International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 30, Issue 01) and (Publishing Month: May 2016)
(An Indexed, Referred and Impact Factor Journal)
ISSN: 2319-6564
www.ijesonline.com

Security Issues of WiMax

Mazin Mohammed Hamza Altaieb[1] and Dr Hala Eldaw Idris[2]

[1,2]Faculty of Engineering, Al-Neelain University, Khartoum, Sudan

Publishing Date: May 31, 2016

Abstract

Security has become a principal concern to supply protected communication in Wireless environment. We know the basic idea of communication is directed the knowledge from source client to destination node but in my view the communication is not delivered the information but the amount of secure information which is sent from source node to destination node. The much awaited technology for wireless high speed access, the WiMAX (Wireless Interoperability for Microwave Access) is finally starting to be available in the market with the target to provide high data rates and provide interoperability of vendor devices simultaneously. In this report we give a review on the several performance evaluations which may have recently been conducted on WiMAX systems and show the existing functions and future trends in the WiMAX technology. Intended for a broadband wireless standard such as WiMax, security is important and must be addressed. This is to ensure wide acknowledgement both from the point of view of the finish users and the companies. In order to compete with existing broadband cable or DSL services, the WiMax network must offer comparable security. We discuss the WiMax security mechanisms for authentication, encryption, and availability. All of us also discuss potential threats to WiMax security. This paper will also discuss how and why these threats play an important role in the elasticity of WiMax.

Keyword*: WiMax, WiMax Security, Encryption, Security, Potential Threats.*

1. Introduction

Together with the introduction of Wireless LANs in the 90s network security became a very important subject of debate among major corporations, service providers, and end users. Security in wireless systems is the maintaining of confidentiality, authentication, non-repudiation, and integrity control [1]. To hold these four areas protected from malevolent attacks, certain protocols were put into place. These types of protocols are constantly being tested and improved as required to keep companies protected from outside, and sometimes inside users. These kinds of protocols are also being employed by home users as more wireless networks are being brought into the homes of end users. Worldwide Interoperability for Micro wave Access (WiMax) is explained as "a standards structured technology enabling the delivery of last mile Wi-Fi broadband access as an alternative to cable and DSL" [2]. WiMax provides many services using point out point and point to multipoint applications. These types of applications are cost effective and cover a much larger area than Wi-Fi (IEEE 802. 11). WiMax uses a base stop to transmit to Consumer Premise Equipment (CPE). Employing a base station allows WiMax to work with applications for fixed, lightweight, or mobile non-line-of-sight services. With this technology WiMax is able to cover an entire city, not simply a coffee shop or office building As stated, network security is important. In order for WiMax to be an accepted wireless service it should meet or exceed the standards already in position. This kind of is especially important for WiMax as it could cover such large areas. Any defects in the safety and hackers would be able to burglary, or there could be interference in one computer to another. Once Wi-Fi was performed the protocols for network security were developed. The first step for wireless security was Wired Equivalent Level of privacy (WEP) [3]. While more flaws were found more protocols were developed. To ameliorate key management and initialization WEP 2 was developed. Unfortunately, this did not include the answer to all the problems wireless security was faced with. Eventually, cordless security evolved to incorporate many different protocols and encryptions that are being used in Wireless today. The lessons discovered with Wi-Fi security flagged the right way to the security actions used for WiMax. WiMax uses Counter Mode with Cipher Block Chaining Concept Authentication Code Protocol (CCMP) to encrypt all traffic on its network. That also uses Advanced Security Standard (AES) to deliver data securely. Both of these are being used in Wi-Fi today and are strong in encryption and key

management. Another protocol developed during the look for network security in Wi-Fi and now used in WiMax, was PKM-EAP (Extensible Authentication Protocol). This protocol can be used for end-to-end authentication. WiMax has profited from the lessons learned with Wi-Fi, but there are still threats and vulnerabilities to be dealt with. The rest of the newspaper is organized as employs. WiMax Security standards are discussed in Section 2, Section 3 discusses mobile wireless WiMax Security Structure, and Section 4 reviewed threats to WiMax, Findings are classified by Section 5.

2. WiMax Security Standards

The Protocol Stack used for WiMax is comparable to that used for Wi-Fi. The structure is the same, but WiMax uses more sublayers. The standards for WiMax Security are also similar. These standards are discussed in the following sections.

