Chapter 11
A Survey of High Performance Cryptography Algorithms for WiMAX Applications Using SDR

Rafidah Ahmad
Universiti Sains Malaysia, Malaysia

Widad Ismail
Universiti Sains Malaysia, Malaysia

ABSTRACT

As wireless broadband technology has become very popular, the introduction of Worldwide Interoperability for Microwave Access (WiMAX) based on IEEE 802.16 standard has increased the demand for wireless broadband access in the fixed and the mobile devices. This development makes wireless security a very serious concern. Even though the Advanced Encryption Standard (AES) has been popularly used for protection in WiMAX applications, still WiMAX is exposed to various classes of wireless attack, such as interception, fabrication, modification, and reply attacks. The complexity of AES also produces high power consumption, long processing time, and large memory. Hence, an alternative cryptography algorithm that has a lower power consumption, faster and smaller memory, is studied to replace the existing AES. A Software Defined Radio (SDR) is proposed as a different way of proving the performance of the cryptography algorithm in real environments because it can be reprogrammed, which leads to design cost and time reductions.

INTRODUCTION

Cryptography is known as the science of using mathematics to encrypt and decrypt data. With cryptography, it enables users to store sensitive information or transmit it across insecure networks such as Internet. The information can only be read by the intended recipient. There are many types of cryptography algorithm which had been evaluated in the recent research works. These algorithms will be studied and analyzed in the literature review, in terms of battery power consumption, memory, and speed for mobile Worldwide Interoperability for Microwave Access (WiMAX).

DOI: 10.4018/978-1-4666-2812-0.ch011

As for WiMAX, it is a Wireless Metropolitan Area Network (WMAN) communications technology that is largely based on the wireless interface defined in IEEE 802.16 standard (Scarfone, et al., 2010). Nowadays, WiMAX is gaining popularity in many regions due to wide coverage and high data rate of multimedia transmission rather than WiFi which has a coverage and speed limitations. A new validation approach for WiMAX communication using Software Defined Radio (SDR) is proposed in this chapter.

SDR is an Information Transfer System (ITS) that combines technologies from historically separated fields of computers and radios (Xu, et al., 2006). Emerging from military applications, SDR has gained much attention among researchers and practitioners working in the wireless communication area. SDR technique has been considered as an important technique to enhance the flexibility and usability of many popular communication standards such as GSM, WiFi and 3G. Since WiMAX has never been verified through SDR platform, this can be one of new method to proof the SDR capability. An overview about WiMAX and SDR are presented in the next section, followed by a survey on cryptography algorithms and SDR implementations in the literature review.

BACKGROUND

WiMAX is used for variety of purposes including, but not limited to, fixed last-mile broadband access, long-range wireless backhaul, and access layer technology for mobile wireless subscribers operating on telecommunications networks (Scarfone, et al., 2010). The WiMAX Forum has estimated that new WiMAX equipment will be capable of sending 40 Mbps data over 10 km in a Line-Of-Sight (LOS) fixed environment (Khan & Zaman, 2009). Therefore, WiMAX technology continues to adapt to market demands and provide enhanced user mobility. IEEE 802.16e-2005 was an amendment that enabled mobile WiMAX. This standard was built on Orthogonal Frequency Division Multiple Access (OFDMA). Most countries have allocated the bands for the wireless access between 3.4 and 3.6 GHz but the United States, Mexico, Brazil, and some Southeast Asian nations, have chosen instead the bands between 2.5 and 2.7 GHz (Ahson & Ilyas, 2008).

The mobile WiMAX system also has more enhanced security features than the existing IEEE 802.16-2004-based WiMAX network system. However, the mobile WiMAX system, which uses Advanced Encryption Standard (AES) scheme (Airspan, 2007; Yuksel, 2007), is still not able to guarantee the reliability of the whole mobile WiMAX systems and network architecture (Joseph, 2011). In this short period of their existence, various weaknesses have emerged. Some of the possible threats are similar to the ones that WiFi faced: this observation stresses on the importance of the WiFi threat analysis and the prevention measures that can be taken for WiMAX (Trimintzios & Georgiou, 2010). WiMAX has security vulnerabilities in both Physical (PHY) and Medium Access Control (MAC) layer, exposing to various classes of wireless attack including interception, fabrication, modification, and reply attacks (Jha & Dalal, 2010).

As in MAC layer, the threats are examined with respect to confidentiality and authentication. As shown in Figure 1(a) based on Mishra and Glore (2008), a MAC layer Protocol Data Unit (PDU) consists of a MAC header, a payload and an optional CRC. The payload may consist of user traffic or management messages. MAC headers are not encrypted and all MAC management messages shall be sent in without protection. Therefore, MAC layer is exposed to eavesdropping, man in the middle and Denial of Service (DoS) attacks. Eavesdropping of management messages may reveal network topology to the eavesdropper, posing a critical threat to Sub-Stations (SSs) as well as the WiMAX system (Ahson & Ilyas, 2008). Weaknesses in management messages authentication also open the door to aggressions