ABSTRACT

The IEEE 802.16 is the basis for Worldwide Interoperability for Microwave Access (WiMAX) certification which is the next evolution in wireless technology. The latest version of the standard, IEEE 802.16e addresses mobility and also enhances the security sub-layer of the IEEE 802.16 standard. However, security schemes in the standard are utilized and applied only to normal data traffic after the initial network entry process not to the control messages during the initial network entry. Security is a key challenge of WiMAX networks and it represents an important example of such scenarios where capturing and forging packets is relatively easy especially for unauthenticated and unencrypted messages during the initial network entry of both WiMAX modes: Point to Multi-Point (PMP), and Mesh. Therefore, the thesis proposes an innovative hybrid approach to resolve such vulnerability problem and establishes secret communication channels via insecure domains.

The proposed protocol is based on Bio Cryptosystem to improve current security level of authentication and Key Exchange between the Subscriber Station (SS), and the Base Station (BS). Novel proposed protocols are defined as the integration of Advanced Encryption Standard (AES) and Biometric Digital Key (BDK). The first is concerned with WiMAX PMP mode, to enhance the security issues in initial network entry mainly the Ranging Request and Response (RNG_REQ/RSP) messages. The second one is concerned about the WiMAX Mesh mode, to enhance security issues in the initial network entry mainly the Mesh Network Entry (MSH_NENT), in addition to solve the issue of the privacy between two nodes that the Mesh network faced. We derived a model of the protocols and implemented it using MATLAB and CASIA V.5 Database. Finally, the research proposed a permutation module using fuzzy scheme for biometric template protection.

ACKNOWLEDGMENT

First of all, my utmost thank should go to **ALLAH** (God) for His mercy, help and guidance, without which this document would not be made possible.

I would like to present my deepest gratitude to Professor Dr. **Salwa Hussein El-Ramly** for her humongous unconditional help, caring, valuable guidance and continuous support. She has generously devoted to me much of her knowledge and time and I deeply acknowledge her for that. I have learned so much from her rigorous research attitude, innovative thinking, and efficient work style. Professor Dr. **Salwa** inspired me a sense of enthusiasm, optimism and motivation. I am very lucky to have Professor Dr. **Salwa** as my supervisor. No words can express my appreciation to her. I will always be very grateful to her for my whole life.

I would like to express sincere appreciation to Professor Dr. **Ahmed Mustafa El-Sherbini** who has shown the courtesy of accepting to be my advisor in spite of his excessively busy schedule. I also owe her my gratitude for his invaluable support and guidance with his exceptionally modest attitude.

I want to extend my greatest gratitude to my esteemed advisor, Professor Dr. **Hesham Mohamed El-Badawy** the head of Network Planning Department, in National Telecommunication Institute for his great support, professional advice, and profound understanding. He offered me so many advices and guided me all the way through my graduate study. His engaging arguments and strong feedback have contributed greatly to this thesis. I was very fortunate to have him as my advisor. Without his valuable thoughts, recommendation and patience, I would have never been able to complete this work.

I would like to thank Mother, father, brothers and wife thank you very much for your sincere love. Without your continuous support and prayers this work would not have been accomplished. Now it is time to dedicate this work to you.