2.1. Data Link Layer Security

The Data Link Layer for WiMax has three sublayers. Privacy and security is handled in the bottom layer. The MAC sublayer is next, which implements secure key exchange and encrypts traffic. The last sublayer is the Service-Specific Convergence sublayer. Figure 1 shows the Protocol structure for WiMax. The WiMax MAC layer uses a scheduling algorithm opposed to contention access used in the Wi-Fi MAC layer. For the initial entry into the network, the scheduling algorithm attempts only once from the Subscriber Station (SS) and then it is appropriated an access slot by the Base Station (BS). This access slot cannot be used by other subscribers, while assigned to the SS. To ensure confidentiality the MAC layer uses electronic signatures to authenticate the user and the device.

2.2. Authentication

One of the main problems that Wi-Fi faced when first launched was authentication. Since this posed huge security issues, a better standard for authentication was used for WiMax. The WiMax network uses a Privacy Key Management (PKM) protocol for Authentication. This dynamic system makes it harder for hackers to act as a legitimate subscriber [4]. This style of authentication gives three types of protocols, a RSA based authentication, which uses a X.509 certificate with RSA encryption. An EAP based authentication, which also has three types of protocols to choose from. These three types are AKA (Authentication and Key Agreement) for SIM based authentication, TLS for X.509 based authentication, and TTLS for MS-CHAPV2 (Microsoft-Challenge Handshake Authentication Protocol). The third type of PKM protocol is RSA based authentication followed by EAP authentication [5].

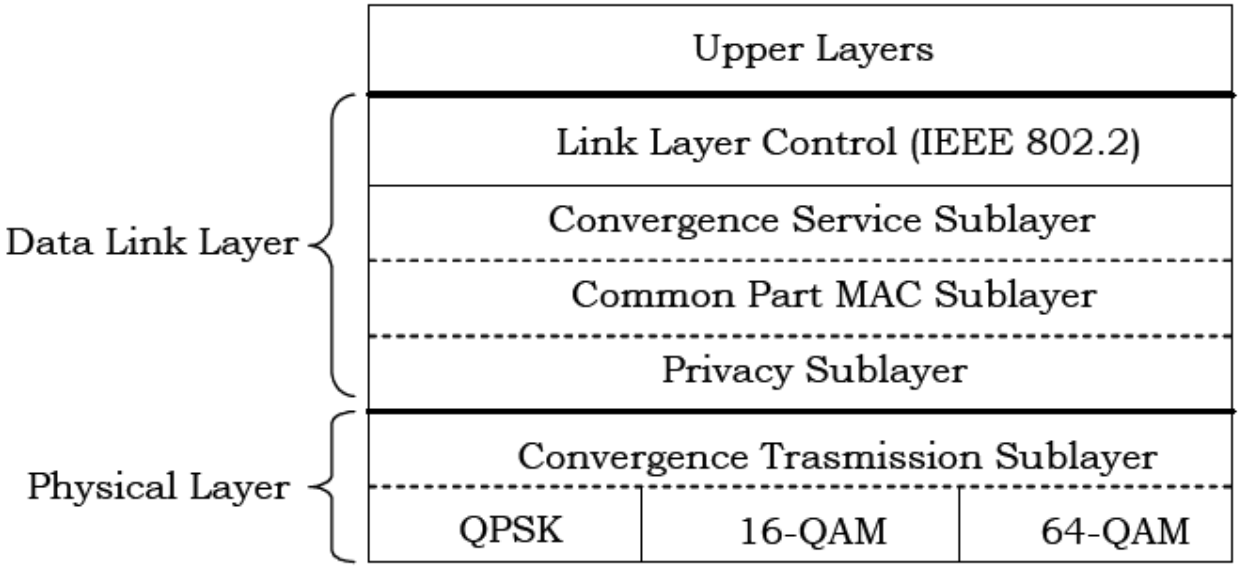

Figure 1: The IEEE 802.16 Protocol Structure

2.3. Authorization

Authorization works hand in hand with authentication when it comes to security for WiMax. In order for a user to receive authorization, the authentication protocols must be met. Immediately following the authentication process, the SS sends an Authorization Request message to the BS [5]. In return an Authorization Reply message is sent back to the SS with the Authorization Key (AK) encrypted in the SS's public key along with the Security Association ID (SAID) of more Security Associations (SA) the SS is authorized to participate with. A lifetime key is also included with this reply. After the initial Authorization the BS periodically re-authorizes the SS.

