IEEE 802.16 Security Issues: A Survey

Mitko Bogdanoski, Pero Latkoski, Aleksandar Risteski, Borislav Popovski
Faculty of Electrical Engineering and Information Technologies
Ss. Cyril and Methodius University
Skopje, Macedonia
mitko.bogdanoski@gmail.com, {pero, acerist, borop}@feit.ukim.edu.mk

***Abstract* — This paper reviews the fundamentals and security issues of WiMAX networks addressed in relevant standards and several papers. At first a global overview of the WiMAX technology is provided followed by a security concerns and problems associated to the WiMAX/IEEE 802.16 broadband wireless technology. Then an explanation of security vulnerabilities and threats mentioned in the available literature is presented along with possible solutions.**

***Keywords* — IEEE 802.16, WiMAX, security, authentication, PKM, PKMv2, threats, vulnerabilities**

I. Introduction

WiMax (Worldwide Interoperability of Microwave Access), also known as the IEEE 802.16 protocol, is the latest standard for wireless networks. It was established in 1999 to prepare specifications for broadband wireless metropolitan area networks. The first 802.16 standard was approved in December 2001 and was followed by three amendments: 802.16a, 802.16b and 802.16c. In 2004 the 802.16-2004 standard (IEEE-SA, 2006) was released and the earlier 802.16 documents including the a/b/c amendments were withdrawn. An amendment to 802.16-2004, IEEE 802.16e-2005 (formerly known as IEEE 802.16e), addressing mobility, was concluded in 2005. This implemented a number of enhancements to 802.16-2004, including better support for Quality of Service, Security and the use of Scalable OFDMA, and is sometimes called "Mobile WiMAX", after the WIMAX forum.

Currently active WiMAX amendments are: 802.16e-2005- Mobile 802.16; 802.16f-2005- Management Information Base; 802.16g-2007- Management Plane Procedures and Services; 802.16k-2007- Bridging of 802.16 (an amendment to 802.1D). There are several amendments under development: 802.16h- Improved Coexistence Mechanisms for License-Exempt Operation; 802.16i- Mobile Management Information Base; 802.16j- Multihop Relay Specification; 802.16Rev2- Consolidate 802.16-2004, 802.16e, 802.16f, 802.16g and possibly 802.16i into a new document. IEEE 802.16 Task Group m (TGm) is working on new amendment: 802.16m- Advanced Air Interface. Proposed work plan would allow completion of the standard by December 2009 for approval by March 2010.

In the IEEE 802.11 technology, security was added later. In IEEE 802.16, security has been considered as the main issue during the design of the protocol. However, security mechanism of the IEEE 802.16 (WiMAX) still remains a question. WiMAX is relatively a new technology; not deployed widely to justify the evidence of threats, risk and vulnerability in real situations. This paper will address the security aspects of the IEEE 802.16 Standard and point out the security vulnerabilities, threats and risks associated with this standard.

II. Security Solutions

IEEE 802.16 security specifications can mainly be found within the MAC layer. Security within the MAC layer is called the *security sublayer*. Its goal is to provide access control and confidentiality of the data link. Figure 1 shows IEEE 802.16 security sublayer. The separate security sublayer provides authentication, secure key exchange, and encryption.

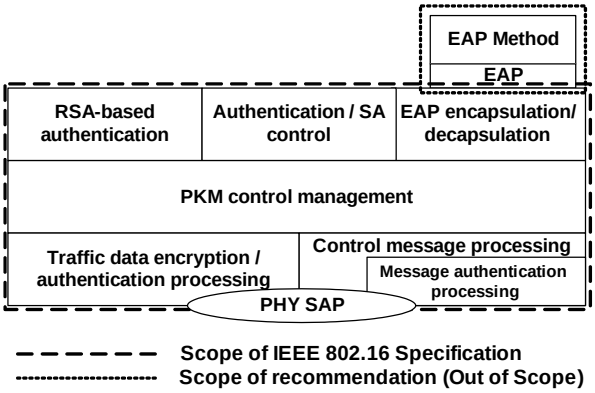

Fig. 1. IEEE 802.16 security sublayer [1]

