A survey of WiMAX security threats

Trung Nguyen, nguyent@seas.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

Abstract:

As a promising broadband wireless technology, WiMAX has many salient advantages over such as: high data rates, quality of service, scalability, security, and mobility. Many sophisticated authentication and encryption techniques have been embedded into WiMAX but it still exposes to various attacks in. This report is a survey of security vulnerabilities found in WiMAX network. Vulnerabilities and threats associated with both layers in WiMAX (physical and MAC layers) are discussed along with possible solutions.

Keywords:

IEEE 802.16, WiMAX, wireless network, threat analysis, vulnerabilities analysis, security, network security, PKM, PKMv2, authentication, encryption, man-in-the-middle attacks, DoS attacks, WiMAX attacks.

Table of Contents

1. Introduction

Established by IEEE Standards Board in 1999, the IEEE 802.16 is a working group on Broad Wireless Access

(BWA) developing standards for the global deployment of broadband Wireless Metropolitan Area Networks [Wiki_802.16]. In December 2001, the first 802.16 standard which was designed to specialize point-to-multipoint broadband wireless transmission in the 10-66 GHz spectrum with only a light-of-sight (LOS) capability. But with the lack of support for non-line-of-sight (NLOS) operation, this standard is not suitable for lower frequency applications. Therefore in 2003, the IEEE 802.16a standard was published to accommodate this requirement. Then, after being revised several times, the standard was ended in the final standard: 802.16-2004 which corresponds to revision D. These standards define the BWA for stationary and nomadic use which means that end devices cannot move between base stations (BS) but they can enter the network at different locations. In 2005, an amendment to 802.14-2004, the IEEE 802.16e was released to address the mobility which enable mobile stations (MB) to handover between BSs while communicating. This standard is often called "Mobile WiMAX7#8221;. The following table provides a summary of the IEEE 802.16 family of standards.

Standard	802.16	802.16a/802.16REVd	802.16e
Spectrum	10 to 66 GHz	< 11 GHz	< 6 GHz
Channel Conditions	Line-of-Sight only	None-Line-of-Sight	Non-Line-of-Sight
Speed (bit rate)	32 to 134 Mbps	75 Mbps max, 20-MHz channelization	15 Mbps max, 5-MHz channelization
Modulation	QPSK 16QAM 64QAM	OFDM 256 subcarrier QPSK 16QAM 64QAM	same as 802.16a
Mobility	Fixed	Fixed	Pedestrian mobility, regional roaming
Channel Bandwidths	20, 25 and 28 MHz	Selectable between 1.25 and 20 MHz	same as 802.16a with sub-channels
Typical Cell Radius	1 – 3 miles	3-5 miles (up to 30 miles, depending on tower height, antenna gain and transmit power)	1-3 miles

Table 1. Summary of the IEEE 802.16 family of standards.

Based on the IEEE 802.16 standard, the WiMAX (Worldwide Inter-operability for Microwave Access) is "a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access"[Wiki_WiMAX]. The WiMAX is supported by the WiMAX forum, which is a non-profit organization formed to promote the adoption of WiMAX compatible products and services [WiMAXABT]. WiMAX is a very promising technology with many key features over other wireless technologies [Jain08]. For instance, WiMAX network has the capability of working on many bands: 2.3 GHz, 2.5 GHz, etc, and provides scalability and mobility with high data rates with NLOS operation. It also provides strong security and strong QoS guaranteed services for data, voice, video, etc. However, in order for WiMAX to achieve a maturity level and become a successful technology, more research on security threats and solution to these threats need to be conducted.

This report is organized as follows. In section 2, WiMAX protocol architecture and security solutions are presented to provide background and detailed information about WiMAX securities specifications in the security sub-layer. Then vulnerabilities in WiMAX security will be discussed in section 3. In this section, some possible threats or vulnerabilities are discussed along with some proposed solutions to them. Finally, section 4 concludes the report.

---

2. WiMAX: protocol architecture and security solutions

In order to understand WiMAX security issues, we first need to understand WiMAX architecture and how securities specifications are addressed in WiMAX. This section provides background and detailed information about WiMAX securities specifications in the security sub-layer.

