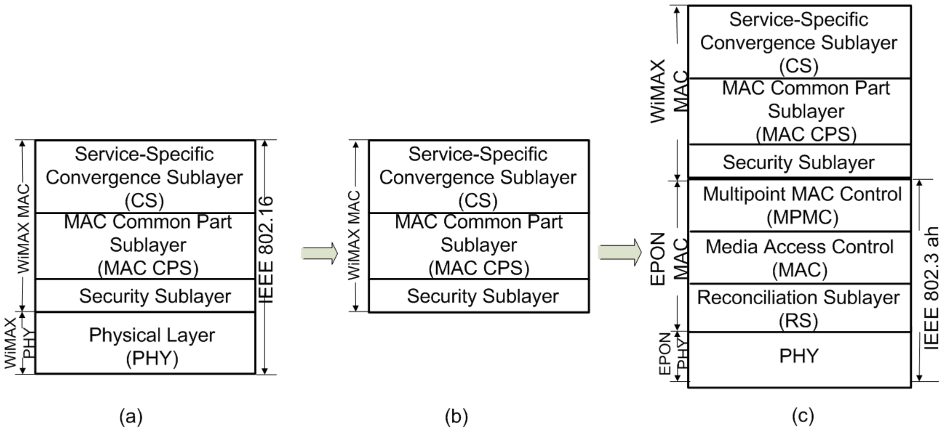

Service-Specific Convergence Sublayer (CS)
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
Physical Layer (PHY)
WiMAX MAC
WiMAX PHY
IEEE 802.16
(a)
Service-Specific Convergence Sublayer (CS)
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
WiMAX MAC
(b)
Service-Specific Convergence Sublayer (CS)
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
Multipoint MAC Control (MPMC)
Media Access Control (MAC)
Reconciliation Sublayer (RS)
PHY
WiMAX MAC
EPON MAC
EPON PHY
IEEE 802.3 ah
(c)

Figure 4.4. WiMAX over EPON reference model

The proposed architecture, like the Hybrid and Unified Connection-Oriented Architectures, integrates the ONU and BS into a single system called ONU-BS. In the upstream direction, when the WiMAX wireless signal from the SS arrives at the ONU-BS, the data frame is processed at the physical layer and turned into the WiMAX MAC PDU. The WiMAX MAC PDU is then placed on top of the EPON MAC layer. Instead of IP, voice, or any other types of data, the upper layer traffic for EPON now is the WiMAX MAC PDU. Each WiMAX MAC PDU is encapsulated into an EPON Ethernet frame which is then sent to the EPON network. Because the payload of the WiMAX MAC PDU is already encrypted at the SS, it does not need to be encrypted again by the encryption key in the EPON network except that the GMH needs to be encrypted. After the Ethernet frame reaches the OLT, it is processed by the EPON management and control system. The Ethernet header and trailer are stripped, turning the Ethernet frame back to the WiMAX MAC PDU. Then the WiMAX MAC PDU is sent to the WiMAX MAC management system for further processing. Similarly, in the downstream direction at the OLT, each WiMAX MAC PDU is encapsulated into an EPON Ethernet frame and sent to the ONU-BS. At the ONU-BS, the Ethernet frame is processed and turned into the WiMAX MAC PDU, which is then processed at the physical layer to generate the wireless signal. Finally the WiMAX wireless data is sent to the SS.

Figure 4.5 shows the encapsulation process in the frame structure. The whole WiMAX MAC PDU is encapsulated into an Ethernet frame, and the original

WiMAX MAC PDU is now the payload of the EPON MAC frame. Theoretically, the maximum frame length of the WiMAX MAC PDU payload, which is 2047 bytes indicated by 11 bits in the LEN field [56], is more than the maximum length of the Ethernet frame payload, which is 1500 bytes [44]. Because the length of the WiMAX MAC PDU, consisting of the MAC SDUs from the upper layer, is optional [56], the length of the WiMAX frame can be made to fit the length of the Ethernet frame, which is also variable.

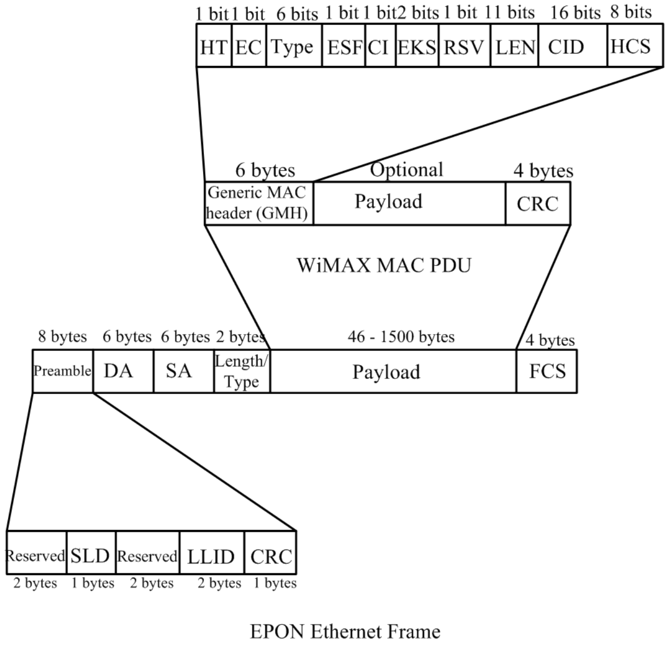


Figure 4.5 Encapsulate WiMAX MAC PDU into EPON Ethernet frame

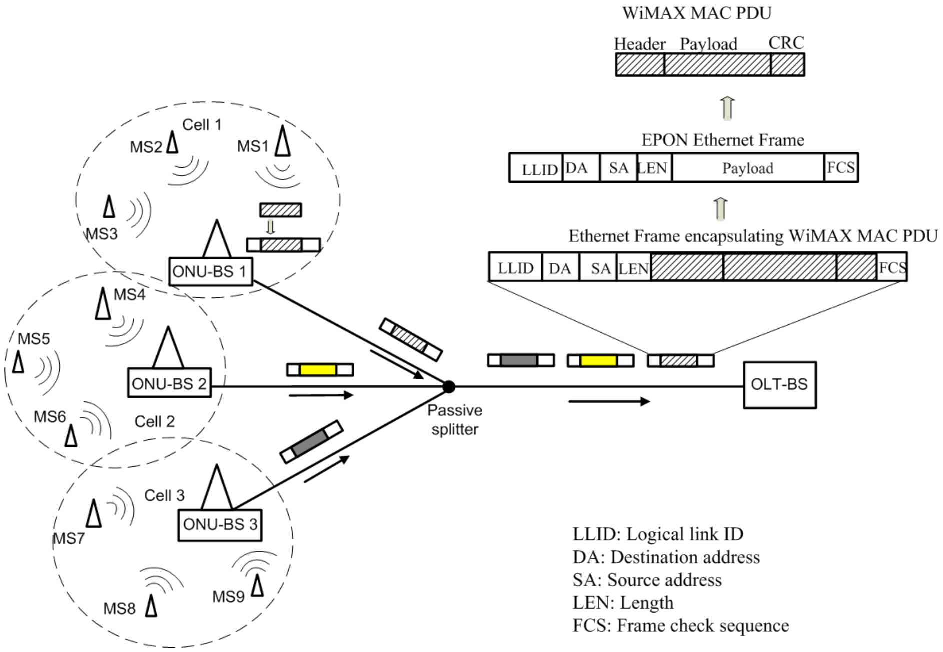
The EPON Ethernet frame now contains both the Ethernet header and the WiMAX GMH, which will increase the overall overhead thereby lowering the system throughput and efficiency. However, compared to the 1500-byte maximum

Ethernet payload length, the size of the WiMAX MAC header and trailer added to the original Ethernet frame is only 10 bytes, which is a very small percentage of the EPON Ethernet frame. Also the length of the WiMAX MAC PDU can be controlled to fully fit the length of Ethernet frame with as little padding as possible to improve the throughput of the system.

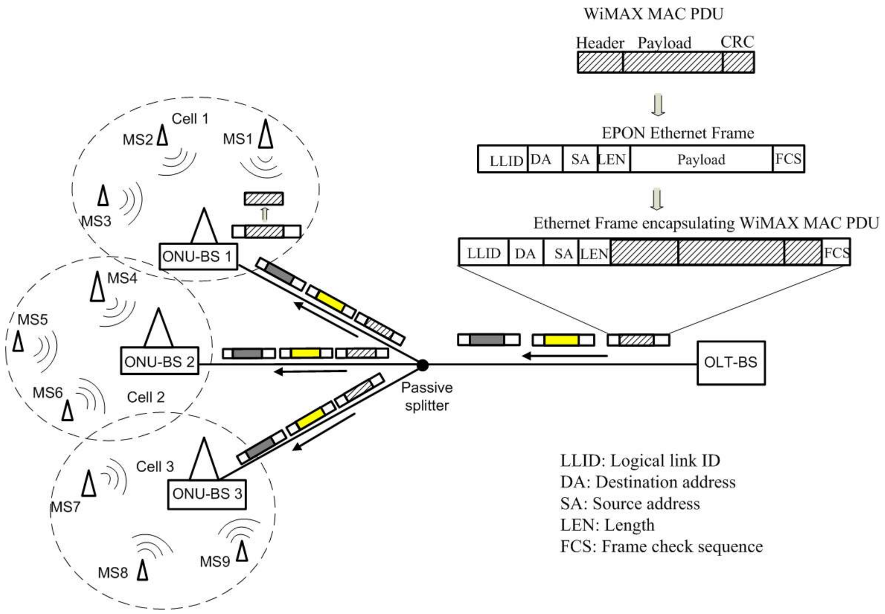
Except for the original ONU functions, in this architecture, the ONU-BS only performs the WiMAX physical layer function. All the WiMAX MAC functions performed by the service-specific convergence sublayer, the MAC common part sublayer, and the security sublayer are moved to the OLT. WiMAX MAC functions including bandwidth management, scheduling and encryption are completed in the SS for upstream traffic and in the OLT for downstream traffic. The MAC layer control messages, including bandwidth request messages and management messages, are exchanged between the OLT and the SS. For the WiMAX user, the ONU-BS is only a device that relays the WiMAX MAC PDU contained in the Ethernet frame to the OLT. Therefore, to better describe the system, from this point, OLT-BS is used to denote OLT for this WiMAX over EPON architecture.

4.3.1 Layer-2 WiMAX over EPON Network Architecture

The Layer-2 architecture of the WiMAX over EPON network is shown in Figure 4.6. The WiMAX MAC layer functions are moved from the BS to the OLT-BS while the ONU-BS does the WiMAX physical layer processing. In the downstream direction at the OLT-BS, each WiMAX MAC PDU is encapsulated into an Ethernet frame, which is sent to the EPON network. The LLID in the Ethernet frame preamble is used to identify the ONU-BS for which the WiMAX MAC PDU is intended. At the ONU-BS, the Ethernet header and trailer are stripped away, which turns the Ethernet frame back to the WiMAX MAC PDU. Then the WiMAX MAC frame is processed at the physical layer to generate the WiMAX wireless signal.



a. Upstream direction



b. Downstream direction

Figure 4.6 Layer-2 WiMAX over EPON network architecture

Similarly, in the upstream direction, the WiMAX MAC PDU from the MS is encapsulated into the Ethernet frame at the ONU-BS and recovered at the OLT-BS. Therefore, ONU-BS is used to relay the WiMAX MAC PDU within the EPON network while the OLT-BS is actually the management center for WiMAX subscribers.

4.3.2 Layer-3 WiMAX over EPON Network Architecture

The end-to-end Layer-3 WiMAX network architecture is shown in Figure 4.7. The ASN-GW is connected with certain number of OLT-BSs. Depending on the splitting ratio, each OLT-BS connects to 16, 32, or more ONU-BSs through a passive optical splitter. The user terminal connects to the OLT-BS via the ONU-

BS. Each OLT-BS has a BSID for operator identification just as the BS does in WiMAX network. The BSID is also used as one of the attributes to derive the PAK and AK shared between the MS and the OLT-BS during the RSA-based mutual authentication. Each ONU-BS has a BSID as well that is named sub-BSID. The sub-BSID is only used to identify different ONU-BSs during the handover process and does not contribute to key management and generation.

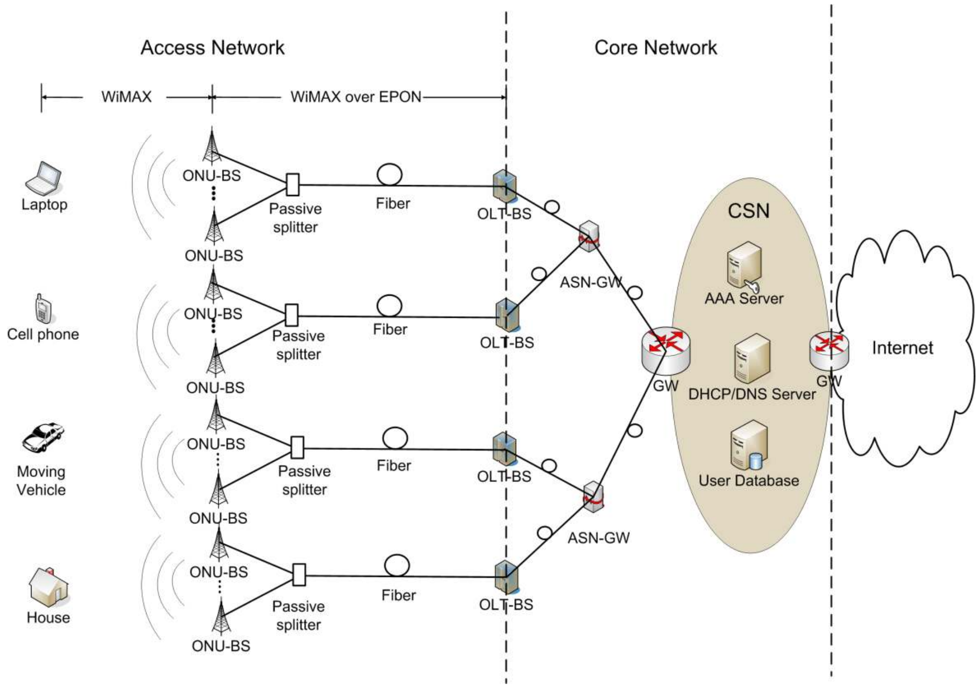


Figure 4.7 End-to-end Layer-3 WiMAX over EPON network architecture

The OLT-BS keeps the OLT functions and manages the WiMAX MAC layer of the original WiMAX BS. The ONU-BS maintains the ONU functions and performs the WiMAX physical layer processing. For example, in the downstream direction, higher layer data from the Internet is sent to the OLT-BS via the ASN-GW. At the OLT-BS, the upper layer data is mapped to the WiMAX MAC PDU, which is then encapsulated into the Ethernet frame sent down to the EPON network. At the ONU-BS, the payload part of the Ethernet frame is turned back to the WiMAX MAC PDU, which is transformed to the wireless signal. In the upstream direction, the WiMAX signal from the user is received by the ONU-BS, encapsulated into the EPON frame, and sent to the EPON network. At the OLT-BS, the WiMAX MAC PDU is recovered from the Ethernet frame and sent to the upper layer.

4.4 Benefits of WiMAX over EPON

The proposed architecture simplifies the management system, saves cost, causes fewer processing delays, and does not modify the original EPON and WiMAX standards:

A. Simplified management

First, for the WiMAX part, because the WiMAX MAC control functions are moved from the ONU-BS to the OLT-BS, the ONU-BS now needs only to implement physical layer processing. Second, for the EPON part, since the ONU-BS simply puts WiMAX MAC PDUs successively into Ethernet frames, no scheduling work needs to be performed. Third, double encryption is eliminated in the proposed architecture: In the upstream direction, the payload of the WiMAX MAC PDU is encrypted in the SS and decrypted in the OLT-BS. In the downstream direction, encryption is done in the OLT-BS and decryption in finished in the SS. Thus, control and management functions in the ONU-BS are largely reduced and simplified. Supposing that one OLT-BS serves 16 ONU-BSs. The WiMAX BS management systems in these 16 ONU-BSs are now integrated into one management system located at the OLT-BS. For a CO that accommodates more than one OLT-BS, it is possible that the WiMAX management systems from different OLT-BSs could be further integrated to a single system. Therefore, the WiMAX MAC control functions of a number of ONU-BSs in a large region served by one CO could be integrated into one control system, which can sufficiently simplify the overall management.

B. No modification to existing standard

As shown in the reference model in Figure 4.5, the only change is to put the WiMAX MAC layer on top of the EPON MAC layer. No modification is made to either the EPON or the WiMAX standards. From the OLT-BS to the ONU-BS, IEEE 802.3ah standard is implemented. EPON is responsible for transporting the WiMAX MAC PDU and can ignore the content of the WiMAX data. From the OLT-BS to the SS, the IEEE 802.16 standard is implemented except that the physical layer function is performed in the ONU-BS. The OLT-BS communicates directly with the SS while the ONU-BS only needs to relay the WiMAX traffic. Therefore, both EPON and WiMAX standards remain intact.