2.4. Encryption

WiMax uses 3DES and AES to encrypt data transported on the network. The Triple Data Encryption Standard (3DES) uses three different keys with a length of 56-bit each. The use of three keys causes for a slower performance in some software. The slow performance and limit on the length of keys is slowly making 3DES obsolete. The main tool for encryption that is used by WiMax is the Advanced Encryption Standard (AES) [6]. AES provides support for 128-bit, 192-bit, or 256-bit encryption keys [4]. AES was built from CCMP and has become a popular algorithm. AES is faster than 3DES, easy to performed and uses very little memory. However, it does require dedicated processors on board the BS, and may not be used by all end-user terminals. Therefore, 3DES remains a vital encryption tool on the WiMax network.

2.5. Availability

WiMax uses Radio Frequency (RF) Spectrum and could function on any frequency below 66 GHz [2]. The highest frequency available in the USA is 2.5 GHz. One of the drawbacks for using RF Spectrum is that the higher the frequency the range of a BS decreases a few hundred meters. Analog TV bands may be available for WiMax use once the rollout of digital TV is complete in February of 2009.

3. Mobile Wireless WiMax Security Architecture

The WiMax Security Architecture is flexible to allow Base Stations of different sizes and Subscriber Stations of different functionality. It also follows the standard end-to-end architecture for the Network Reference Model (NRM). The network is divided into two major parts, Access Service Network (ASN) and the Connectivity Service Network (CSN). The ASN control and monitors the traffic between the Base Stations and the ASN Gateways. It also maintains the authentication and the key distributions. There are three ASN profiles, A, B, and C. Profiles A and C implements Radio Resource Management (RRM) and Handover functions, using a centralized ASN Gateway. These functions are used in the BS. Profile B embeds the key inside the BS. This eliminates the need for a centralized ASN Gateway. CSN controls the ASNs and end users with services such as AAA, Home Agent Functions, and DHCP Server. CSN also connects to operator's networks and enables inter-operator and inter-technology roaming.

4. WiMax Threats

Many of the security threats found in WiMax have been addressed. These are issues that were found with the deployment of Wi-Fi. This gives WiMax an advantage. If all, or at least most of the security issues can be addressed before WiMax's mainstream deployment, it will make it a more accepted network than Wi-Fi. This section of the paper will discuss the known security threats in WiMax. These include: DoS attacks, Network manipulation with spoofed management frames, Rogue base stations, Man-in-the-middle attacks, and threats in the physical layer.

4.1. DoS Attacks

Denial of Service (DoS) attacks is defined as an attempt to make a computer resource unavailable to its intended users [8]. Hackers usually use this kind of attack on web servers for banks, credit card payment gateways or DNS root servers. A DoS attack uses the IP address to flood the user's network and obstruct communication between the intended user and the victim. This type of attack is not preventable; however steps can be taken to quickly resolve the attack. Some firewalls have built-in protection from DoS attacks, that monitor the amounts of packets

received and the time frame they were received. It has been proposed that a Shared Authentication Information (SAI) protocol could be used to offer a defense mechanism against DoS attacks, without incurring overhead at the ASN gateway and base station. This proposal uses the unused upper 64-bit of the 128-bit Cipher Based Message Authentication Code (CMAC) to calculate a CMAC key [9]. This proposal could be the answer to prevention of DoS threats.

4.2. Network Manipulation with Spoofed Management Frames

The management frames in WiMax are comparable to WiFi's. When WiFi was first deployed vulnerabilities were found in the management frames that allowed DoS attacks by disrupting the wireless session between two nodes. WiMax has cryptographic protections from spoofed identities, but that does not mean it is safe. Replay DoS attacks still remain a threat to WiMax, due to the lack of any mechanisms to specifically detect and discard repeated packets [12].

