Chapter 2
Security in Wireless Metropolitan Area Networks: WiMAX and LTE

Lei Chen
Sam Houston State University, USA

Cihan Varol
Sam Houston State University, USA

Qingzhong Liu
Sam Houston State University, USA

Bing Zhou
Sam Houston State University, USA

ABSTRACT

Thanks to the much larger geographical coverage and pleasing bandwidth of data transmissions, Wireless Metropolitan Area Networks (WMANs) have become widely accepted in many countries for everyday communications. Two of the main wireless technologies used in WMANs, the Worldwide Interoperability for Microwave Access (WiMAX, also known as Wireless Local Loop or WLL) and Long Term Evolution (LTE), have generated billions of dollars in the ever-growing wireless communication market. While the IEEE 802.16 standards for WiMAX and the 3GPP standards LTE are updated and improved almost annually, it is inevitable that current standards still contain a number of security vulnerabilities, potentially leading to various security attacks. To address the security concerns in these two WMANs technologies, this chapter presents the technical details of security aspects of WiMAX and LTE. More specifically, the key generation, authentication, data, and key confidentiality and integrity of both technologies are deliberated. The chapter ends with a discussion of the security vulnerabilities, threats, and countermeasures of WiMAX and LTE.

DOI: 10.4018/978-1-4666-4691-9.ch002

1. INTRODUCTION

A Metropolitan Area Network (MAN) can be described as a communication network that spreads over one or multiple adjacent neighboring cities and geographical areas (Ghosh, Wolter, Andrews, and Chen, 2005; MAN, 2009). The purpose of MANs is to enable an efficient transportation of data-oriented traffic in a much larger geographical area compared to Wireless Local Area Networks (WLANs) (WiMAX, n.d.; LTE, n.d.). Scalability is a main challenge in such a network that covers a relatively large range. Conventional wireless technologies would not survive in such situation when trying to meet the high capacity demands from nowadays users. As an example, researchers at Sprint's Applied Research & Advanced Technology Labs (AR&ATL) have proposed a next-generation, high-capacity metropolitan area network under their HORNET project that is designed to achieve cost-effective scaling using hybrid optoelectronic ring network (White, Rogge, Shrikhande, and Kazoysky, 2003).

A Local Area Network (or simply LAN), according to the IEEE 802-2002 standard (IEEE L/M SC, 2002), is generally owned and operated by a single organization whereas a MAN is usually designed to be used by more than one individuals and organizations, and sometimes also as public utilities. A variety of applications and services, such as file transfer, graphics, text and data processing, emails, database access and multimedia, are supported by both LANs and MANs. What makes a LAN and a MAN different mainly is the geographic regions covered: 0-2 miles for a typically LAN, and 2-30 miles for MANs. Both types of networks make used of a variety of network technologies, e.g. Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI), Switched Multi-megabit Data Service (SMDS) and linked together using microwave, radio, infra-red or Ethernet-based connections. Some common examples of MANs can be found in large cities where the fire stations and emergency responder networks are interlinked across jurisdictions. Media companies such as newspapers, cable networks employ metro networks to coordinate their activities across different branch offices. In the next few sections, we will have a discussion of the basics and security aspects of two dominant WMAN technologies: WiMAX and LTE.

2. FUNDAMENTALS OF WIMAX AND LTE

WiMAX and LTE are the two most widely accepted and applied MAN technologies. WiMAX can provide up to 70 mbps of bandwidth over a radius of several miles (WiMAX, n.d.), and is a true 4G technology being used by consumers in over 150 countries and gaining acceptance in several industries. The WiMAX Forum is an industry-led, not-for-profit organization that certifies and promotes the compatibility and interoperability of broadband wireless products based on the IEEE 802.16 Standards. Its competitor LTE, based on the GSM/EDGE and UMTS/HSPA network technologies, as specified in the 3rd Generation Partnership Project (3GPP) Release 8 and 9 document series, was not originally considered as a true 4G technology, but was later decided by the International Telecommunication Union (ITU) and introduced, for marketing purpose, by major service providers such as Verizon Wireless as a 4G technology. LTE supports cell sizes from tens of meters to up to 62 miles with peak download rates up to 300 mbps and upload rates up to 70 mbps (LTE, n.d.).

In the rest of this section, we will examine the fundamentals of WiMAX, the IEEE 802.16 Standard, and LTE. The IEEE 802.16 working group was formed to address the projected increase in the demand for metropolitan and wide-area wireless internet access over the next few years. This working group has put forth a standard for Broadband Wireless Access (BWA) systems, namely the IEEE 802.16 Standards. In this section