C. Cost saving

Because processing and management is simplified in the ONU-BS, the cost for designing and manufacturing the ONU-BS is reduced. For an integrated system with one OLT-BS and 16 ONU-BSs, rather than 16 WiMAX management systems for ONU-BSs, only one is needed for the OLT-BS, potentially saving substantial cost. Also because both EPON and WiMAX standards are not modified, there is no cost incurred when manufacturing products that adopt the new standards.

D. Less delay in ONU-BS

Compared to the Hybrid and Unified Connection-Oriented Architecture, less management and processing work needs to be done in the ONU-BS and double encryption is eliminated. The EPON scheduler inside the ONU-BS does not need to do any classification or scheduling work, thus minimizing processing time.

E. Integrated security management

In this proposal, instead of letting the ONU-BS manage and distribute keying materials, the OLT-BS is responsible for security management for SSs. SSs served by 16 different ONU-BS are now being managed by the same security center located at the OLT-BS, which increases key management integration and efficiency. More detailed discussion of security aspects are presented in the next chapter.

4.5 Summary

This chapter has proposed a WiMAX over EPON network architecture which places the WiMAX MAC layer on top of the EPON MAC layer so as to encapsulate each WiMAX MAC PDU into one EPON Ethernet frame. It has also presented the Layer-2 and 3 network architectures for the proposed WiMAX over EPON network. Compared to other current WiMAX and EPON integration solutions, the WiMAX over EPON network achieves integrated and simplified system management, improves the overall network efficiency, and reduces cost.

Chapter 5 A Unified Security Framework for WiMAX over EPON Access Networks

Abstract: This chapter first presents the Layer-2 security framework for the proposed WiMAX over EPON networks based on public key infrastructure (PKI) and X.509 certificates. Then it presents the Layer-3 security framework for WiMAX over EPON networks based on RSA and EAP. Finally, this chapter analyzes the proposed security frameworks. The analysis shows that the proposed security framework enhances overall system security and achieves efficient security management.

5.1 Layer-2 Security Framework for WiMAX over EPON Networks

In the Layer-2 security framework proposed in this section, the OLT-BS is responsible for key management and distribution. It plays the roles of both the OLT in EPON and the BS in WiMAX. PKI is used between the OLT-BS and ONU-BS, and PKM is adopted between the OLT-BS and SS. The proposed security framework is described in the following two parts.

5.1.1 Security Protocol between OLT-BS and ONU-BS

Figure 5.1 shows security protocol between OLT-BS and ONU-BS. Both symmetric and asymmetric cryptographies are used to provide two stages of authentication. A unique shared secret keyword (SK) is pre-distributed to each OLT-BS and ONU-BS pair. This keyword could be generated by the manufacturer and written into the device or calculated using a certain algorithm in the device module's chip. For a typical EPON network with 16 ONU-BSs, 16 SKs are pre-entered into the OLT-BS, and X.509 certificates are issued to the OLT-BS and ONU-BSs.

The following two steps are needed to complete this part.

5.1.1.1 Auto Discovery

This step uses five messages. First, the OLT-BS sends a broadcast GATE message to the network to advertise its discovery grant. In this message, the LLID is set to broadcast, and the SA is the OLT-BS's MAC address. Upon receipt of this discovery GATE, the uninitialized ONU-BS sends back a REGISTER_REQ message containing the ONU-BS's MAC address and a pending grant request. When the OLT-BS receives this message, it learns the ONU-BS's MAC address and selects the corresponding SK. The third message, which is a REGISTER message, is then sent by the OLT-BS to the ONU-BS, including the LLID assigned to the ONU-BS in the payload encrypted by the SK. In this message, the LLID field in the preamble is still set to broadcast. The DA shows the designated ONU-BS's MAC address while the SA is set to the OLT-BS's MAC address. DA and SA are sent in clear while only the payload is encrypted. Although this message is broadcast to all ONU-BSs, only the ONU-BS holding the correct SK can decrypt the message and get the assigned LLID, thus providing the first stage of authentication.

After that, the OLT-BS sends out another GATE message that contains the granted window slot in its payload encrypted by the SK. The LLID field in this message uses the ONU-BS's LLID, and both DA and SA fields are encrypted by the SK to prevent an attacker from relating the LLID to the corresponding ONU-BS's MAC address. At this point, the ONU-BS obtains its LLID as well as its transmission window. It then sends back a REGISTER_ACK to acknowledge the completion of auto discovery and ONU-BS registration.

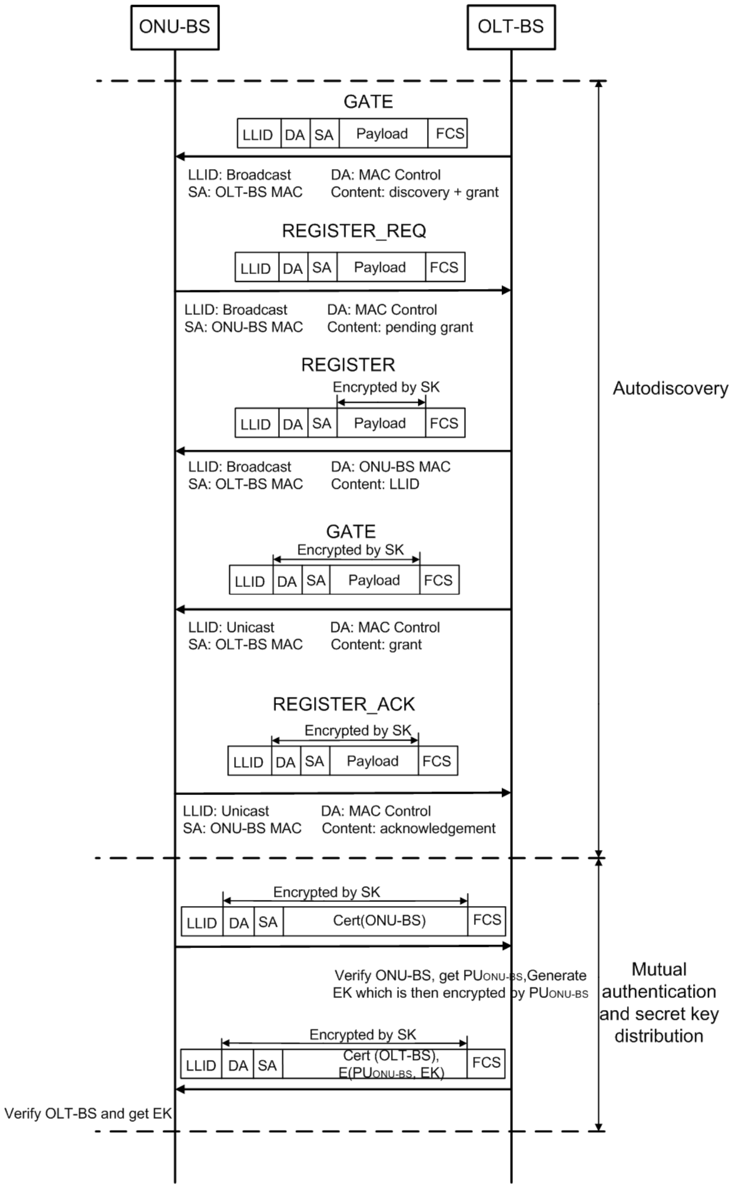


Figure 5.1 Proposed security protocol between OLT-BS and ONU-BS

5.1.1.2 Mutual Authentication and Secret Key Distribution

This step uses two messages to exchange the certificates of the OLT-BS and ONU-BS. The first message is sent by the ONU-BS which incorporates its X.509 certificate in its payload encrypted by the SK. DA and SA fields are also encrypted. Upon receipt, the OLT-BS decrypts the message, verifies the ONU-BS's identity, and obtains its public key PUONU-BS. An encryption key (EK) is then generated by the OLT-BS, encrypted using PUONU-BS and included in the second message, which also contains the OLT-BS's certificate. Similar to the first message, DA, SA, and payload fields of the second message are encrypted by the SK. When the ONU-BS receives this message, the EK is obtained and the OLT-BS's identity is verified. This step provides the second stage of authentication and distributes a new secret key EK to the OLT-BS and ONU-BS. After this step, all messages exchanged between the OLT-BS and ONU-BS will be encrypted using the EK. Upon receipt of every key update request, the OLT-BS will generate a new EK encrypted by PUONU-BS and send it to the corresponding ONU-BS.

As discussed before, the payload part of the MPCP message does not have enough space to accommodate the public key certificate. Because the auto discovery uses the MPCP messages, in the proposed protocol, certificate exchange is performed by two regular Ethernet data frames after the autodiscovery process. The payload of the Ethernet frame, which is up to 1500 bytes, is sufficient to incorporate the X.509 certificate.

5.1.2 Security Protocol between OLT-BS and SS

Figure 5.2 shows the security protocol between OLT-BS and SS. The PKM authorization protocol is adopted except that now it is implemented between the OLT-BS and SS. Before the PKM is invoked, the SS needs to synchronize itself to the network. After that, initial ranging and basic capabilities association are performed [56]. During this process, the ONU-BS encapsulates the WiMAX management messages in Ethernet frames and relays them to the OLT-BS. DA, SA, GMH, and payload fields are encrypted by the EK to prevent eavesdropping in the optical channel.

During the PKM authorization process, the Authorization Information message containing the SS's manufacturer's certificate is first sent by the SS to the ONU-BS. The ONU-BS encapsulates this message into an EPON Ethernet frame and sends it to the OLT-BS. The shared EK encrypts the GMH and payload fields of this WiMAX message as well as the DA and SA fields of the Ethernet frame. Then the SS sends an Authorization Request message to the ONU-BS, including the SS's certificate, cryptographic capabilities, basic CID, and a random number generated by the SS. Like the first message, it is relayed by the ONU-BS to the OLT-BS and encrypted by the EK. Upon acceptance, the OLT-BS obtains the SS's public key PUSS, validates the SS's identity, and actives a pre-PAK. After that, the OLT-BS sends out an Authorization Reply message containing the OLT-BS's certificate, pre-PAK encrypted by the PUSS, PAK sequence number, PAK lifetime, SAID, the SS's random number and a random number generated by the OLT-BS. When the SS receives this message, the OLT-BS's identity is verified and the pre-

PAK is obtained by the SS.

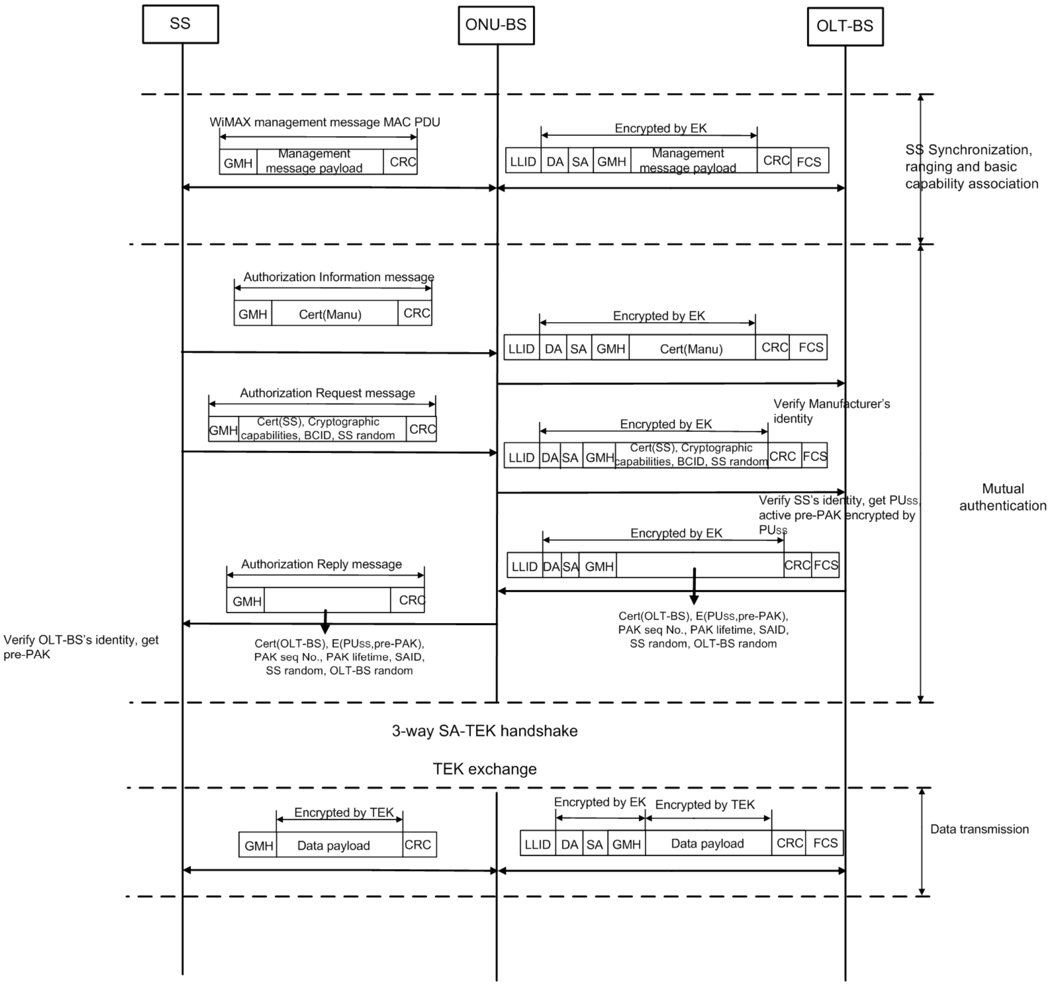

SS
ONU-BS
OLT-BS
WiMAX management message MAC PDU
GMH
Management message payload
CRC
Encrypted by EK
LLID
DA
SA
GMH
Management message payload
CRC
FCS
SS Synchronization, ranging and basic capability association
Authorization Information message
GMH
Cert(Manu)
CRC
Encrypted by EK
LLID
DA
SA
GMH
Cert(Manu)
CRC
FCS
Authorization Request message
GMH
Cert(SS), Cryptographic capabilities, BCID, SS random
CRC
Verify Manufacturer's identity
Encrypted by EK
LLID
DA
SA
GMH
Cert(SS), Cryptographic capabilities, BCID, SS random
CRC
FCS
Verify SS's identity, get PUss, active pre-PAK encrypted by PUss
Mutual authentication
Encrypted by EK
LLID
DA
SA
GMH
CRC
FCS
Authorization Reply message
GMH
CRC
Cert(OLT-BS), E(PUss,pre-PAK), PAK seq No., PAK lifetime, SAID, SS random, OLT-BS random
Verify OLT-BS's identity, get pre-PAK
Cert(OLT-BS), E(PUss,pre-PAK), PAK seq No., PAK lifetime, SAID, SS random, OLT-BS random
3-way SA-TEK handshake
TEK exchange
Encrypted by TEK
GMH
Data payload
CRC
Encrypted by EK
Encrypted by TEK
LLID
DA
SA
GMH
Data payload
CRC
FCS
Data transmission

Figure 5.2 Proposed security protocol between OLT-BS and SS

The subsequent 3-way SA-TEK handshake and TEK exchange process follow the similar rules as the previously described PKM authorization. When the corresponding WiMAX management messages come into the EPON network, their header and payload part as well as the Ethernet frame's DA and SA are encrypted by the EK.

At this point, the authentication and key distribution of the WiMAX over EPON network completes. During the data transmission phase, the payload of the WiMAX MAC PDU is encrypted by the TEK. Between the SS and ONU-BS, the GMH field is left in clear. Between the ONU-BS and OLT-BS, the WiMAX MAC frame is encapsulated into the Ethernet frame, and the EK will encrypt the DA, SA, and GMH fields while the payload part is kept unmodified as shown in Figure 5.2.

5.2 Layer-3 Security Framework for WiMAX over EPON Networks

As shown in Figure 5.4, the proposed layer-3 security framework for the WiMAX over EPON network is based on Layer-3 WiMAX security framework adopting both RSA and EAP. The ASN-GW is used as the authenticator, and the AAA server acts as the authentication server. The WiMAX over EPON architecture is applied between the ONU-BS and OLT-BS, and the ONU-BS relays the WiMAX MAC PDUs between the MS and the OLT-BS. It is assumed that the ONU-BS has already established connection with the OLT-BS and that the MS has completed synchronization, ranging, and basic capability association. The security framework is described as follows.

First, the RSA-based authentication process is implemented using PKMv2 RSA-Request and PKMv2 RSA-Reply message, resulting in the pre-PAK to generating the PAK shared between the MS and OLT-BS. The PAK is then transferred from the OLT-BS to the ASN-GW for future use. Second, the EAP-based authentication is initiated by the PKMv2 EAP-Start message. The PKMv2

EAP-Transfer message is then used to encapsulate the EAP payload between the MS and OLT-BS. An authentication relay protocol is utilized to relay the EAP messages from the OLT-BS to the ASN-GW, which then forwards the EAP credentials to the AAA server over the AAA protocol such as RADIUS or Diameter [75].