Chapter 1

Introduction

Chapter 2

WiMAX
Architecture and Security Challenges

Chapter 3

Bio-Cryptography

Chapter 4

Security Enhancement of PMP Topology

Chapter 5

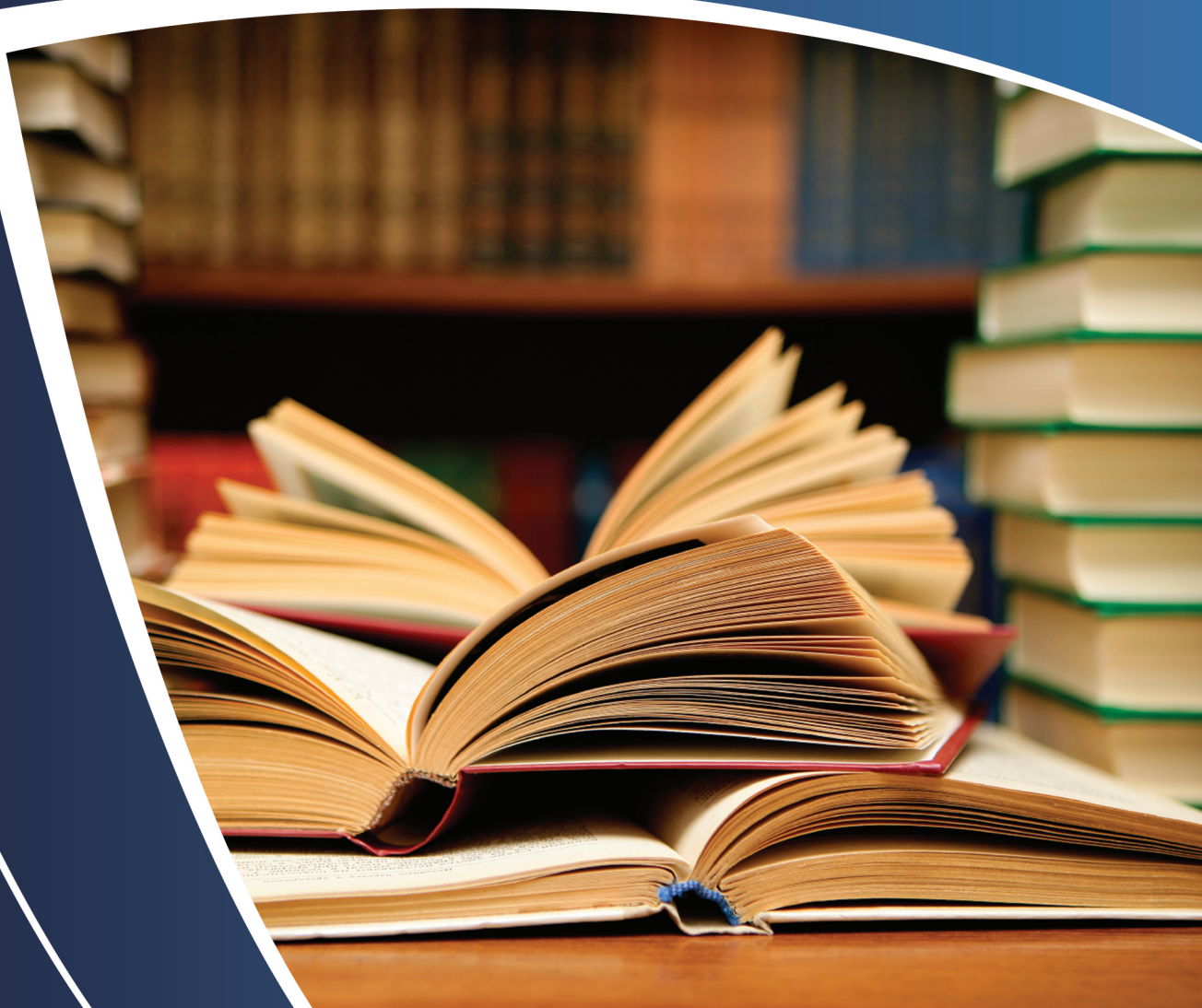
Security Enhancement of Mesh Topology

Chapter 6

Conclusion and future work

Extracted papers from the thesis

References



CHAPTER 1

INTRODUCTION

1.1 Introduction

Designing a secure Worldwide Interoperability for Microwave Access (WiMax) is a major research challenge that has been approached in many publications. There are various versions of IEEE standards while one of the main factors driving a new release of IEEE standard is to enhance its security features. Though, there are still several security vulnerabilities in MAC management messages in these standards [1],[2],[3],[4].

According to literature survey scarce studies discuss the security issues of messages in the initial network entry process. The initial network entry is the most vital process, as it is considered the foremost step to build network connection while carrying multiple parameters such as performance factors and security context between Base Station (BS) and Subscriber Station (SS) determined in the middle of this process.

However, security schemes are utilized and applied only to normal data traffic after the initial network entry process, but not to control messages during the initial network entry [3]. BS and SS communication in the initial network entry is susceptible to forgery. As a result, there can be various security vulnerabilities especially unauthenticated messages and unencrypted management communication that expose important management data [5]. Hence, it is an area worthy of interest due to this fact a tradeoff between security and effectiveness is being considered in this research through a new approach to enhance security of MAC management message during network entry initialization.