4.3. Rogue Base Stations

A Rogue Base Station is defined as an attacker station that imitates a legitimate base station [7]. This kind of attack results in disruptions in service and allows hackers to confuse subscribers. This is more difficult, but not impossible to do in the WiMax network. WiMax uses time division multiple access, therefore the rogue base station must transmit with a stronger strength at the same time the legitimate station transmits. The rogue base station captures the legitimate base station's identity and uses it to authenticate with the subscriber station. The authentication protocols used in WiMax help mitigate this threat. WiMax uses the EAP Protocol as its main protocol for authentication. This protocol forces mutual authentication, therefore the subscriber station would send an authentication message to the rogue base station. This does not completely alleviate the threat of rogue base stations, but it does make it more difficult.

4.4. Man-in-the-Middle Attacks

Man-in-the-Middle attacks are forms of eavesdropping. The hacker establishes separate connections between two victims and relays the messages between them [10]. The hacker intercepts the public key from one of the victims and sends his or her own public key to the intended victim. When that victim responds the hacker then has that public key. The use of the RF Spectrum in WiMax allows for vulnerabilities to the man-in-the-middle attack. However, WiMax uses a three-way handshake scheme that supports re-authentication mechanisms for fast handovers to prevent man-in-the-middle attacks [11]. If the base station is constantly changed the public key changes making it almost impossible for hackers to eavesdrop using public keys.

4.5. Threats in the Physical Layer

Blocking and rushing are the major threats located in the physical layer. Blocking or jamming activates a strong frequency to lower the capacity of the channel creating a DoS to all stations. This threat is detectable with a radio analyzer device. This device does not block this threat, but it alerts the end-user so that steps can be taken to immediately recover. Rushing or scrambling is another type of jamming, but it only activates for short periods of time and only affects certain frames. Jamming can be prevented using an increased signal or using frequency hopping. Control or Management messages are not in danger of rushing or blocking. Scrambling the uplink slots is too difficult for hackers [13].

5. Conclusions

WiMax security has been reviewed in this paper. The teachings learned with WiFi's deployment have given WiMax a benefit in providing a safer wireless network. The provision taken with WiMax were not done for WiFi. These security procedures were not taken at WiFi's launch because the threats were unknown. Presented that the threats are known and understood, they have been addressed before to WiMax's deployment. On the other hand, this does not indicate that WiMax is perfect there may be new threats that are unidentified and will not be addressed until WiMax is launched. WiMax does have much potential. WiMax would allow customers a totally cable free network connection in their homes or businesses. WiMax would can provide better services for mobile cell phones. There are also some valuation for WiMax to be used in video gaming consoles. While security is an important subject and was obviously a main cause of delay in the first stages of

development for WiMax, it includes now been faced with technological down falls.

References

[1] A. S. Tanenbaum, "Computer Networks," 4th Edition, Prentice Hall, Inc., New Jersey, 2006.
[2] http://en.wikipedia.org/wiki/WiMax
[3] S. P. Ahuja and P. K. Potti, "Evolution of Wireless LAN Security," International Conference on Parallel and Distributed Processing Techniques and Applications, Las Vegas, 24-17 July 2008.
[4] T. Sanders, "Premium Five Essential Elements of WiMax Security," WiMax.com, November 2007.
[5] http://myhsc.pbwiki.com/wimax::aaa
[6] P. Korsenlowski, "Staying Safe in a WiMax World," TechNewsWorld.com, 27 February 2007.
[7] M. Barbeau, J. Hall and E. Kranakis, "Detecting Impersonation Attacks in Future Wireless and Mobile Networks," Secure Mobile Ad-hoc Networks and Sensors, Ottawa, 2006, pp. 80-95.
[8] M. McDowell, "Understanding Denial of Service Attacks," National Cyber Alert System, 1 August 2007.
[9] K. Youngwook, L. Hyoung-Kyu and B. Saewoong, "Shared Authentication Information for Preventing DDoS Attacks in Mobile WiMax Networks," Proceedings of the 5th Consumer Communications and Networking Conference, Las Vegas, 10-12 January 2008.
[10] N. Beacham, "Man in the Middle (MITM) Attacks," Technology and More, 28 June 2008.
[11] J. M. Hartley, "WiFi and WiMax Protocols of Security," December 2008. http://softwarecommunity.intel.com/articles/eng/3708.html.
[12] R. Millman, "Security Experts See Vulnerablilites in WiMax," WiMax.com, 17 October 2006.
[13] M. Barbeau, "Threats: Threats to WiMax," http://www. freewimaxinfo.com/physical-layer.html.