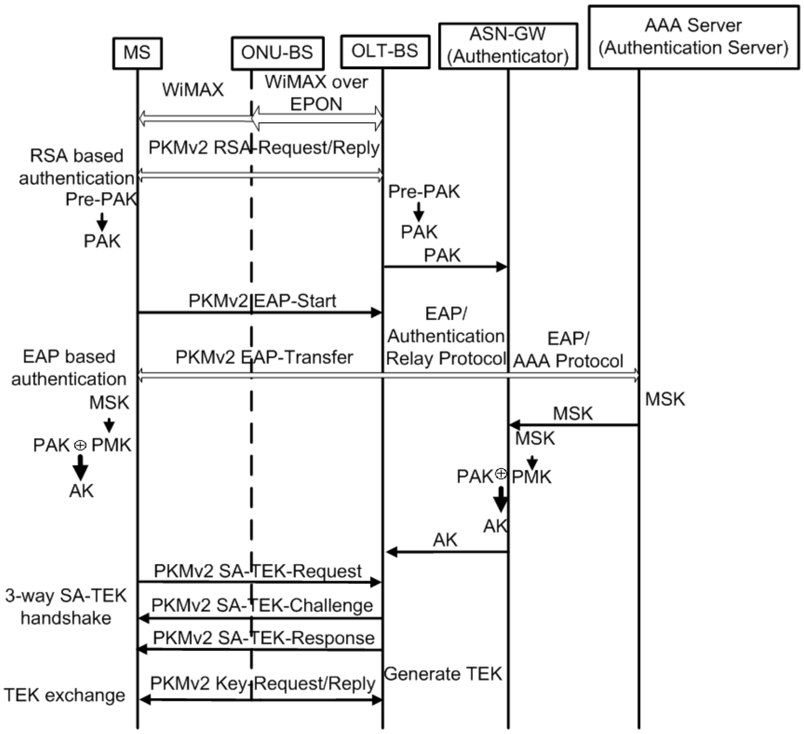


Figure 5.3 Layer-3 security framework for the WiMAX over EPON network

After the EAP authentication procedure, a MSK is generated in both the MS and AAA server. The MSK is then sent from the AAA server to the ASN-GW where the PMK is derived from the MSK. So far, both the MS and ASN-GW hold the PAK and PMK, which are subsequently used to derive the AK. Next, the ASN-

GW transfers the AK to the OLT-BS. In the third step, the PKMv2 3-way SA-TEK handshake is performed between the MS and OLT-BS to verify the security association based on the AK. Finally, TEK exchange is implemented to transmit the generated TEK from the OLT-BS to the MS. The framework is complete.

5.3 Security Analysis

In the proposed security framework for the WiMAX over EPON network, PKI is adopted in the EPON part and the PKM protocol is utilized for the WiMAX part. The OLT-BS combines the security functions of the OLT in EPON and the BS in WiMAX, so instead of issuing two certificates for the OLT and the BS, respectively, one certificate is issued for the OLT-BS to simplify the system. A two-stage authentication mechanism is provided in the first part of this security model using both symmetric and asymmetric cryptography. In the first stage, the ONU-BS needs to prove it shares the same SK as the OLT-BS to be able to decrypt the MPCP message sent by the OLT-BS. In the second stage, the ONU-BS's certificate needs to be verified by the OLT-BS whose identity also needs to be validated by the ONU-BS to realize mutual authentication. Even if a malicious ONU-BS cracks the autodiscovery process and obtains the SK to finish the first stage of authentication, it still needs to get a legal X.509 certificate to complete the whole authentication process, making it difficult to execute a masquerade attack.

In all current EPON security solutions mentioned in section 3.1.2, the MPCP messages are not encrypted. For data messages, only the payload is encrypted, and DA and SA fields are sent in clear. A malicious ONU could easily learn both the LLID and MAC address of a legal ONU to implement impersonation. In the proposed protocol, the following changes are made in the four different scenarios as shown in Figure 5.1. First, the Gate and REGISTER_REQ messages are kept unencrypted. Because the LLID fields are set to broadcast in both of these two messages, the attacker cannot relate the ONU-BS's MAC to its LLID. Second, the REGSTER message payload field containing the LLID is encrypted by the SK when it is sent to the ONU-BS. Although this message is sent in the downstream, which is the broadcast channel, and the DA field sent in clear indicating the MAC address of the designated ONU-BS and because the LLID in the preamble is set to broadcast, the attacker could not relate the MAC address to a legal LLID. Therefore, the DA field showing the ONU-BS's MAC address does not need to be encrypted. Third, for the GATE, REGISTER_ACK and two mutual authentication messages, the DA, SA, and payload fields are encrypted by the SK. In this case, only the LLID is exposed for addressing purpose, and the attacker has no way to relate the LLID to its corresponding ONU-BS's MAC address. In the last scenario, when the OLT-BS and ONU-BS complete mutual authentication and EK distribution, the EK is used to encrypt the DA, SA, and payload fields of all the subsequent exchanged Ethernet frames while the LLID is kept in clear for addressing purpose. Therefore, the LLID and its corresponding ONU-BS' MAC address never expose themselves at the same time to prevent masquerade attack.

In the EPON segment part of this framework, the OLT-BS is chosen to generate and distribute shared session key, rather than the ONU-BS or both, in order to realize efficient and simplified management. If the ONU-BS were responsible for generating the session key, more functions and calculations would be needed in the ONU-BS, which would raise the cost of manufacturing and management. Because each OLT-BS serves 16 ONU-BSs, for a CO that accommodates many OLT-BSs, this would cost much to add functions to a large number of ONU-BSs. Besides, in the second part of the framework, the OLT-BS is also in charge of managing and distributing TEKs for WiMAX end-users. So for the WiMAX over EPON architecture, the OLT-BS is the key management center for both EPON and WiMAX networks, makng the whole system easy and simple to manage and control. When the EK is distributed to the ONU-BS, it is first encrypted by the ONU-BS's public key, encapsulated into the Ethernet payload, and then encrypted by the SK; therefore it is secure enough to prevent the attacker from compromising the EK.

Double encryption is eliminated in this security model. In upstream traffic, for example as shown in Figure 5.2, WiMAX data transmitted in the wireless channel between the ONU-BS and SS is encrypted by the TEK. This part is the same as the original WiMAX network. When data enters the optical channel between the ONU-BS and OLT-BS, the GMH and payload of WiMAX MAC management messages that are sent in clear are encrypted by the EK while the CRC field is not encrypted just like the Ethernet FCS field. But for the WiMAX data MAC PDU, which is already encrypted by the TEK, the payload part is left unmodified and only the GMH part is encrypted. Thus, for the Ethernet frame transmitted between the OLT-BS and ONU-BS that encapsulates the WiMAX MAC PDU, all other fields are encrypted to prevent eavesdropping with the exception of LLID, CRC, and FCS. Instead of double encryption by both the EK and TEK, which would add complexity and delay to the system while providing no help to increase the security level, the WiMAX data MAC PDU only needs to go through the encryption process once: encrypted in the SS and decrypted in the OLT-BS.

5.4 Summary

This chapter has presented the Layer-2 and 3 security frameworks for the proposed WiMAX over EPON networks based on PKI and EAP. Our analysis has shown that the proposed security frameworks realizes mutual authentication, enhances overall system security, achieves efficient and simplified key management, and eliminates double encryption.

Chapter 6 Secure and Fast Handover Schemes for WiMAX over EPON Networks

Abstract: This chapter first introduces three types of handover scenarios in WiMAX over EPON networks: intra-OLT-BS handover, inter-OLT-BS handover, and inter-ASN handover. Then it proposes secure handover schemes using the pre-authentication method and the communication framework of the ranging step. Finally, this chapter analyzes the proposed handover schemes and shows that the handover mechanisms simplify the handover procedure and keep the handover process secure.

6.1 Handover Scenarios

The proposed handover scheme is based on the standard WiMAX hard handover procedure described in section 2.3.3. In this chapter, it is assumed the handover happens within the home NSP, referred to as the intra-CSN handover. Figure 6.1 shows the handover scenarios in the WiMAX over EPON network. The NAP has two ASNs managed by the home NSP: ASN #1 and ASN #2. The ASN-GW1 contained in the ASN #1 connects to the OLT-BS1 and OLT-BS2. The ASN #2 owns the ASN-GW2, which is connected to the OLT-BS3. For simplicity while not losing generosity, each OLT-BS connects to only two ONU-BSs instead of to 16 or 32. For example, the OLT-BS1 controls ONU-BS11 and ONU-BS12, the OLT-BS2 controls ONU-BS11 and ONU-BS12, and the OLT-BS3 controls ONU-BS31 and ONU-BS32. Cell 11 is the area covered by ONU-BS11, and cell 12 is controlled by ONU-BS12. Both cell 11 and 12 are covered by cell 1, which refers to the area managed by OLT-BS1. The name of cells covered by OLT-BS2 and OLT-BS3 follow the same rules as shown in Figure 6.1.

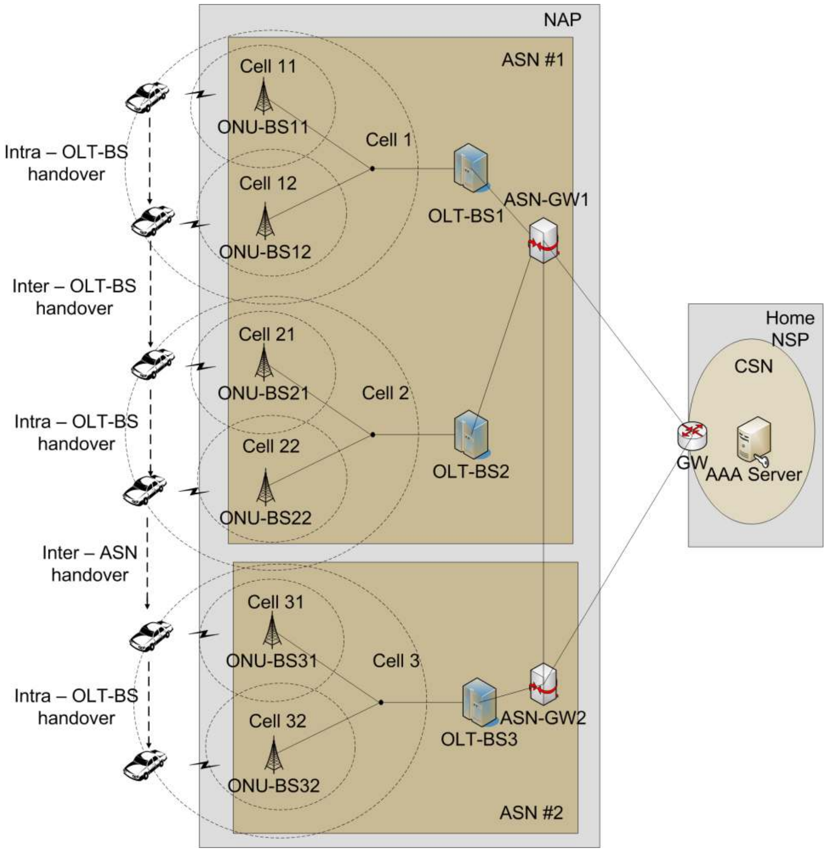


Figure 6.1 Handover scenarios in WiMAX over EPON network

Three types of handover scenarios are defined: intra-OLT-BS handover, inter-OLT-BS handover, and inter-ASN handover. Intra-OLT-BS handover happens within the area covered by a single OLT-BS when the MS moves from cell 11 to cell 12 (within cell 1). An inter-OLT-BS handover takes place when the serving ONU-BS and the target ONU-BS belong to different OLT-BSs while still inside the same ASN, for example, when the MS moves from cell 12 (cell 1) to cell 21 (cell 2). Inter-ASN handover refers to the handoff between different ASNs but managed by the same CSN, for instance, when the MS moves from cell 22 (cell 2) to cell 31 (cell 3).

Table 6.1 Terms used in the handover procedure

Terms	**Descriptions**
PU_{MS}	Public key of the MS
PR_{MS}	Private key of the MS
MS-Random	Random number generated by the MS
MS_{MAC}	MAC address of the MS
$PU_{OLT\text{-}BS}$	Public key of the OLT-BS
$PR_{OLT\text{-}BS}$	Private key of the OLT-BS
OLT-BS-Random	Random number generated by the OLT-BS
(pre-)PAK#	(Pre-) primary authorization key shared between the MS and OLT-BS#
AK#	authorization key shared between the MS and OLT-BS#

6.2 Handover Schemes

In the proposed handover schemes, the ranging management messages including RNG-REQ and RNG-RSP are used to carry authentication related information to realize mutual authentication between the MS and the mobile network. Pre-authentication is used in this scheme to pre-distribute the AK, thus accelerating the handover process in the inter-OLT-BS handover and inter-ASN handover.

Details of the three handover procedures are described in sections 5.1 - 5.3, and the terms used in the handover are shown in Table 6.1.

6.2.1 Intra-OLT-BS Handover

This section uses the scenario where ONU-BS11 is the serving ONU-BS and ONU-BS12 is the target ONU-BS. Because the MS is communicating with the same OLT-BS during the handover, the OLT-BS holds all the MS-related information, including the MSMAC and keying materials. The handover procedure is shown in Figure 6.2.

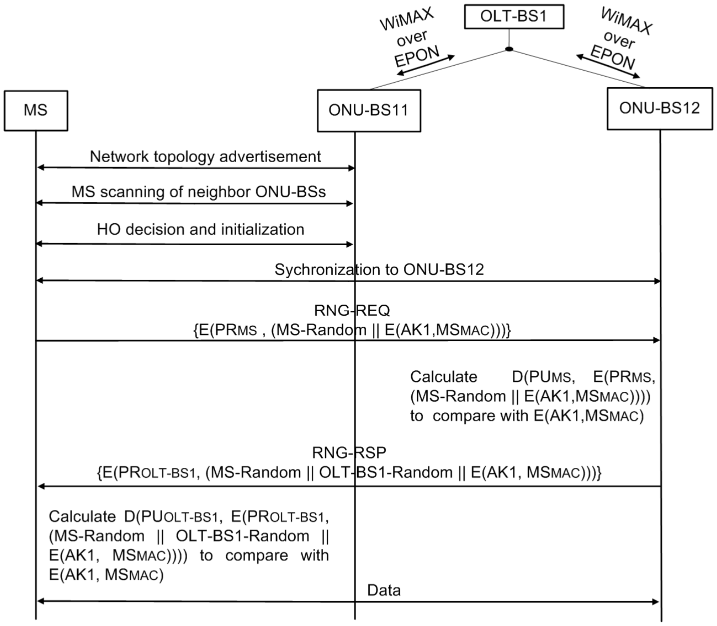

WiMAX over EPON
OLT-BS1
WiMAX over EPON
MS
ONU-BS11
ONU-BS12
Network topology advertisement
MS scanning of neighbor ONU-BSs
HO decision and initialization
Sychronization to ONU-BS12
RNG-REQ
{E(PRMS , (MS-Random || E(AK1,MSMAC)))}
Calculate D(PUMS, E(PRMS, (MS-Random || E(AK1,MSMAC)))) to compare with E(AK1,MSMAC)
RNG-RSP
{E(PROLT-BS1, (MS-Random || OLT-BS1-Random || E(AK1, MSMAC)))}
Calculate D(PUOLT-BS1, E(PROLT-BS1, (MS-Random || OLT-BS1-Random || E(AK1, MSMAC)))) to compare with E(AK1, MSMAC)
Data

Figure 6.2 Intra-OLT-BS handover in the WiMAX over EPON network

The first four steps are network topology advertisement, MS scanning of neighbor ONU-BSs, HO decision and initialization, and synchronization to the target ONU-BS. During this process, the MS compares the scanning results of the neighbor ONU-BSs, makes the HO decision, and synchronizes to the chosen ONU-BS which is ONU-BS22. Because the neighbor of ONU-BS11 is ONU-BS12, which is managed by the same OLT-BS, it is very convenient for OLT-BS1 to collect channel information from ONU-BS12 and send it to the MS through ONU-BS11. The sub-BSIDs are used to identify different ONU-BSs.