2.1. IEEE 802.16 protocol architecture:

The IEEE 802.16 protocol architecture is structured into two main layers: the Medium Access Control (MAC) layer and the Physical (PHY) layer, as described in the following table [Jain08]:

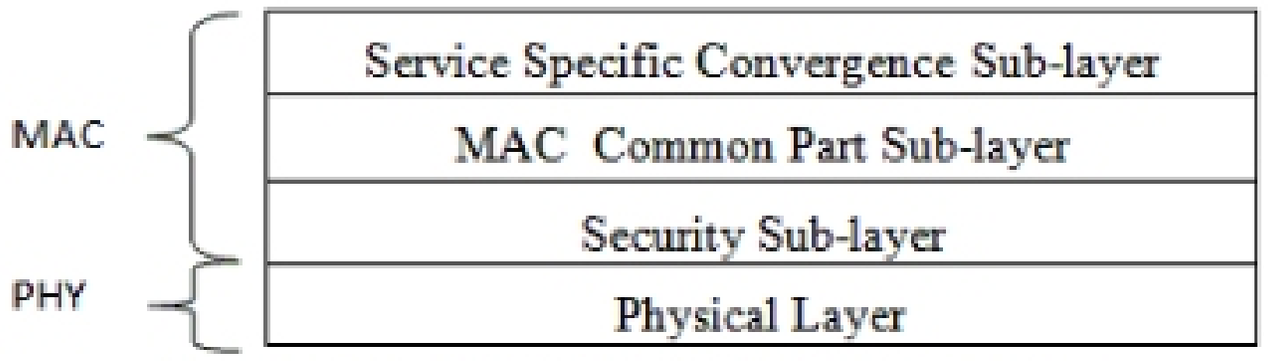

Figure 1. The IEEE 802.16 Protocol structure

MAC layer consists of three sub-layers. The first sub-layer is the Service Specific Convergence Sub-layer (CS), which maps higher level data services to MAC layer service flow and connections [Elleithy08]. The second sub-layer is Common Part Sub-layer (CPS), which is the core of the standard and is tightly integrated with the security sub-layer. This layer defines the rules and mechanisms for system access, bandwidth allocation and connection management. The MAC protocol data units are constructed in this sub-layer. The last sub-layer of MAC layer is the Security Sub-layer which lies between the MAC CPS and the PHY layer, addressing the authentication, key establishment and exchange, encryption and decryption of data exchanged between MAC and PHY layers.

The PHY layer provides a two-way mapping between MAC protocol data units and the PHY layer frames received and transmitted through coding and modulation of radio frequency signals.

2.2. WiMAX security solutions:

By adopting the best technologies available today, the WiMAX, based on the IEEE 802.16e standard, provides strong support for authentication, key management, encryption and decryption, control and management of plain text protection and security protocol optimization. In WiMAX, most of security issues are addressed and handled in the MAC security sub-layer as described in the following figure:

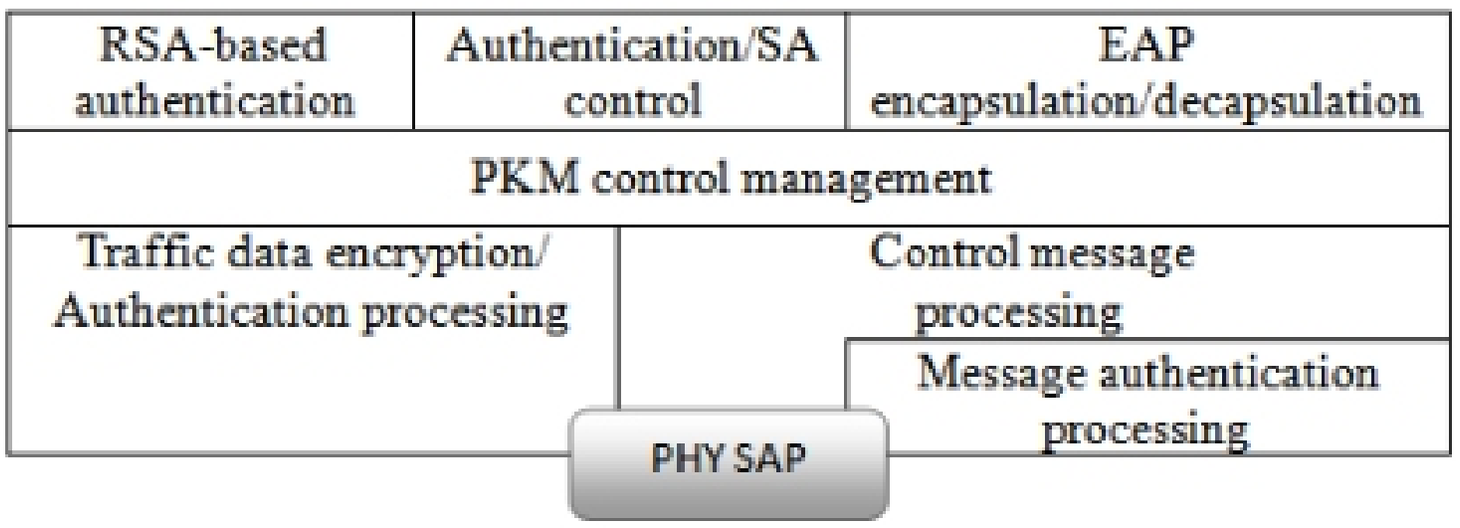

Figure 2 . MAC Security sub-layer

Two main entities in WiMAX, including Base Station (BS) and Subscriber Station (SS), are protected by the