The research examined how cryptography principles and biometrics could be used jointly to provide authentication key distribution in addition to ensure data integrity, confidentiality, authentication, and non-repudiation.

The remaining of the chapter is organized as follows: Section 1.2 gives a general background about WiMAX technology, cryptography, and biometrics. Section 1.3 present evolutions of IEEE 802.16. Section 1.4 states the research area problems. Section 1.5 presents the thesis contribution. Finally, thesis organization is outlined.

1.2 General Background

The following sub-sections will provide a brief to the three major areas that are elementary in our research.

1.2.1 WiMAX

WiMAX technology is a wireless communications technology that is largely based on the wireless interface defined in the IEEE 802.16 standard [7]. The industry trade association, the WiMAX Forum, coined the WiMAX trademark and defines the scope of WiMAX technology through technical specifications and guide of securing WiMAX. The original purpose of IEEE 802.16 technology was to provide last mile broadband wireless access as an alternative to cable, digital subscriber line. Figure 1.1 show cases WiMAX network which can be used with different devices.

The IEEE amendment that enabled mobile WiMAX operations is IEEE 802.16e-2005. Prior to its release, deployment of WiMAX networks was limited to fixed operations by the IEEE 802.16-2004 standard. Additionally, IEEE 802.16e-2005 [8] provided significant security enhancements to its predecessor by incorporating more robust mutual authentication mechanisms, as well as support for Advanced Encryption Standard (AES). Although the IEEE 802.16-2004 and 802.16e-2005 standards were released within a year of each other, IEEE 802.16e-2005 product certification did not start until 2008, and IEEE 802.16-2004 products are still used in today's information technology (IT) environments [8]. in chapter 2 we will go into detail of WiMAX architecture and its security features.