During the subsequent ranging process, the MS encrypts the MSMAC using AK1, referred to as E (AK1, MSMAC); and the MS-Random is concatenated with E (AK1, MSMAC) to ensure the freshness of the message. (MS-Random || E (AK1, MSMAC)) is then encrypted by PRMS to form E (PRMS, (MS-Random || E (AK1, MSMAC))) which is incorporated in the RNG-REQ message. The RNG-REQ message is sent to ONU-BS12, which relays the message to OLT-BS1. Upon the receipt of RNG-REQ, OLT-BS1 decrypts E (PRMS, (MS-Random || E (AK1, MSMAC))) using PUMS to get E (AK1, MSMAC) and compares it with its own calculation to verify the MS's identity. After that, OLT-BS1 concatenates ONU-BS-Random to (MS-Random || E (AK1, MSMAC)) and encrypts (OLT-BS1-Random || MS-Random || E (AK1, MSMAC)) by PROLT-BS to form E (PROLT-BS1, (OLT-BS1-Random || MS-Random || E (AK1, MSMAC))), which is contained in the RNG-RSP message. OLT-BS1 then sends the RNG-RSP message to the MS. The MS decrypts it with PUOLT-BS1 and compares the E (AK1, MSMAC) with the one it already has to verify the identity of OLT-BS1.

So far, since the MS and OLT-BS1 are authenticated by each other within the ranging process and the new ONU-BS connects the MS to the same OLT-BS, the following standard handover steps, including basic capabilities negotiation, PKM authentication, TEK establishment, and registration could all be skipped by indicating in the HO Process Optimization TLV field contained in the RNG-RSP message.

6.2.2 Inter-OLT-BS Handover

This section uses the scenario in which the MS moves from ONU-BS12 to ONU-BS21. Now the MS switches to a different OLT-BS while still within the area covered by the same ASN. Therefore, the PAK derived by RSA-based authentication needs to be updated while the PMK derived by the EAP-based authentication, which is cached in the same ASN-GW, is still valid. A pre-authentication method is used to derive the PAK2, thus generating the AK2. The procedure is described in Figure 6.3.

During the pre-authentication phase, OLT-BS2's certificate is sent to OLT-BS1 via ASN-GW1, and RSA-based pre-authentication is implemented to derive a shared pre-PAK2, which is sent to OLT-BS2 via ASN-GW1. The pre-PAK2 is used to generate the PAK2, which is then transferred back to ASN-GW1. Combing the PAK2 and PMK, an AK2 is derived and an AK2 is generated at the MS. The pre-authentication procedure is completes. During the handover phase, the first four steps are the same as the intra-OLT-BS handover. ONU-BS21's channel information controlled by OLT-BS2 is collected by OLT-BS1 via ASN-GW1 and then sent to the MS through ONU-BS12 for evaluation. In the HO decision and initialization step, MSMAC is transferred from the OLT-BS1 to OLT-BS2 via ASN-GW1, and the AK2 is sent from the ASN-GW1 to the OLT-BS2. After this point, both the MS and OLT-BS2 hold the MSMAC and AK2. The following ranging step is the same as the ranging process in the intra-OLT-BS handover except that AK2's and OLT-BS2's keying materials are used. This step realizes mutual authentication between the MS and OLT-BS2 and confirms the authentication of MS to the AAA server. After ranging, basic capabilities negotiations takes place to negotiate channel capabilities. Then the TEK establishment step is implemented to transmit the newly generated TEK from the OLT-BS2 to the MS.

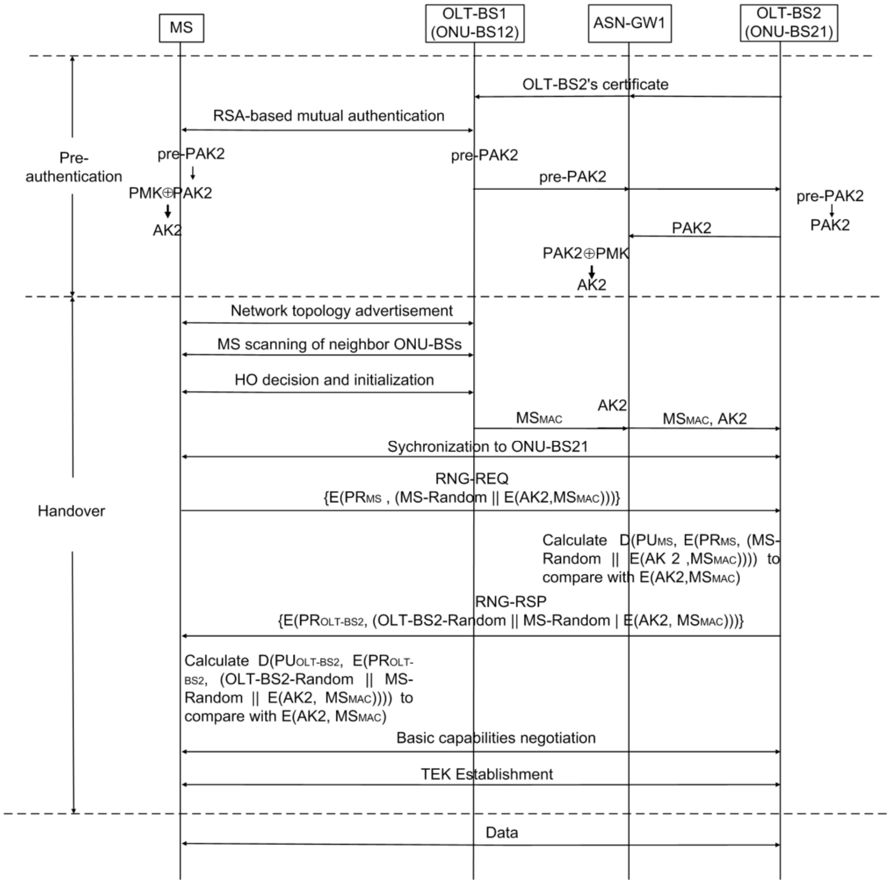

MS
OLT-BS1 (ONU-BS12)
ASN-GW1
OLT-BS2 (ONU-BS21)
Pre-authentication
OLT-BS2's certificate
RSA-based mutual authentication
pre-PAK2
PMK⊕PAK2
AK2
pre-PAK2
pre-PAK2
pre-PAK2
PAK2
PAK2
PAK2⊕PMK
AK2
Handover
Network topology advertisement
MS scanning of neighbor ONU-BSs
HO decision and initialization
AK2
MSMAC
MSMAC, AK2
Sychronization to ONU-BS21
RNG-REQ
{E(PRMS , (MS-Random || E(AK2,MSMAC)))}
Calculate D(PUMS, E(PRMS, (MS-Random || E(AK 2 ,MSMAC)))) to compare with E(AK2,MSMAC)
RNG-RSP
{E(PROLT-BS2, (OLT-BS2-Random || MS-Random | E(AK2, MSMAC)))}
Calculate D(PUOLT-BS2, E(PROLT-BS2, (OLT-BS2-Random || MS-Random || E(AK2, MSMAC)))) to compare with E(AK2, MSMAC)
Basic capabilities negotiation
TEK Establishment
Data

Figure 6.3 Inter-OLT-BS handover in the WiMAX over EPON network

6.2.3 Inter-ASN Handover

In this scenario, it is assumed the MS moves from ONU-BS22 to ONU-BS31. During this process, the MS changes both its attached OLT-BS and ASN-GW while still within the same CSN. Therefore, the PAK needs to be updated, and the PMK needs to be sent from ASN-GW1 to ASN-GW2 during pre-authentication. The handover procedure is shown in Figure 6.4.

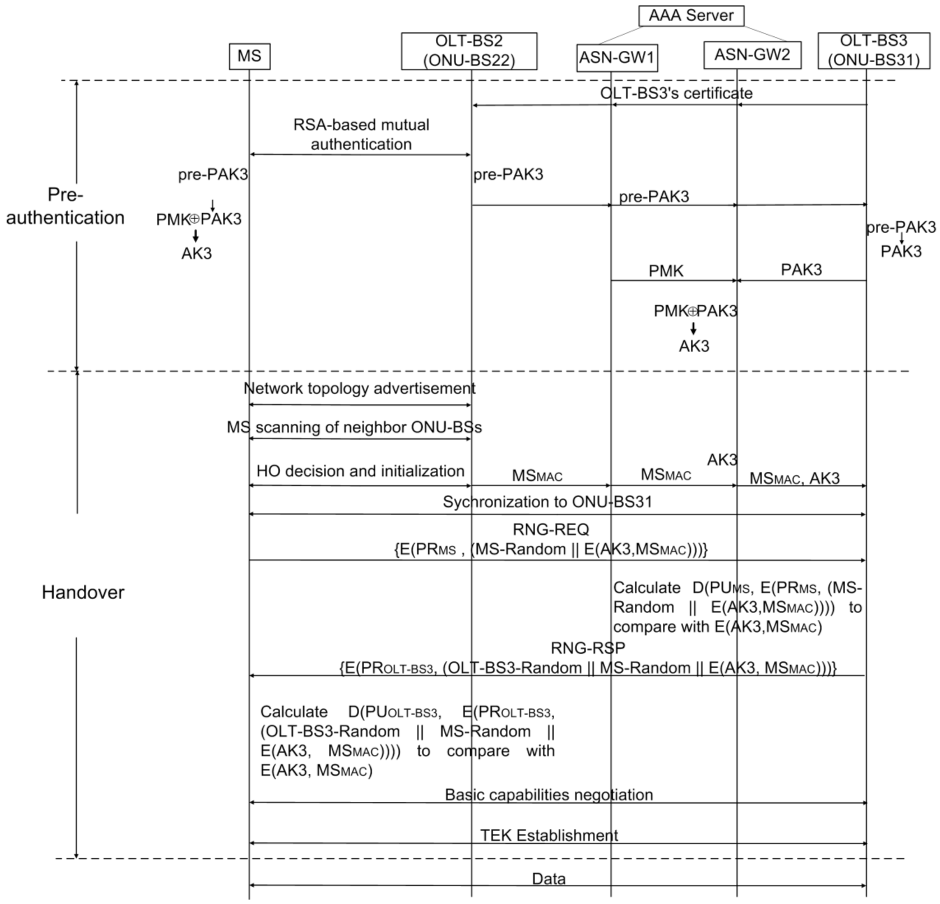

AAA Server
MS
OLT-BS2 (ONU-BS22)
ASN-GW1
ASN-GW2
OLT-BS3 (ONU-BS31)
OLT-BS3's certificate
RSA-based mutual authentication
Pre-authentication
pre-PAK3
PMK⊕PAK3
AK3
pre-PAK3
pre-PAK3
pre-PAK3
PAK3
PMK
PAK3
PMK⊕PAK3
AK3
Network topology advertisement
MS scanning of neighbor ONU-BSs
HO decision and initialization
MSMAC
MSMAC
AK3
MSMAC, AK3
Sychronization to ONU-BS31
RNG-REQ
{E(PRMS , (MS-Random || E(AK3,MSMAC)))}
Handover
Calculate D(PUMS, E(PRMS, (MS-Random || E(AK3,MSMAC)))) to compare with E(AK3,MSMAC)
RNG-RSP
{E(PROLT-BS3, (OLT-BS3-Random || MS-Random || E(AK3, MSMAC)))}
Calculate D(PUOLT-BS3, E(PROLT-BS3, (OLT-BS3-Random || MS-Random || E(AK3, MSMAC)))) to compare with E(AK3, MSMAC)
Basic capabilities negotiation
TEK Establishment
Data

Figure 6.4 Inter-ASN handover in the WiMAX over EPON network

During the pre-authentication process, OLT-BS3's certificate is transferred via the ASN-GW1 and ASW-GW2 to OLT-BS2 for RSA-based mutual authentication to derive a shared pre-PAK3 between the MS and OLT-BS2. The pre-PAK3 is then transmitted over the two ASN-GWs to OLT-BS3 where a PAK3 is derived. The PMK cached in the ASN-GW1 is sent to ASN-GW2, and is combined with the PAK3 transmitted from OLT-BS3 to derive an AK3. The AK3 is cached at the ASN-GW2 for future use. At the same time, the MS generates the AK3 because it holds both the PMK and PAK3.

The first four steps of the handover are the same as the intra-OLT-BS handover procedure. The channel information of ONU-BS31 is transferred from OLT-BS3 to OLT-BS2 via ASN-GW1 and ASN-GW2 for the MS to scan and evaluate. During the HO decision and initialization step, the MS_{MAC} is transferred from the OLT-BS2 to OLT-BS3 via the two ASN-GWs, and AK3 is transferred from the ASN-GW2 to OLT-BS3. The next ranging step is the same as the intra-OLT-BS handover ranging process except that AK3 and OLT-BS3's keying materials are used. Mutual authentication between the MS and OLT-BS3 is realized during this step, and the MS is verified that it has already been authenticated by the AAA server. After the ranging step, the basic capabilities negotiation takes place to negotiate channel capabilities. The TEK establishment step is needed to exchange the TEK generated by OLT-BS3.

6.3 Analysis of the Handover Schemes

6.3.1 Security Analysis of the Ranging Process

In this proposed three handover scenarios, the communication framework of the ranging step is used to realize both the RSA-based and EAP-based authentication. During the ranging process, as described in section 6.2, I incorporate E (PR_{MS}, (MS-Random || E (AK, MS_{MAC}))) in the RNG-REQ message sent from the MS to the OLT-BS. Since the OLT-BS holds the MS's public key, it can decrypt the message and obtain E (AK, MS_{MAC}). If the E (AK, MS_{MAC}) is the same as the OLT-BS's own calculation result, the MS's identity is verified because only the MS that holds the correct private key can encrypt (MS-Random || E (AK, MS_{MAC})). The match also proves that the MS holds the same AK as the OLT-BS because only the MS that has the correct AK is able to calculate the right E (AK, MS_{MAC}). In the RNG-RSP message replied by the OLT-BS, ($PR_{OLT\text{-}BS}$, (OLT-BS-Random || MS-Random || E (AK, MS_{MAC}))) is contained. The MS decrypts the message using the OLT-BS's public key and compares the obtained E (AK, MS_{MAC}) to the one it holds. The match verifies that the OLT-BS has the correct private key, thus confirming its identity. Therefore, the ranging step realizes mutual authentication between the MS and the mobile network which means the PKM authentication step could be skipped.

Although the security context in the RNG-REQ message is encrypted by the MS's private key, which means any malicious OLT-BS or MS that holds the MS's public key can decrypt the message, the MS's MAC address is encrypted by the AK, which is hard for an attacker to compromise. To implement the masquerade attack, the malicious entity needs to obtain the private key from either the legal OLT-BS or the MS to encrypt E (AK, MS_{MAC}), which makes the attack difficult.

For the same reason, the RNG-RSP message is also not easy to compromise. The random numbers generated by the MS and the OLT-BS are used as nonce to ensure the freshness of the message, thus preventing the reply attack.

Given that the AK is derived from the PAK and PMK while the PMK is generated through the EAP authentication process, it is verified that the MS holds the correct PMK. It also proves that before the handover process, the MS has already been authenticated by the AAA server via EAP protocol and registered to the CSN. Therefore, the registration step can also be skipped.

For the intra-OLT-BS handover, because the MS and the OLT-BS holds the same keying material and the original TEK is still valid, the basic capabilities negotiation and TEK establishment steps can also be skipped. For the inter-OLT-BS and inter-ASN handover, because the MS is switched to a different OLT-BS, the basic capabilities negotiation step is needed to negotiate channel capabilities. The TEK establishment step also needs to be implemented for the MS and the target OLT-BS to exchange the new TEK.

6.3.2 Security Analysis of the Pre-authentication

To shorten the handover procedure in inter-OLT-BS and inter-ASN handover, a pre-authentication method is utilized. During the inter-OLT-BS handover, the MS changes the attached OLT-BS while still managed by the same ASN. So the MS only shares the PMK with the target OLT-BS and the PMK is cached in the ASN-GW. During the pre-authentication process, the target OLT-BS's certificate is sent via the ASN-GW to the serving OLT-BS to implement RSA-based mutual authentication. The derived pre-PAK is transferred to the ASN-GW to generate the AK shared between the MS and the target OLT-BS. Thus, during the handover process, the MS and the target OLT-BS will hold the shared AK and each other's public/private key pair. In the HO decision and initialization, the MS's MAC address is sent from the serving OLT-BS to the target OLT-BS for authentication use.

The inter-ASN handover follows the same procedure as the inter-OLT-BS handover, except that in the pre-authentication process, the security context transfers between the serving OLT-BS and the target OLT-BS need to travel through two ASN-GWs instead of one. Also an extra step, the transfer of the PMK from the serving ASN-GW to the target ASN-GW, is needed. So a new AK is generated between the MS and the target OLT-BS through the pre-authentication process while the original PMK is still in use.

6.3.3 Comparison between the Proposed and Standard Handover Schemes

The comparison between the standard handover scheme defined in the IEEE 802.16e and the proposed three types of handover schemes is shown in Table 6.2. All the three proposed handover schemes *eliminate the PKM authentication step*, which contains the time-consuming RSA-based and EAP-based authentication, thus improving the efficiency of the handover. Compared to the standard nine-step WiMAX handover procedure, the intra-OLT-BS handover *consists of only five* *steps*, which greatly simplifies the handover process. The number of steps involved in both the inter-OLT-BS and inter-ASN handover is *reduced to seven*, which also shortens the handover process.