When two parties establish a link, they are protected via a set of protocols that ensure confidentiality and unique access of the authorized parties. The unique handshaking between the two entities; namely base station (BS) and subscriber station (SS), is done at the MAC layer through security sublayer, which is based on the following concepts [2]:

Security associations: A security association (SA) is a set of security information parameters that a BS and one or more of its client SSs share in order to support secure communications. Data SA has a 16bit SA identifier, a Cipher (DES in CBC mode) to protect the data during transmission over the channel and two traffic encryption keys (TEKs) to encrypt data: one is the current operational key and the other is TEK [3]. When the current key expires, TEK a 2bit key identifiers is used. A 64bit

initialization vector (IV) is used for each TEK.

Three types of SAs are defined [4,5]: *primary*, *static*, and *dynamic*. Each manageable SS establishes a Primary Security association during the initialization process. Static SAs are provisioned within the BS. Dynamic SAs are used for transport connections when needed. Both Static and Dynamic can be shared by multiple SSs. It may use separate SAs for uplink and downlink channels [6]. BS ensures that each SS has access only to its authorized SAs.

Public key infrastructure (PKI): The WiMAX standard uses the Privacy and Key Management Protocol for securely transferring keying material between the base station and the mobile station. The privacy key management (PKM) protocol is responsible for privacy, key management, and authorizing an SS to the BS. The initial draft for WiMAX mandates the use of PKMv1 [6], which is a one-way authentication method. PKMv1 requires only the SS to authenticate itself to the BS, which poses a risk for a Man-in-the-middle (MITM) attack.

To overcome this issue, PKMv2 was proposed (later adopted by 802.16e), which uses a mutual (two-way) authentication protocol [5]. Here, both the SS and the BS are required to authorize and authenticate each other. PKMv2 is preventing from the following [7]: BS and SS impersonations, MITM attack and Key exchange issue. PKMv2 authentication/authorization method is shown in Figure 2.

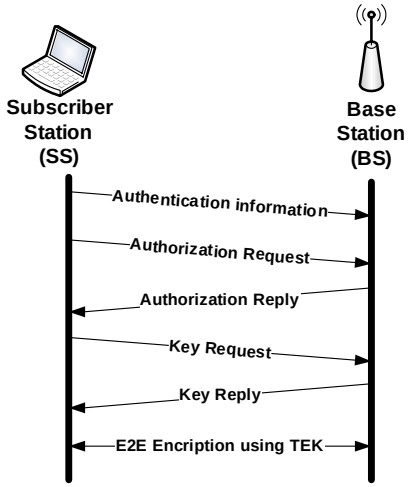

Fig. 2. The 2-way authentication and authorization of PKMv2 [8]

PKMv2 supports the use of the Rivest-Shamir-Adlerman (RSA) public key cryptography exchange. The RSA public key exchange requires that the mobile station establish identity using either a manufacturer-issued X.509 digital certificate or an operator-issued credential such as a subscriber identity module (SIM) card. The X.509 digital certificate contains the mobile station's Public-Key (PK) and its MAC address. The mobile station transfers the X.509 digital certificate to the WiMAX network, which then forwards the certificate to a certificate authority (Figure 3). The certificate authority validates the certificate, thus validating the user identity.

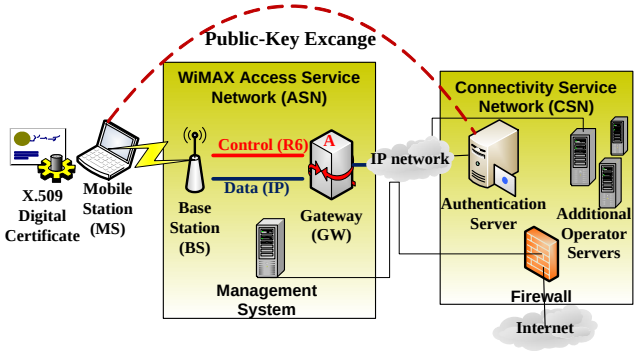

Fig. 3. Public Key Infrastructure

Once the user identity is validated, the WiMAX network uses the public key to create the authorization key, and sends the authorization key to the mobile station. The mobile station and the base station use the authorization key to derive an identical encryption key that is used with the advanced encryption standard (AES) algorithm.