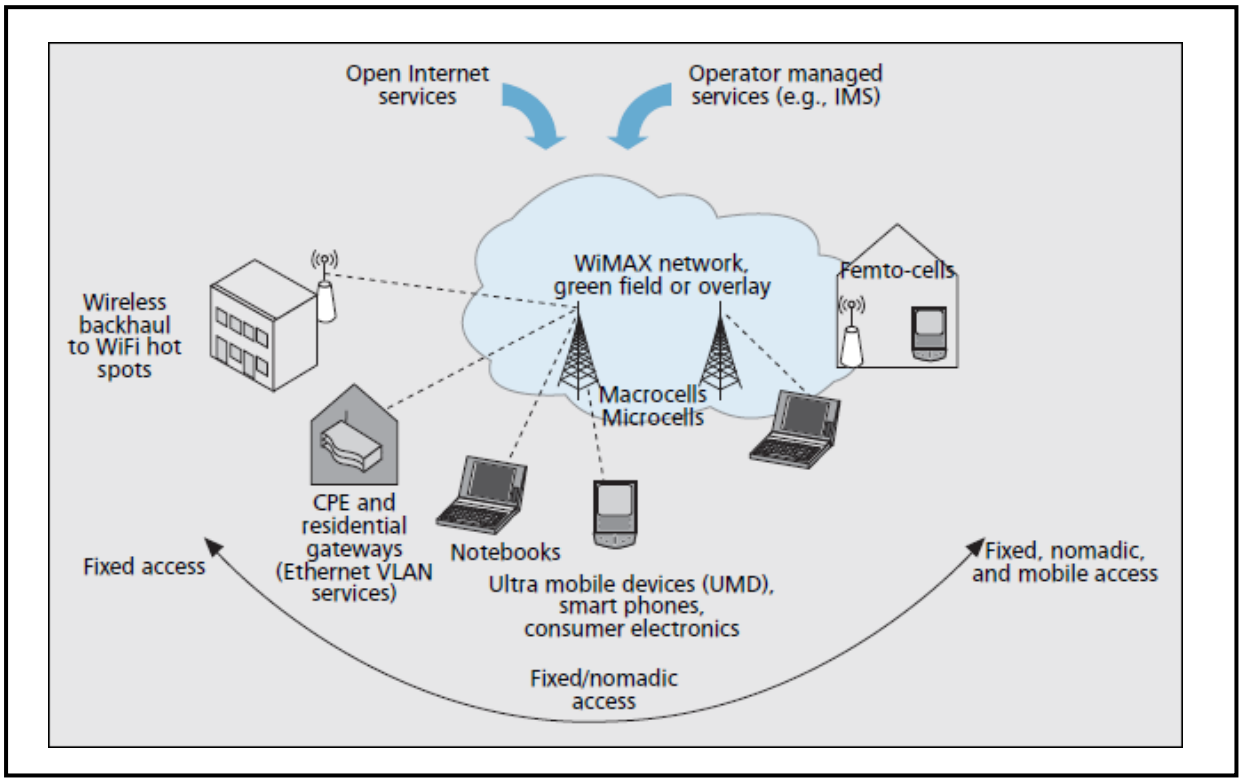


Figure 1.1: WiMAX Networks [9].

1.2.2 Cryptography

Cryptography is likely the most important part of communications security and is becoming increasingly substantial as a basic building block for computer security. Cryptographic mechanisms are one of the most robust ways to provide security services for electronic applications and protocols and for data storage. The national institute of standards and technology (NIST) [11] publish federal information processing standards (FIPS) and NIST recommendations that specify cryptographic techniques for protecting sensitive, unclassified information [10]. Cryptography is categorized in two forms of encryption which are commonly used: symmetric encryption and public key or asymmetric encryption. Eventually, the security of information protected by cryptography directly relies on the keys strength, the mechanisms effectiveness and protocols associated with keys, and the protection afforded to the keys.

The cryptographic protocols enable to set up secure communications on insecure networks by using cryptographic functions and shared secrets for authentication and confidentiality. Since there is a trade-off between performance and security, the symmetric-key cryptography is used for all data traffic, and public key cryptography is widely used for the authentication protocols themselves which aim to establish the session key [10].

1.2.3 Biometrics

Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic; a biometric is a measurable biological anatomical, physiological and behavioral characteristic that can be used for automated recognition [12].

Biometrics is being used in multiple locations for security enhancement; as the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming more evident [11]. Biometric-based authentication can offer non-repudiation and personal data privacy. The need for biometrics can be found in central and local governments, in the military, in commercial applications, and enterprise-wide network security infrastructures, government IDs, secure electronic banking [13].

Biometric-based authentication includes many applications such as, workstation access control, network security, and domain access, single sign-on; secure application logon, data protection, and remote access to resources, transaction security and internet security.

1.3 Evolution of IEEE 802.16 Standards

In October 2001, IEEE 802.16 standard was published. This defines the air interface and Medium Access Control (MAC) protocols for supplying Broadband Wireless Access in a metropolitan area network. This initial standard specifies the physical layer for frequencies 10 to 66 GHz. The main problem with this is that at such short wavelengths it is required to have a line of sight between BS and SS. This introduces difficult deployment issues. This issue was addressed in IEEE 802.16a standard, which was published in January 2003; it introduced provision for the physical layer to operate in the 2 to 11 GHz band. This, together with Orthogonal Frequency Division Multiple (OFDM) technology and sub-channelization allows for Non-Line of Sight (NLOS) and operation. Following this, the 802.16-2004 standard was released [7], [3] which was basically an integration of 802.16 and 802.16a. The 802.16e standard builds on the previous ones and introduces support for mobile subscriber stations traveling at vehicular speeds [8]. As such, it specifies necessary amendments in MAC and PHY layers to allow for this. The research was concerned with MAC layer frames to evaluate the security enhancement during the network entry process.

1.4 Research Problems Area

The research examines vulnerable security elements that MAC management messages in WiMAX initial network entry face in both modes point to multipoint (PMP) and Mesh topologies.
The main problems tackled in this thesis are addressed as follow:

- The vulnerabilities on ranging request/response (RNG_REQ, and RNG-RSP) messages.
- Mesh network entry request message (MSH_NENT: Request) is not encrypted or authenticated, which could lead to several attacks against network topology.
- Privacy among nodes as operator shared secret (OSS) is shared across all nodes.
- The link establishment between SS with its neighbors follows a Challenge-Response message based on OSS of the network which could lead to threats, as its security depends on OSS, which leads to link establishment.