Table 6.2 Comparison between standard WiMAX handover and proposed handover schemes

Handover types		**Standard**	**Intra-OLT-BS**	**Inter-OLT-BS**	**Inter-ASN**
Pre-authentication		—	—	✓	✓
Handover procedures	Network topology advertisement	✓	✓	✓	✓
	MS scanning	✓	✓	✓	✓
	HO decision and initialization	✓	✓	✓	✓
	Synchronization	✓	✓	✓	✓
	Ranging	✓	✓	✓	✓
	Basic capabilities negotiation	✓	—	✓	✓
	PKM authentication	✓	—	—	—
	TEK establishment	✓	—	✓	✓
	Registration	✓	—	—	—

One disadvantage of the proposed handover schemes is that the use of pre-authentication brings extra cost and power consumption for the key transfer between different OLT-BSs and increases the amount of computations within the MS and the OLT-BS. However, because in practice, each OLT-BS can connect to 16–32 or even more ONU-BSs, the area covered by a single OLT-BS could be sufficiently large. As long as the topology of the WiMAX over EPON network is designed properly, the chance for the MS to apply the inter-OLT-BS and inter-ASN handover could be reduced while the intra-OLT-BS handover serves as the major handover scheme.

6.4 Summary

This chapter has presented handover scenarios in WiMAX over EPON networks, and proposed secure and efficient handover schemes using pre-authentication method and the communication framework of the ranging step. Our analysis has shown that the proposed handover schemes simplify and accelerate the handover process while maintaining the procedure secure.

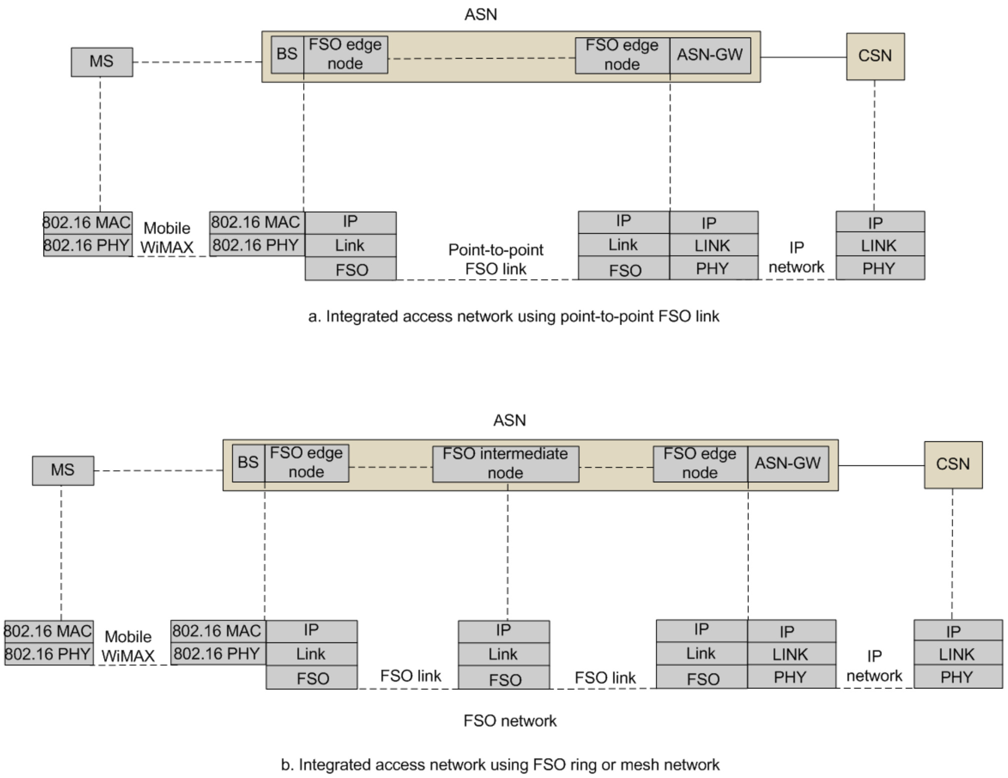
Chapter 7 A Unified Security Framework for Integrated Mobile WiMAX and FSO Broadband Access Networks

Abstract: This chapter first proposes a new network architecture which integrates Mobile WiMAX and FSO networks. Then it proposes a unified security framework for this integrated Mobile WiMAX and FSO broadband access networks utilizing EAP-TTLS and IPsec. Finally the analysis shows that EAP-TTLS provides a flexible and secure authentication scheme, and IPsec provides a efficient method to secure the data path in the FSO network.

7.1 Integrated Mobile WiMAX and FSO Access Network

7.1.1 Layered Model of the Integrated Mobile WiMAX and FSO Access Network

The reference model for the proposed integrated Mobile WiMAX and FSO access network is shown in Figure 7.1. To integrate FSO into the Mobile WiMAX network, the IP network between the BS and ASN-GW is built on the FSO physical layer. The simplest form is to use FSO point-to-point link as shown in Figure 7.1a. One end FSO edge node is connected to the BS and the other to the ASN-GW, through a common standard interface such as Ethernet. Upper layer traffic between the BS and ASN-GW is transmitted over the FSO link using the IP infrastructure.



a. Integrated access network using point-to-point FSO link

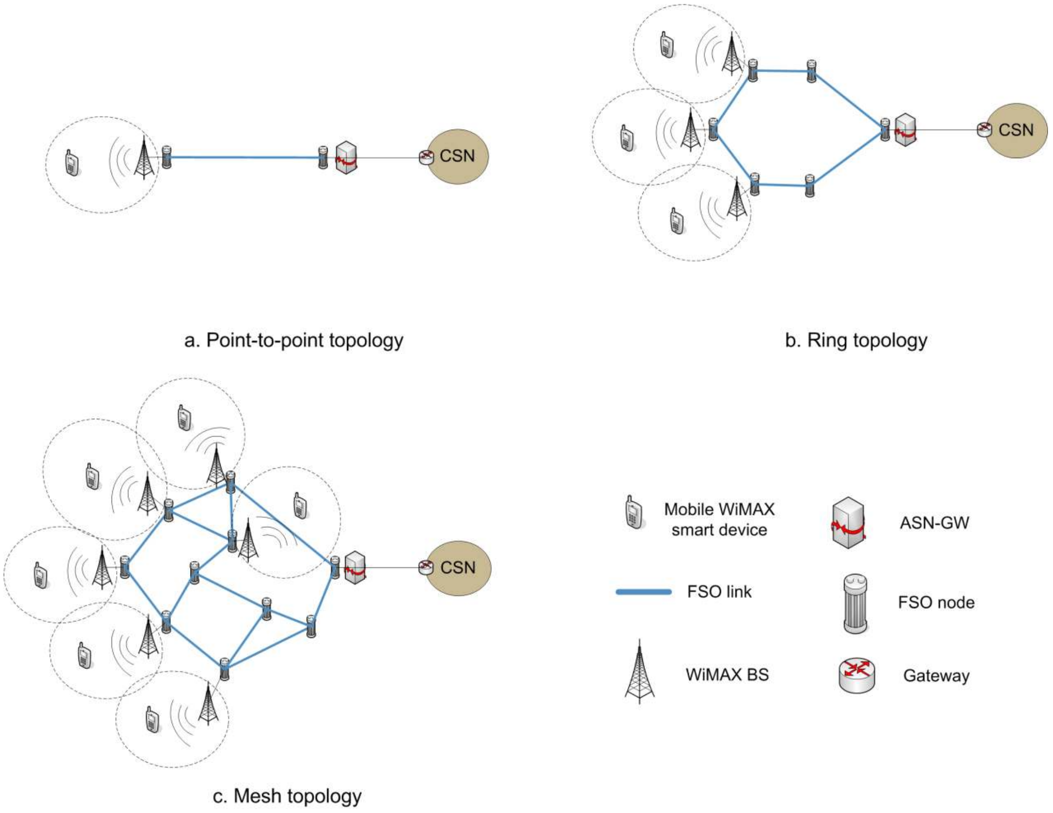
b. Integrated access network using FSO ring or mesh network

Figure 7.1 Reference model for the Integrated Mobile WiMAX and FSO access network

Figure 7.1b shows the reference model when the FSO ring or mesh network is deployed between the FSO edge nodes interconnected by the FSO intermediate nodes. Each of the FSO intermediate nodes has Layer-3 routing ability, and data packets from the BS are routed across the FSO network to the ASN-GW.

7.1.2 Network Architecture of the Integrated Mobile WiMAX and FSO Access Network

The integrated Mobile WiMAX and FSO access network architecture is shown in Figure 7.2. According to various terrains and building density and arrangements in the city as well as the amount of capital investment, different FSO network topologies could be adopted. Part (a) shows the integrated network with a point-to-point FSO link. Part (b) shows the integrated network with a ring FSO network topology. Part (c) shows the integrated network architecture with a mesh FSO network topology.



a. Point-to-point topology

b. Ring topology

c. Mesh topology

Figure 7.2 Integrated Mobile WiMAX and FSO access network architecture

Compared to integrated access networks with point-to-point and ring FSO topology, the mesh topology is considered to be the most general solution which is the architecture adopted in this dissertation. First, for network deployment in rural areas, the mesh topology could cover a much wider area. Each FSO node in the mesh network is able to connect to a BS to become a FSO edge node while the other FSO nodes work as the FSO intermediate node to perform the routing function. Therefore, each ASN-GW could manage a number of BSs to reach a wide area of coverage, and the area served by a single ASN could be sufficiently large. Second, the mesh network could achieve better routing and simpler protection strategy. In case one FSO intermediate node confronts congestion or malfunction, the traffic could be routed through other FSO intermediate nodes.

The integrated Mobile WiMAX and FSO access network provides fiber-like capacity backhaul and extends the coverage of the broadband access network. When the integrated Mobile WiMAX and fiber access network is not applicable, it provides an alternative integrated broadband solution. Such examples include areas with complex terrain where establishing fiber network is not feasible, a city downtown where fiber infrastructure is expensive and time-consuming to deploy, and natural disaster situations where fast, temporary network recovery is needed.

7.2 Unified Security Framework for Integrated Mobile WiMAX and FSO Access Networks

The security protection for the integrated Mobile WiMAX and FSO access network covers the access network between the MS and ASN-GW, including the Mobile WiMAX link established between the MS and BS, and the FSO network deployed between the BS and ASN-GW. The connection between the ASN-GW and CSN does not belong to the access network, and its security is not considered in this dissertation.

In the proposed security framework for the integrated Mobile WiMAX and FSO networks, the EAP framework is adopted to be compatible with the existing

Mobile WiMAX network architecture. EAP-TTLS is chosen as the authentication method to realize mutual authentication between the MS and AAA server and establish an encrypted Transport Layer Security (TLS) tunnel. The authentication related information carried by the EAP messages transported across the Mobile WiMAX link and the FSO network are protected by this secure TLS tunnel. IPsec is used to protect the keying material transfer after the EAP authorization as well as the normal data transmission between the BS and ASN-GW across the FSO network.

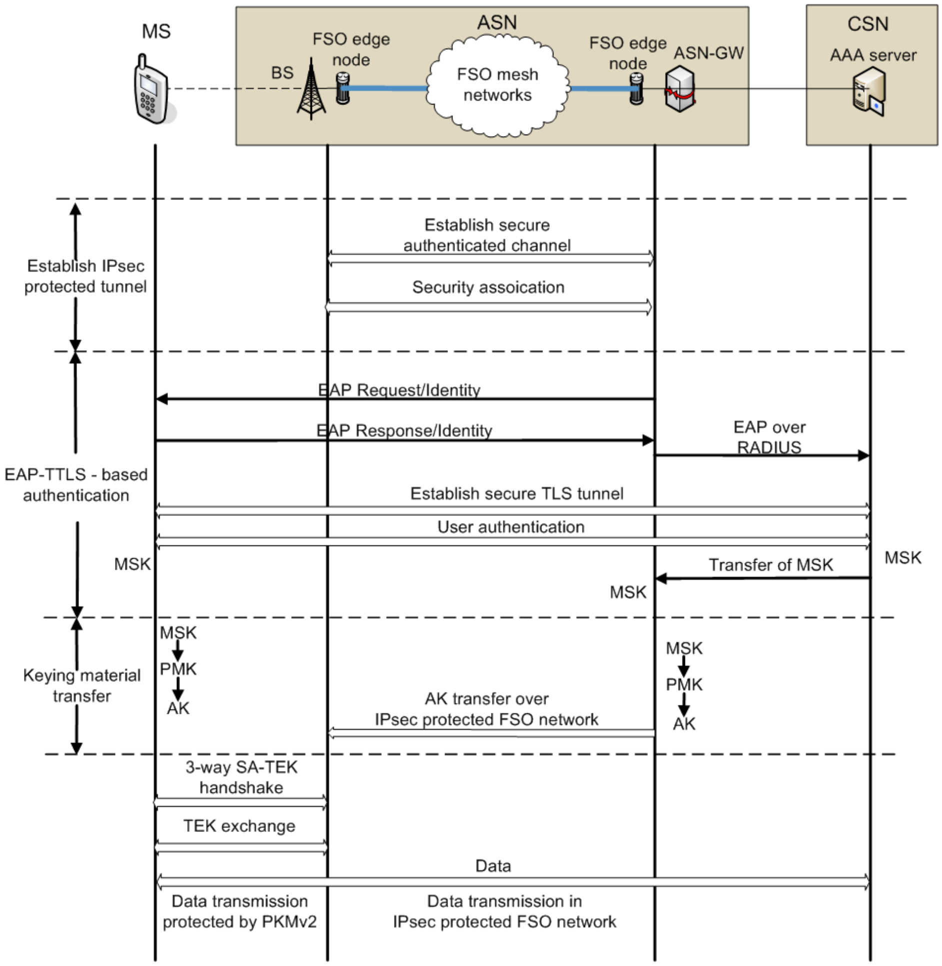


Figure 7.3 Security framework for Integrated Mobile WiMAX and FSO access network

The proposed security framework for the Mobile WiMAX and FSO access network is shown in Figure 7.3. Before the EAP-based authentication, the BS launches an IPsec protected tunnel with the corresponding ASN-GW. The IPsec security association is set up using Internet Key Exchange (IKE) protocol [76, 77] and includes two steps. First, the two FSO edge nodes authenticate each other using either pre-shared key or public key algorithm, and establish a secure communication channel. Second, security associations are negotiated between the BS and ASN-GW to generate keying material which is used to protect the IP datagram.

Next, the EAP-TTLS-based authentication takes place in two phases which are the TLS handshake phase and TLS tunnel phase. During the TLS handshake, the MS authenticates the AAA server, and the AAA server optionally authenticates the MS, based on the public-key certificates. A secure TLS tunnel is then established to secure the subsequent EAP-TTLS authentication. The cipher suite and shared keying material to encrypt the TLS tunnel is agreed by the handshake process. During the second phase, user authentication is performed and protected by the encrypted TLS tunnel, and the MSK is derived through the user authentication, which could be an EAP-based method or non-EAP-based authentication protocols. After that, the MSK is transferred from the AAA server to the ASN-GW, and an AK is derived at both the MS and ASN-GW. Then the AK located at the ASN-GW is transferred to the BS over the IPsec protected FSO network. So far, both MS and BS hold a newly generated AK. Finally, the PKMv2 security association and

TEK exchange are implemented. At the data transmission stage, the user data is encrypted by the TEK between the MS and BS and protected by the IPsec secured tunnel over the FSO network between the BS and ASN-GW.

The EAP protocol has its own in-order delivery and retransmission mechanisms [66], and it could run directly on the link layer without relying on the network layer protocol. The IKE protocol is implemented over the UDP/IP infrastructure and the generated keys are sent down to the IPsec stack. Therefore, the proposed security framework utilizing EAP-TTLS and IPsec is implemented above the link layer and is transparent to the FSO edge and intermediate nodes. The security framework also applies to the backup RF link.

7.3 Security Analysis of the Unified Framework

The EAP-based PKMv2 procedure is divided into the following three phases as shown in Figure 7.3: the EAP authentication process: the transmission of the AK from the ASN-GW to the BS and the establishment of the security association between the MS and BS. The third phase is detailed in the 802.16 standard, so here the first two phases are presented.

7.3.1 Discussion on EAP-TTLS

In EAP-based authentication described by IEEE 802.16 and WiMAX Forum, the particular credentials and EAP methods to be used are not specified. Various EAP methods, such as EAP-Transport Layer Security (EAP-TLS) [34] , EAP for Authentication and Key Agreement (EAP-AKA) [69], and EAP for GSM

Subscriber Identity (EAP-SIM) [68], are available. Currently, mutual authentication based on public key certificates is one of the most robust and secure authentication methods [66]. Like RSA-based authentication defined in PKM, EAP-TLS is also based on public key infrastructure and, therefore, is considered a strong candidate for the Mobile WiMAX network. During the EAP-TLS process, the client and the server exchange their certificates to authenticate each other and use public-key encryption techniques to generate shared master keys.

However, for the Mobile WiMAX access link between the MS and BS, the EAP packets are encapsulated in the PKMv2 management messages, and no encryption or data authentication service is provided (data authenticity is only implemented during re-authentication process [18]). For the FSO network, the EAP information is carried by the authentication relay protocol [53], and no security service is described for the authentication relay in the WiMAX Forum specification. As a result, the EAP-TLS process is performed in unencrypted form, exposing the user identity to the eavesdropper through the EAP-Identity messages and the certificate face value [66]. Furthermore, the certificate-based authentication requires the exchange of lengthy certificates, which causes latency and provides relatively low-efficiecy, especially during the handover procedure. Finally, although certificates are used by some network operators for device authentication, the X.509 certificates installed within the Mobile WiMAX CPE devices are considered manageable without incurring significant expenses. But when the certificate is used for user authentication, the maintenance and management of the large number of user certificates add much complexity and cost to the security system. Although compared to the certificate-based authentication method, legacy password-based authentication protocols, such as password authentication protocol (PAP) [78], challenge-handshake authentication protocol (CHAP) [79] and Microsoft PPP CHAP Extensions **(**MS-CHAP) [80] do not provide the same strong security level, they are more efficient and still preferred by many widely deployed authentication infrastructures for user authentication.

Therefore, in the proposed security framework, the two-phase EAP-TTLS is adopted as the authentication mechanism. The TLS tunnel established provides a secure platform where various more time-saving user authentication methods could be performed according to different vendor and market needs. In the TLS handshake phase, the client authentication part is optional. So the WiMAX network operator is able to use the first phase for the network side authentication while the second phase is implemented for client authentication using either EAP-based or non EAP-based methods. In case where the network operator wants to perform only the certificate-based mutual authentication, the second phase could be skipped and only the TLS handshake phase, which equals to EAP-TLS authentication, is implemented. Therefore, EAP-TTLS provides much flexibility and is efficient and easy to manage. Also the establishment of the TLS tunnel ensures the secret exchange of authentication information.

7.3.2 Transfer of the AK

After the EAP-based authentication finishes, the AK and its related security parameters, including AK identifier, AK sequence number and AK lifetime, which are stored in the key distributor at the ASN-GW, need to be transferred to the key receiver at the BS over a context transfer protocol [53] across the FSO network. Because this process does not belong to the EAP authentication, the transfer is not protected by the secure TLS tunnel. Also the context transfer protocol itself does not provide any security service. Although the FSO network provides a highly secure physical layer transmission channel, there still exists the vulnerability for eavesdropping. Therefore, a higher layer secure association needs to be established between the BS and ASN-GW to protect the transfer of the AK.

One approach is to apply encryption at the data link layer. Compared to Layer-3 encryption, Layer-2 encryption reduces overhead and latency and is more efficient. Additionally, less configuration and maintenance efforts are needed once deployed. However, Layer-2 encryption is only suitable for the point-to-point FSO connection where no Layer-3 action needs to be performed in between. If implemented for the FSO mesh network where Layer-3 routing is needed, double encryption and decryption have to be performed at each FSO intermediate node which increases the processing burden. Also a pair of encryption keys must be shared among every two FSO nodes, adding to the complexity of security management for the FSO node. Therefore higher layer protection solution is preferred. In the proposed security framework, IPsec is applied, which is indicated as one of the possible secure methods by the WiMAX Forum specification. As an

IP layer security mechanism, IPsec establishes a security channel between two entities to provide data confidentiality, data integrity, anti-replay protection, and a number of other security services [66]. The transfer of the AK and the data transmission are protected by the IPsec secured FSO network.

The establishment of IPsec security association also prevents a disguised BS from implementing a masquerade attack. In the integrated Mobile WiMAX and FSO networks, during the IKE process, mutual authentication is performed between the BS and ASN-GW across the FSO network. On the other hand, the ASN-GW has already established a trust relationship with the AAA server in the CSN when the Mobile WiMAX broadband network was initially built. As a result, after the BS is authenticated by the ASN-GW, it is also authenticated by the CSN. During the initial authentication process or the handover procedure where re-authentication is needed, because only a legal BS has the ability to build trust relationship with the CSN, it is impossible for a malicious BS to acquire the AAA server's certificate and relay it to the MS to complete the EAP authentication so as to perform masquerading.

7. 4 Summary

This chapter has presented an integrated Mobile WiMAX and FSO broadband access network. It has proposed a unified security framework for the integrated WiMAX-FSO access network based on EAP-TTLS and IPsec. The analysis has shown that EAP-TTLS provides a flexible, efficient, and secure authentication framework, and IPsec could secure the key transfer and data transmission across the FSO mesh network.

Chapter 8 Performance Evaluation of EAP-based Authentication for Proposed Integrated Mobile WiMAX and FSO Access Networks

Abstract: This chapter evaluates and compares the performance of EAP-TLS and EAP-TTLS for the proposed integrated FSO-WiMAX access network. It also evaluates the impact of the point-to-point FSO link in the integrated access network. The measurement shows that compared to EAP-TLS, EAP-TTLS provides a more flexible, efficient, and secure way to protect the integrated FSO-WiMAX access network. The experiment also demonstrates that the point-to-point FSO link does not degrade the performance of EAP authentication in the integrated network.

8.1 EAP-TLS and EAP-TTLS

The EAP-based authentication protocol stack for the integrated Mobile WiMAX and FSO access network is shown in Figure 8.1. Between the MS and BS, EAP messages are encapsulated in PKMv2 management messages and transported by the 802.16 protocol. Between the BS and ASN-GW, the EAP messages are relayed by an authentication relay protocol [53]. Between the ASN-GW and the AAA server, EAP packets are forwarded over the UDP/IP network by AAA protocols, such as remote authentication dial in user service (RADIUS) [60].

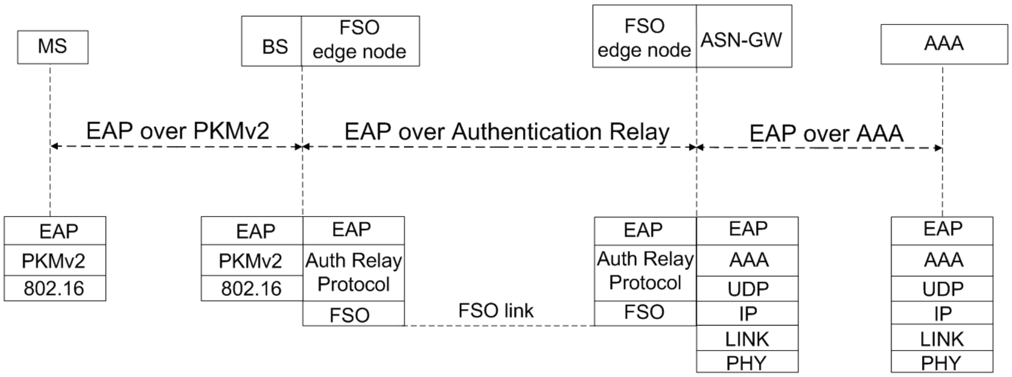


Figure 8.1 EAP-based authentication protocol stack for integrated Mobile WiMAX and FSO networks

In IEEE 802.16 standards and WiMAX Forum[52], the particular credentials and EAP methods to be used are not specified [31, 53], and a variety of EAP methods are considered. In this chapter, the performance of EAP-TLS and EAP-TTLS is mainly evaluated for integrated Mobile WiMAX and FSO access networks.

EAP-TLS is based on Public Key Infrastructure (PKI) [32] and the use of X.509 certificate [32]. The EAP-TLS procedure is shown in Figure 8.2, and RADIUS is used as the AAA server. During the EAP-TLS process, the client and the RADIUS server exchange their certificates to authenticate each other’s identity, negotiate the cipher suit to be used, and use public-key encryption techniques to generate shared master keys.

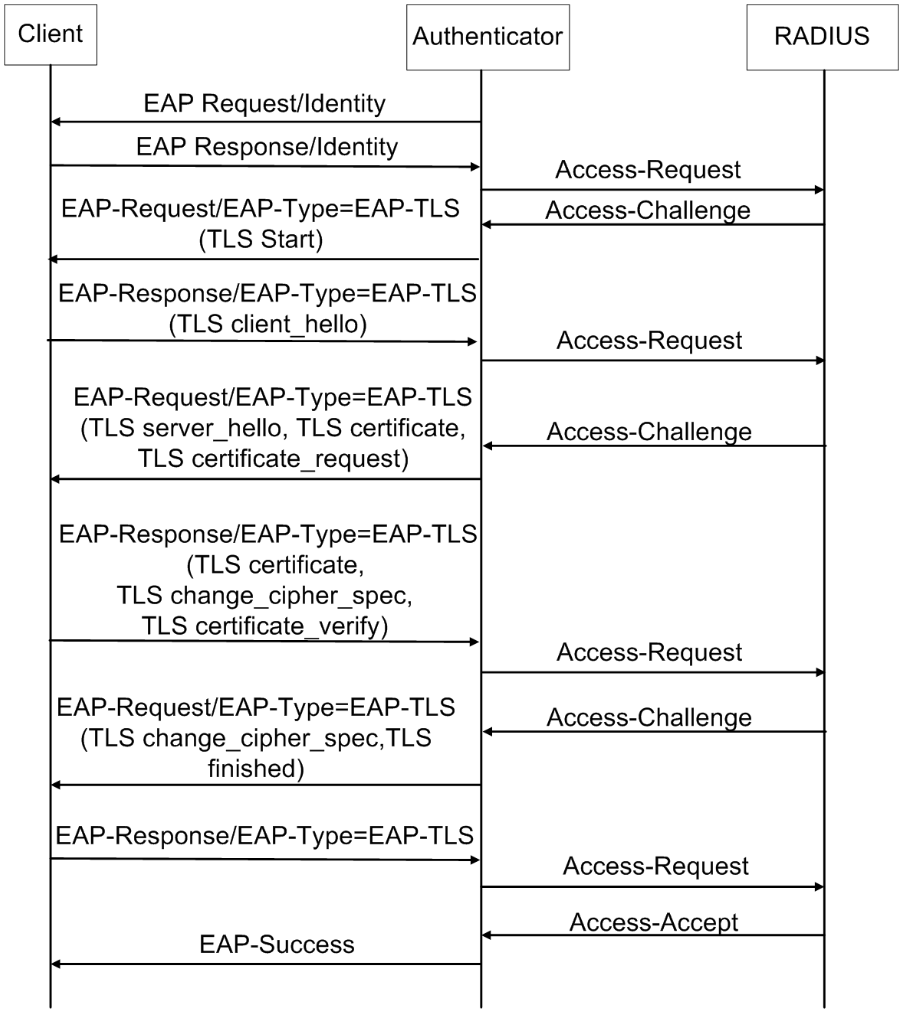


Figure 8.2 EAP-TLS procedure

EAP-TTLS is an EAP method which incorporates both the TLS handshake phase and a data phase. During the TLS handshake phase, the client authenticates the server, and the server optionally authenticates the client, based on the public-key certificates. Shared keying material is generated to encrypt the TLS tunnel to secure the subsequent user authentication. During the data phase, user authentication is performed within the protected TLS tunnel. The authentication method could be an EAP-based method or legacy password-based authentication protocols. The client authentication part in the TLS handshake phase is optional, and the Mobile WiMAX network operator is able to use the first phase for the network side authentication while the second phase is implemented for user authentication using password-based methods. In a case where both device and user authentication are needed, mutual authentication between the client side and server side based on certificates is performed during the TLS handshake phase, and the client side authentication could be served for device authentication. The user authentication is then implemented during the data phase.

8.2 Performance Evaluation

8.2.1 Evaluation Purpose

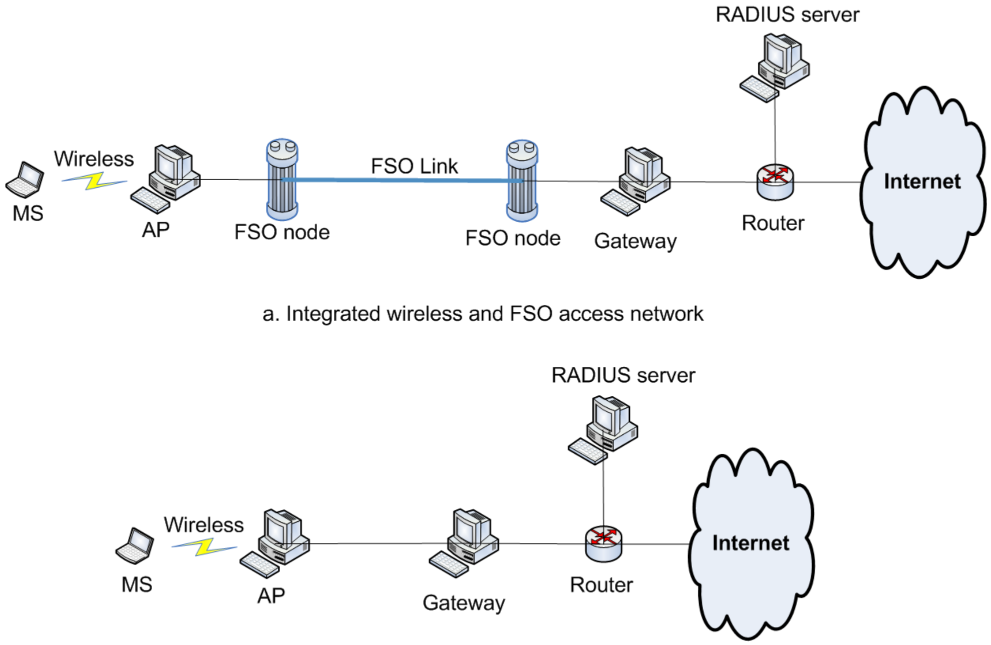
The first evaluation purpose is to compare the performance of EAP-TLS and EAP-TTLS in integrated Mobile WiMAX and FSO access networks. In the experiment, Wi-Fi air interface is used to replace the WiMAX air interface, and the Wi-Fi access point (AP), rather than the ASN-GW, behaves as authenticator. The EAP authentication happens between the MS and the RADIUS server, and the authenticator only acts as a pass-through device to relay the EAP message. Furthermore, the EAP is implemented above the link layer, and it does not care about the air interface that it is running over. Therefore, the replacement will not affect the comparison of EAP-TLS and EAP-TTLS.

Two performance metrics are used in the evaluation: the number of authentication messages (N) and the authentication time (T). During the EAP procedure after the EAP client sends the EAP Response/Identity to the authenticator, the first RADIUS Access-Request message is used to denote the beginning of the authentication process and the RADIUS Access-Accept message that indicates the completion. The number of authentication messages (N) is defined as the total number of RADIUS messages involved to perform the EAP process. The authentication time (T) is defined as the time taken to complete the EAP authentication.

The second evaluation purpose is to test the impact of the FSO link on the performance of the EAP authentication process. To test how the FSO link affects the authentication performance in the integrated access network, all evaluations are performed in two network scenarios. The first scenario is an integrated network that incorporates both Wi-Fi and FSO segments while the second scenario does not contain the FSO link.

8.2.2 Testbed Setup

Figure 8.3 illustrates the experimental setup. Here the integrated wireless and FSO access network is named scenario (a) and the access network without the FSO link is named scenario (b). In scenario (a), point-to-point FSO network topology is used.



a. Integrated wireless and FSO access network

b. Access network without FSO link

Figure 8.3 Testbed architecture

A. Hardware Configuration

The MS is a Toshiba laptop with Intel Pentium M 1.5 GHz. AP is a Dell desktop with Intel Pentium 4 2.8 GHz. The Wi-Fi card used in the MS is an Intel Corporation PRO/Wireless 2200BG Network Connection. The Wi-Fi card used in the AP to function as the wireless access point is a Broadcom Corporation BCM4318 802.11g Wireless LAN Controller. The gateway is a Dell desktop with Intel Pentium 4 1.6 GHz. A point-to-point FSO link is established between the AP and Gateway using two FSO nodes. One of the FSO nodes is connected to the AP, and the other one is connected to the Gateway. The FSO node uses OmniNode manufactured by Omnilux, Inc. [81]. A Juniper SSG5 router connects the Gateway to the outer network. A RADIUS server is also connected through the router to the access network, and the server is a Dell desktop with Intel Pentium 4 2.8 GHz. For scenario (b), the FSO link is eliminated, and the AP is connected directly to the Gateway.

Table 8.1 Open-source software used in the testbed

Component	**Software**
MS	wpa_supplicant
AP	hostapd, Wireshark
Radius server	Freeradius, OpenSSL, Wireshark

B. Software Configuration

The MS uses the Ubuntu Linux operating system with a 2.6.27 version kernel, and all the other computers use Ubuntu Linux operating system with a 2.6.32 version kernel. The open-source software installed is shown in Table 8.1. The MS uses wpa_supplicant [82] to support the EAP client function. The AP uses hostapd [83] to implement IEEE 802.11 access point management and the EAP authenticator/RADIUS client. Freeradius [84] is installed in the server machine to perform the RADIUS protocol and function as the AAA server. OpenSSL [85] is utilized to create the X.509 certificates. Wireshark is used to capture and analyze the RADIUS and EAP messages.

8.2.3 Evaluated EAP Methods

The EAP methods implemented in the evaluation are show in Table 8.2. In the evaluation of EAP-TTLS, for the TLS phase, two scenarios are considered. In the first scenario, only server side authentication is implemented. In the second scenario, mutual authentication between the client and the server based on X.509 certificates is performed. EAP-TTLSm is used to denote the EAP-TTLS method where mutual authentication between the client and server are performed during the TLS phase.

Table 8.2 Evaluated EAP methods

No.	**EAP method**	**TLS Phase**		**Data Phase**
		Client Auth	**Server Auth**	**User Auth**
1	EAP-TLS	✓	✓	×
2	EAP-TTLS/CHAP	×	✓	✓
3	EAP-TTLS/PAP	×	✓	✓
4	EAP-TTLS/MS-CHAPv1	×	✓	✓
5	EAP-TTLS/MS-CHAPv2	×	✓	✓
2m	EAP-TTLSm/CHAP	✓	✓	✓
3m	EAP-TTLSm/PAP	✓	✓	✓
4m	EAP-TTLSm/MS-CHAPv1	✓	✓	✓
5m	EAP-TTLSm/MS-CHAPv2	✓	✓	✓

Regarding the data phase of EAP-TTLS, four widely deployed password-based authentication methods are considered in the evaluation: password authentication protocol (PAP) [78], challenge-handshake authentication protocol (CHAP) [79], Microsoft PPP CHAP Extensions **(**MS-CHAPv1) [80], and Microsoft PPP CHAP Extensions, version 2 (MS-CHAPv2). PAP is based on username and password sent in the clear text. CHAP uses an algorithm (MD5[86] is used in this dissertation) to calculate the shared value between the client and the server to avoid the transmission of the password. MS-CHAP is a variant version of CHAP developed by Microsoft, and two versions exist: MS-CHAPv1 and MS-CHAPv2.

8.3 Evaluation Results

The experimental results are presented and compared in this section. All the EAP methods are implemented in both scenario (a) and (b) shown in Figure 8.3.

8.3.1 Number of Authentication Messages (N)

For each EAP method listed in Table 8.2, Figure 8.4 illustrates the number of authentication messages that are transferred between the EAP authenticator and the RADIUS server. The EAP protocol is running over the FSO layer; therefore, the FSO link will not affect the number of authentication messages. For each EAP method, the number of authentication messages in scenario (a) is the same as that in scenario (b).

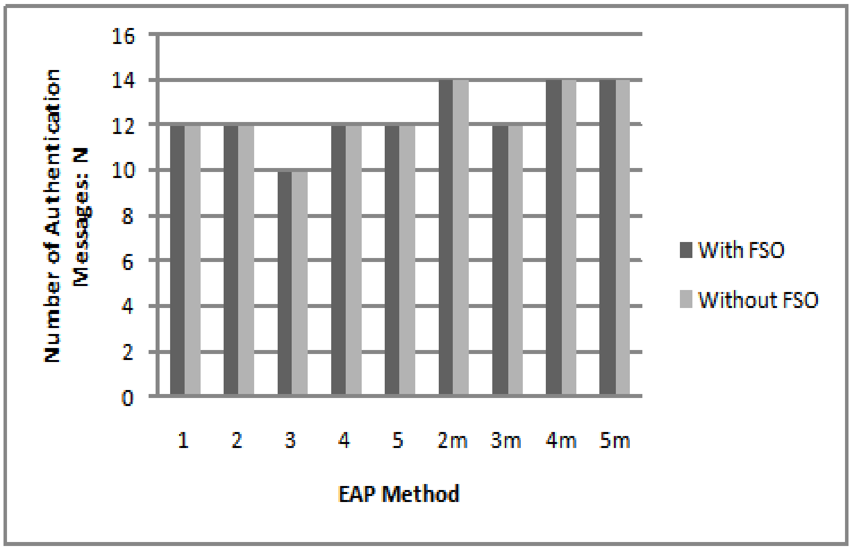


Figure 8.4 Number of authentication messages

EAP-TLS involves 12 RADIUS messages. Among these 12 messages, the first one is used to transmit the client’s identity to the server, and the second one is used to indicate the start of the EAP process. Then 8 messages are used for TLS phase to exchange certificates, associate cipher suits, and derive encryption keys. The 11th message is EAP-Response and the last one is EAP-Success. The same as EAP-TLS, EAP-TTLS/CHAP also involves 12 messages. Because the client authentication is skipped, only 6 messages are used to complete the TLS phase. Then 3 messages are used to perform CHAP authentication and the last one is EAP-Success. EAP-TTLS/PAP involves 10 messages. The first 8 messages are the same as those in EAP-TTLS/CHAP, and the 9th message is used for PAP authentication to convey the user name and password to the server. Both EAP-TTLS/MS-CHAPv1 and EAP-TTLS/MS-CHAPv2 need 12 messages. The functions of these messages are the same as that of EAP-TTLS/CHAP, and 3 messages are used to implement MS-CHAP authentication.

For EAP-TTLSm, because the client authentication is added in the TLS phase, two more messages are needed. Therefore, EAP-TTLSm/CHAP uses 14 messages, EAP-TTLSm/PAP uses 12 messages, and both EAP-TTLS/MS-CHAPv1 and EAP-TTLS/MS-CHAPv2 use 14 messages.

8.3.2 Authentication Time (T)

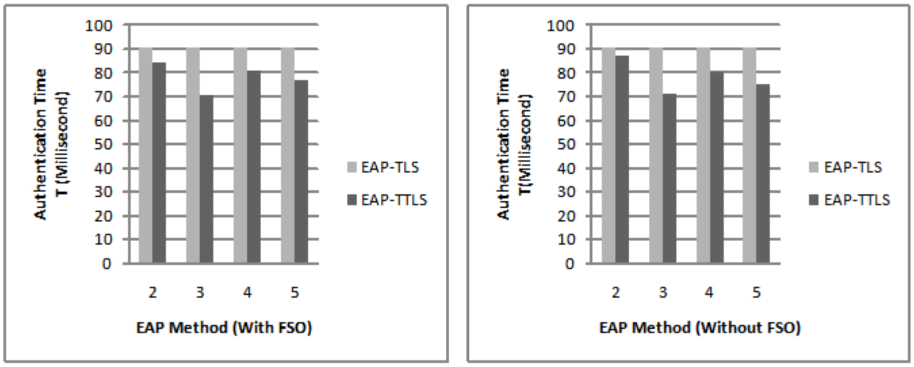
Table 8.3 illustrates the authentication time for each EAP method in both scenario (a) and (b).

Table 8.3 Authentication time (T)

No.	**EAP method**	**T (Millisecond)** **Scenario (a)**	**T (Millisecond)** **Scenario (b)**
1	EAP-TLS	91.0199	90.7220
2	EAP-TTLS/CHAP	84.4217	87.4979
3	EAP-TTLS/PAP	70.8996	71.5485
4	EAP-TTLS/MS-CHAPv1	81.0693	80.7520
5	EAP-TTLS/MS-CHAPv2	76.9929	75.1873
2m	EAP-TTLSm/CHAP	95.3690	98.5901
3m	EAP-TTLSm/PAP	92.7377	92.7284
4m	EAP-TTLSm/MS-CHAPv1	98.2864	96.6281
5m	EAP-TTLSm/MS-CHAPv2	94.5589	94.8455

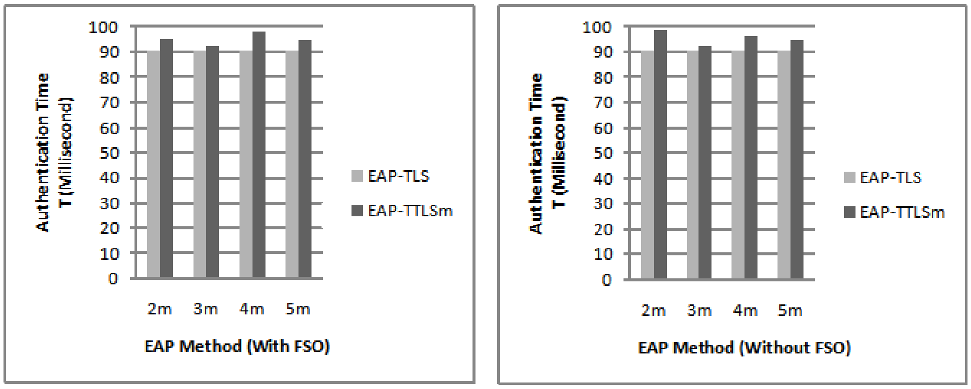
Figure 8.5 compares the authentication time between EAP-TLS and EAP-TTLS. Figure 8.5 (a) shows the comparison result of scenario (a). It is observed that

EAP-TTLS causes less authentication delay than EAP-TLS because the certificate-based, client-side authentication is skipped during the TLS phase for EAP-TTLS. Among the four EAP-TTLS methods, EAP-TTLS/PAP takes less time than the other three schemes due to the fact that CHAP uses two more EAP messages than PAP. Figure 8.5 (b) demonstrates the comparison result of scenario (b), which shows the same characteristic as scenario (a).



(a) (b)

Figure 8.5 EAP-TLS vs. EAP-TTLS



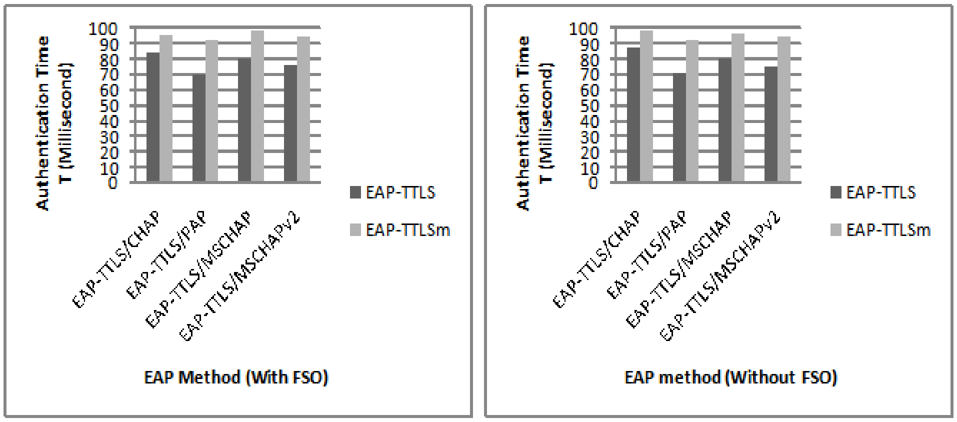
(a) (b)

Figure 8.6 EAP-TLS vs. EAP-TTLSm

Figure 8.6 compares the authentication time between EAP-TLS and EAP-

TTLSm. Because both EAP-TLS and EAP-TTLSm implement mutual authentication in the TLS phase while EAP-TTLSm has one more data phase, it is observed that each of the four EAP-TTLSm methods involves longer authentication time than EAP-TLS. Again, evaluation results in scenario (a) and (b) show the same feature.

Figure 8.7 compares the performance between EAP-TTLS and EAP-TTLSm. Because the incorporation of the client side authentication in TLS phase, each of the EAP-TTLSm methods takes longer authentication time than its EAP-TTLS version.



(a)

(b)

Figure 8.7 EAP-TTLS vs. EAP-TTLSm

Figure 8.8 compares the EAP authentication performance in scenarios (a) and scenario (b). For each EAP method, it is observed that the difference of authentication time between scenario (a) and scenario (b) is less than 4 milliseconds. Among all the authentication methods, there is 3.1-millisecond time difference for EAP-TTLS/CHAP and a 3.2-millisecond time difference for EAP-TTLSm/CHAP. There is 1.8-millisecond time difference for EAP-TTLS/MS-CHAPv2 and 1.7-millisecond time difference for EAP-TTLSm/MS-CHAPv1. The time difference for each of the other EAP methods is less than 1 millisecond. Therefore, from the experiment, it is concluded that the point-to-point FSO link does not add any latency to EAP-based authentication.

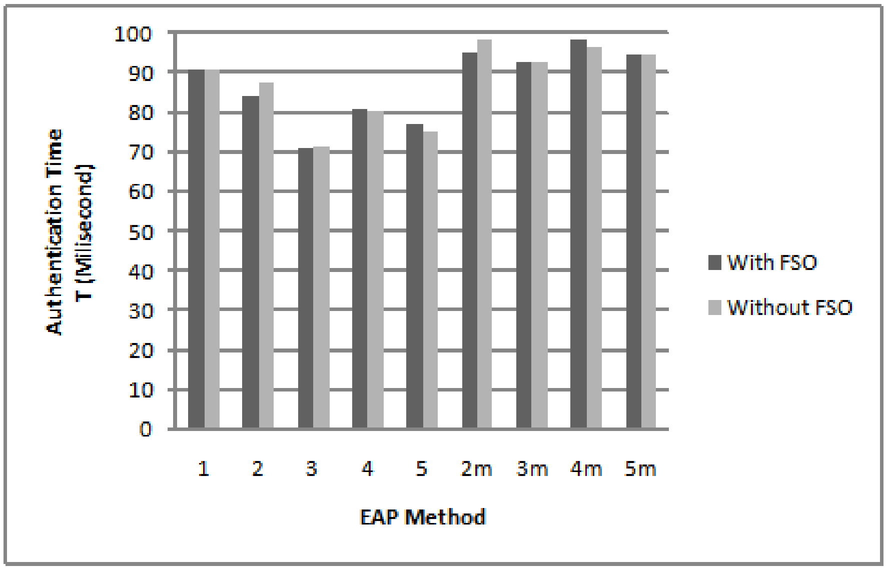


Figure 8.8 Scenario (a) vs. Scenario (b)

8.3.3 Discussion

In WiMAX Forum, both EAP-TLS and EAP-TTLS are considered candidates for the authentication of Mobile WiMAX networks. Currently the X.509 certificate is widely used by network operators for device authentication. Certificates installed within the Mobile WiMAX CPE devices are considered manageable without incurring great expense. But when the certificate is used for user authentication, the maintenance and management of the large number of the user certificates increase delay, complexity, and cost to the security system. Through the measurement and evaluation, it is observed that when no certificate-based, client-side authentication is performed during the TLS phase, the implementation of EAP-TLS involves longer authentication time than EAP-TTLS because the exchange of lengthy certificate causes more latency than password-based authentication. Compared to the certificate-based authentication method, legacy password-based authentication protocols are more efficient and still preferred by many widely deployed authentication infrastructures for user authentication. Therefore, EAP-TTLS provides a TLS tunnel where various more time-saving user authentication methods could be performed.

Furthermore, in integrated Mobile WiMAX and FSO access networks, for the WiMAX air interface, no encryption or data authentication service is provided for the EAP packets (data authenticity is only implemented during re-authentication process [18]). For the FSO network, the EAP information is carried by the authentication relay protocol, and no security service is described for the authentication relay in the WiMAX Forum specification. As a result, the EAP-TLS process is performed in unencrypted form, which exposes the user identity to the eavesdropper through the EAP-Identity messages and the certificate face value. Compared to EAP-TLS, EAP-TTLS offers a secure tunnel established by TLS handshake to protect the FSO network from eavesdropping.

From the experiment, it is observed that when client-side authentication is enabled, EAP-TTLS authentication involves EAP-TLS authentication *and* user authentication, and it takes a longer time than EAP-TLS authentication to finish. Therefore, EAP-TTLS could incorporate the full function of EAP-TLS to provide more flexibility and better management according to different vendor and market needs.

Finally, it is observed that the insertion of the point-to-point FSO link does not add delay to EAP-based authentication. Because the FSO signal propagates at the speed of light, the transmission distance is also not considered a factor that affects the performance of the authentication process. However, when the FSO mesh topology is adopted, a number of intermediate FSO nodes are required and the processing delay in each FSO node is increased. Therefore, more evaluations are needed to test the impact of FSO mesh network on the performance of EAP authentication procedure.

8.4 Summary

This chapter has evaluated and compared the performance of EAP-TLS and EAP-TTLS for the proposed integrated Mobile WiMAX and FSO access network. A hybrid access network testbed was established in the laboratory. This consisted of a front-end Wi-Fi network and a backhaul point-to-point FSO link. The measure has shown that compared to EAP-TLS, EAP-TTLS provides a more flexible and efficient way to secure the integrated access network. Also the evaluation has shown that the point-to-point FSO does not degrade the performance of EAP-based authentication.

Chapter 9 Conclusions

This dissertation has proposed new network architectures for functionally integration of WiMAX and optical access networks. The proposed integrated access networks combine the strengths of optical and wireless technologies, and achieve efficient and simplified system management. Based on the integrated architectures, the dissertation proposed security frameworks to unify both the WiMAX and optical security systems and protect the access network security. The analysis has shown that the integrated security solutions enhance the overall system security level and realize efficient and unified management.

In the first part of the dissertation, a WiMAX over EPON reference model is proposed, which places the WiMAX MAC layer on top of the EPON MAC layer so as to encapsulate each WiMAX MAC PDU into one EPON Ethernet frame. Then an end-to-end WiMAX over EPON network architecture and its layer-3 security framework are presented. Compared to other contemporary WiMAX and EPON integration solutions, the WiMAX over EPON network achieves integrated and simplified system management, improves the overall network efficiency, reduces latency, and saves cost. A security framework for the WiMAX over EPON network using PKI and PKM authorization protocol is further presented. Through the analysis, it is shown that this framework enhances the system security and realizes unified and efficient key management.

In the second part of the dissertation, three handover scenarios in the WiMAX over EPON network are introduced, intra-OLT-BS, inter-OLT-BS, and inter-ASN handover, and the corresponding handover schemes are proposed. In the proposed mechanisms, the ranging management messages including RNG-REQ and RNG-RSP are used to carry authentication-related information to implement mutual authentication, and a pre-authentication method is utilized to pre-distribute the shared authorization key. Through analysis, it is shown that compared to the standard 9-step WiMAX handover process, the proposed intra-OLT-BS handover scheme consists of only 5 steps, and both the inter-OLT-BS and inter-ASN handover procedure is reduced to 7 steps. Further, the proposed schemes realize mutual authentication between the MS and the mobile network.

In the third part of the dissertation, an integrated mobile WiMAX and FSO broadband access network is proposed where the FSO mesh network is used to backhaul the front end Mobile WiMAX access. Next, a unified security framework for the integrated Mobile WiMAX and FSO access network is presented. In this framework, EAP-TTLS is used as the authentication and key management protocol, and IPsec as the security scheme for the FSO network. Such higher layer protection applies to both the FSO and backup RF links. Through the analysis, it is shown that EAP-TTLS provides a flexible, efficient, and secure authentication framework, and IPsec could secure the key transfer and data transmission across the FSO mesh network.

In the last part of the dissertation, the performance of EAP-TLS and EAP-TTLS for the proposed integrated Mobile WiMAX and FSO access network is evaluated and compared. A hybrid access network testbed is built, which consists of a front-end Wi-Fi network and a backhaul point-to-point FSO link. The number of authentication messages and authentication time is tested. The measurements show that compared to EAP-TLS, EAP-TTLS provides a more flexible and efficient way to secure the integrated access network. Also the evaluation shows that the point-to-point FSO does not degrade the performance of EAP-based authentication.

Based on research presented in this dissertation, future research could focus on the following areas. First, in the WiMAX over EPON access networks, secure and time-saving handover mechanism is needed for scenarios when the MS moves between different CSNs and the authentication procedure involves more than one AAA server. Second, because the WiMAX over EPON and LTE networks use different authentication and encryption schemes, security interoperability needs to be explored when the handover takes place between the integrated access network and the LTE network. Third, regarding the integrated Mobile WiMAX and FSO access network, the implementation experiment used for the security frameworks presented in this dissertation could be expanded to evaluate the impact of ring and mesh FSO networks.

References

[1] "Evolution Of Dialup Internet Access," http://www.free-dialup.net/free-internet-articles/evolution-of-dialup-internet-access.html.

[2] "Dial-up Internet access," http://en.wikipedia.org/wiki/Dial-up_Internet_access.

[3] "The Birth of Broadband," http://www.itu.int/osg/spu/publications/birthofbroadband/faq.html.

[4] "What is Broadband," http://www.fcc.gov/cgb/broadband.html.

[5] "List of countries by number of broadband Internet users "; http://en.wikipedia.org/wiki/List_of_countries_by_number_of_broadband_Internet_users.

[6] "US 20th in broadband penetration, trails S. Korea, Estonia," http://arstechnica.com/tech-policy/news/2009/06/us-20th-in-broadband-penetration-trails-s-korea-estonia.ars.

[7] C. M. Akujuobi, and M. N. O. Sadiku, “The present and future of broadband communications,” *Potentials, IEEE,* vol. 24, no. 4, pp. 12-16, 2005.

[8] "IEEE Standard for Information technology-Telecommunications and information exchange between systems - Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE std. 802.11*, 2007.

[9] J. Gibbons, and S. Ruth, “Municipal Wi-Fi: big wave or wipeout?,” *Internet Computing, IEEE,* vol. 10, no. 3, pp. 66-71, 2006.

[10] "IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CMSA/CD) Access Method and Physical Layer Specifications," *IEEE Std 802.3ah*, 2008.

[11] "ITU-T Recommendation ITU-T G.984. Gigabit Capable Optical Access Network.."

[12] "SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS. Digital sections and digital line system – Optical line systems for local and access networks: Gigabit-capable passive optical networks (GPON): General characteristics," *ITU-T G.984.1*, 2008.

[13] W. Stallings, *Data and Computer Communications, Seventh Edition*: Pearson Prentice Hall, 2004.

[14] H. Willebrand, and B. Ghuman, *Free space optics: enabling optical connectivity in today's networks*: SAMS, 2002.

[15] S. V. Kartalopoulos, "Free Space Optical Mesh Networks For Broadband Inner-city Communications," in NOC 2005, 10th European Conference on Networks and Optical Communications, University College London, 2005, pp. 344-351.

[16] S. V. Kartalopoulos, "Security of reconfigurable FSO mesh networks and application to disaster areas," in Enabling Photonics Technologies for Defense, Security, and Aerospace Applications IV, Orlando, FL, USA, 2008, pp. 69750A-7.

[17] "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," *IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001)*, 2004, pp. 0_1-857.

[18] "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," *IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004)*, 2006, pp. 0_1-822.

[19] "ITU global standard for international mobile telecommunications ´IMT-Advanced´," http://www.itu.int/ITU-R/index.asp?category=information&rlink=imt-advanced&lang=en.

[20] "International Telecommunication Union," http://www.itu.int.

[21] Z. Abichar, P. Yanlin, and J. M. Chang, "WiMax: The Emergence of Wireless Broadband," *IT Professional*, vol. 8, no. 4, pp. 44-48, 2006.

[22] "Radiocommunication Sector (ITU-R)," http://www.itu.int/ITU-R/index.asp?category=information&rlink=rhome&lang=en.

[23] "Requirements related to technical performance for IMT-Advanced radio interface(s)," *ITU-R M.2134*, ITU, 2008.

[24] "IEEE 802.16 Task Group m (TGm)," http://www.ieee802.org/16/tgm/.

[25] "3GPP - LTE-Advanced," http://www.3gpp.org/LTE-Advanced.

[26] H. Holma, and A. Toskala, *WCDMA for UMTS: radio access for third generation mobile communications*: Wiley, 2001.

[27] "3rd Generation Partnership Project," http://www.3gpp.org/.

[28] T. Wen, E. Sich, Z. Peiying *et al.*, “True broadband multimedia experience,” *Microwave Magazine, IEEE*, vol. 9, no. 4, pp. 64-71, 2008.

[29] R. Sailer, H. Federrath, and A. Pfitzmann, “Security Functions in Telecommunications: Placement & Achievable Security,” *Multilateral Security in Communications, Addison-Wesley-Longman*, pp. 323-348, 1999.

[30] "WiMAX Deployment Considerations for Fixed Wireless Access in the 2.5 GHz and 3.5 GHz Licensed Bands," *WiMAX Forum White Paper*, June, 2005. Available at: http://www.wimaxforum.org/sites/wimaxforum.org/files/document_library/deploymentconsiderations_white_paperrev_1_4.pdf

[31] "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems," *IEEE Std 802.16-2009 (Revision of IEEE Std 802.16-2004)*, 2009, pp. C1-2004.

[32] W. Stallings, *Cryptography and network security: principles and practice*: Pearson / Prentice Hall, 2006.

[33] "Extensible Authentication Protocol (EAP)," *RFC 3748*, 2004.

[34] "The EAP-TLS Authentication Protocol," *RFC 5216*, 2008.

[35] "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)," *RFC 5281*, IETF, 2008.

[36] W. W. Diab, and H. M. Frazier, *Ethernet in the First Mile project - Access for Everyone*: IEEE Standards Information Network, 2006.

[37] C. H. Lee, W. V. Sorin, and B. Y. Kim, “Fiber to the Home Using a PON Infrastructure,” *Lightwave Technology, Journal of*, vol. 24, no. 12, pp. 4568-4583, 2006.

[38] "10Gb/s Ethernet Passive Optical Network," *IEEE Std. 802.3av*, 2009.

[39] K. Grobe, and J. P. Elbers, “PON in adolescence: from TDMA to WDM-PON,” *Communications Magazine, IEEE*, vol. 46, no. 1, pp. 26-34, 2008.

[40] S. V. Kartalopoulos, *Introduction to DWDM Technology: Data in a Rainbow*: Wiley-IEEE Press, 1999.

[41] S. V. Kartalopoulos, “Next Generation Hierarchical CWDM/TDM-PON network with Scalable Bandwidth Deliverability to the Premises,” *Optical Systems and Networks*, vol. 2, pp. 164-175, 2005.

[42] S. V. Kartalopoulos, “Security and Bandwidth Elasticity Aspects of the CWDM/TDM-PON network,” *WSEAS Transactions on Communications,* vol. 5, no. 8, pp. 1461-1468, 2006.

[43] S. V. Kartalopoulos, and A. Sierra, “Engineering a Scalable and Bandwidth Elastic Next Generation PON,” *Optical Fiber Communication and the National Fiber Optic Engineers Conference, 2007. OFC/NFOEC 2007. Conference on*, pp. 1-8, 2007.

[44] K. Glen, *Ethernet passive optical networks*: McGraw-Hill, 2005.

[45] S. V. Kartalopoulos, “Free space optical nodes applicable to simultaneous ring and mesh networks,” in Advanced Free-Space Optical Communication Techniques/Applications II and Photonic Components/Architectures for Microwave Systems and Displays, Stockholm, Sweden, 2006, pp. 639902-6.

[46] S. V. Kartalopoulos, "Protection Strategies and Fault Avoidance in Free Space Optical Mesh Networks." pp. 797-801.

[47] J. Akella, L. Chang, D. Partyka *et al.*, "Building blocks for mobile free-space-optical networks." pp. 164-168.

[48] A. Desai, and S. Milner, “Autonomous Reconfiguration in Free-Space Optical Sensor Networks,” *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 8, pp. 1556-1563, 2005.

[49] K. Yoshida, and T. Tsujimura, "Tracking Control of the Mobile Terminal in an Active Free-Space Optical Communication System." pp. 369-374.

[50] K. Peng, T. Deng, Y. Lu *et al.*, "Research of signal tracking technology in FSO communication." pp. 67951U-5.

[51] "Mobile WiMAX–Part I A Technical Overview and Performance Evaluation," *WiMAX Forum white paper*, 2006.

[52] “WiMAX Forum,” *http://www.wimaxforum.org/*.

[53] "WiMAX Forum® Network Architecture (Stage 2: Architecture Tenets, Reference Model and Reference Points), Release 1.5 Version 1," *WiMAX Forum*, 2009.

[54] K. Tsagkaris, and P. Demestichas, "WiMax network," *Vehicular Technology Magazine, IEEE,* vol. 4, no. 2, pp. 24-35, 2009.

[55] "Generic Routing Encapsulation over IPv4 networks," *RFC 1702*, IETF, 1994.

[56] L. Nuaymi, *WiMAX: Technology for Broadband Wireless Access*: Wiley, 2007.

[57] "Port Based Network Access Control," *IEEE 802.1x*, 2004.

[58] J. Weise. "Public Key Infrastructure Overview," http://www.sun.com/blueprints/0801/publickey.pdf.

[59] K. Su-Hyung, K. Young-Seok, and O. Yun-Je, *US2004/0179521A1 - Authentication Method and Apparatus in EPON*, A. P. Office, 2004.

[60] "Remote Authentication Dial In User Service (RADIUS)," *RFC 2865*, 2000.

[61] R. Sun-Sik, and K. Su-Hyun, "Security model and authentication protocol in EPON-based optical access network." pp. 99-102 vol.1.

[62] L. Hak-Phil, P. Se-Kang, S. Whan-Jin *et al.*, *US2005/0047602A1 - Gigabit Ethernet based Passive Optical Network and Data Encryption Method*, A. P. Office, 2005.

[63] E. Jee-Sook, and K. Yool, "The Design of Key Security in Ethernet PON." pp. 1026-1030.

[64] H. Ziping, S. V. Kartalopoulos, and P. K. Verma, "NIS03-3: RC4-based Security in Ethernet Passive Optical Networks." pp. 1-3.

[65] "Optical Wireless Security," http://www.freespaceoptics.org/freespaceoptics/materials/pdf/LightPointe_WP_Security2.0.pdf.

[66] M. Nakhjiri, and M. Nakhjiri, *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility*: John Wiley & Sons, 2005.

[67] "The EAP-TLS Authentication Protocol," *RFC 5216*, 2008.

[68] "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)," *RFC 4186*, 2006.

[69] "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," *RFC 4187*, 2006.

[70] S. Gangxiang, R. S. Tucker, and C. Chang-Joon, “Fixed Mobile Convergence Architectures for Broadband Access: Integration of EPON and WiMAX [Topics in Optical Communications],” *Communications Magazine, IEEE,* vol. 45, no. 8, pp. 44-50, 2007.

[71] "Dynamic Frequency Selection," http://www.ciscosystems.co.ck/en/US/docs/routers/access/wireless/software/guide/RadioChannelDFS.pdf.

[72] “Deploying License-Exempt WiMAX Solutions,” *Intel White Paper*, 2005. Available at : http://ecee.colorado.edu/~ecen4242/marko/WiMax/WiMax/WiMAXSolutions.pdf.

[73] Y. Kun, O. Shumao, K. Guild *et al.*, “Convergence of ethernet PON and IEEE 802.16 broadband access networks and its QoS-aware dynamic bandwidth allocation scheme,” *Selected Areas in Communications, IEEE Journal on,* vol. 27, no. 2, pp. 101-116, 2009.

[74] N. Ghazisaidi, M. Maier, and C. Assi, “Fiber-wireless (FiWi) access networks: a survey,” *Communications Magazine, IEEE,* vol. 47, no. 2, pp. 160-167, 2009.

[75] “Diameter Base Protocol,” *RFC 3588*, 2003.

[76] "The Internet Key Exchange (IKE)," *RFC 2409*, 1998.

[77] "Internet Key Exchange (IKEv2) Protocol," *RFC 4306*, 2005.

[78] "PPP Authentication Protocols," *RFC1334*, IETF, 1992.

[79] "PPP Challenge Handshake Authentication Protocol (CHAP)," *RFC 1994*, IETF, 1996.

[80] "Microsoft PPP CHAP Extensions," *RFC 2433*, IETF, 1998.

[81] "Omnilux, Inc.," www.omnilux.net.

[82] "Linux WPA/WPA2/IEEE 802.1X Supplicant," http://hostap.epitest.fi/wpa_supplicant/.

[83] "hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator," http://hostap.epitest.fi/hostapd/.

[84] "The FreeRADIUS Project," http://freeradius.org/.

[85] "The OpenSSL Project," http://www.openssl.org/.

[86] "The MD5 Message-Digest Algorithm," *RFC 1321*, 1992.

Appendix

List of Publications

Book Chapter

[1] **Wen Gu**, Stamatios V. Kartalopoulos, and Pramode K. Verma, “Security Architectures and Protocols in WLANs and B3G/4G Mobile Networks”, Chapter in: *Security and Privacy in Mobile and Wireless Networking*, Stefanos Gritzalis, Tom Karygiannis and Charalabos Skianis (Eds), Troubador Publishing Ltd, Leicester, UK, 2009.

Journal Papers

[1] **Wen Gu**, Pramode K. Verma and Stamatios V. Kartalopoulos, "A Unified Security Framework for WiMAX over EPON Access Networks," Security and Communication Networks, Wiley, July 1, 2010, doi: 10.1002/sec.204.

[2] **Wen Gu**, Stamatios V. Kartalopoulos, and Pramode K. Verma, "Fast and Secure Handover Schemes Based on Proposed WiMAX over EPON Network Security Architecture," WSEAS Transactions on Communications, issue 2, volume 9, 2010, pp. 115-126.

Conference Papers

[1] **Wen Gu**, Stamatios V. Kartalopoulos, and Pramode K. Verma, "Secure and Efficient Handover Schemes for WiMAX over EPON networks", Proceedings of the 4th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications, Cambridge, MA, USA, 2010, pp. 39-44.

[2] **Wen Gu**, Stamatios V. Kartalopoulos and Pramode K. Verma, "Performance Evaluation of EAP-based Authentication for Proposed Integrated Mobile WiMAX and FSO Access Networks," accepted by IEEE Wireless Communications and Networking Conference (WCNC), 2011, 28-31 March, 2011.