Authentication: Authentication is the process of validating a user identity and often includes validating which services a user may access. The authentication process typically involves a supplicant (that resides in the mobile station), an authenticator (that may reside in the base station or a gateway), and an authentication server (Figure 4).

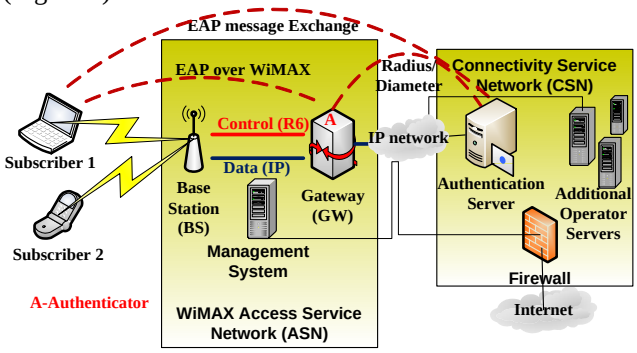

Fig. 4. EAP-based authentication

WiMAX uses the Extensible Authentication Protocol (EAP) to perform user authentication and access control. EAP is actually an authentication framework that requires the use of "EAP methods" to perform the actual work of authentication. The network operator may choose an EAP method such as EAP-TLS (Transport Layer Security), or EAP-TTLS MS-CHAP v2 (Tunneled TLS with Microsoft Challenge-Handshake Authentication Protocol version 2). The messages defined by the EAP method are sent from the mobile station to an authenticator. The authenticator then forwards the messages to the authentication server using either the RADIUS or DIAMETER protocols [9].

Data privacy and integrity: WiMAX uses the AES to produce ciphertext. AES takes an encryption key and a counter as input to produce a bitstream. The bitstream is then XORed with the plaintext to produce the ciphertext (Figure 5).

AES algorithm is the recommendation of 802.16e security sub-layer, since it can perform stronger protection

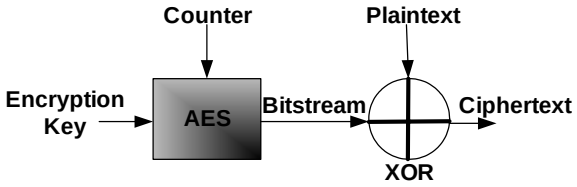

Fig. 5. AES Encryption

from theft of service and data across broadband wireless mobile network. Besides CCM-Mode and ECB-Mode AES algorithm supported in 802.16-2004, 802.16e supports three more AES algorithms: CBC-Mode AES, CTR-Mode AES and AES-Key-Wrap.

III. Threats and Vulnerabilities

In WiMAX, security threats apply to both the PHY and MAC layers. Possible PHY level attacks include jamming of a radio spectrum, causing denial of service to all stations, and flooding a station with frames to drain its battery. Currently, there are no efficient techniques available to prevent PHY layer attacks. Therefore, the focus of WiMAX security is completely at the MAC level [10]. In this section, we discuss some of the open security threats and vulnerabilities in the WiMAX networks.

A. Physical Layer Threats and Vulnerabilities

802.16 security is implemented as a sublayer at the bottom of MAC layer in order to protect data exchanged between the MAC layer and the PHY layer. In essence, it does not protect the PHY layer itself against the attacks which target the inherent vulnerability of wireless links.

Jamming and scrambling can be the form of attack to the PHY as the WiMAX 802.16 is defenseless. Jamming is achieved by introducing a source of noise strong enough to significantly reduce the capacity of the WiMAX channel. The information and equipment required to perform jamming are not difficult to acquire. Scrambling [10] is similar to jamming but this usually instigated for short intervals of time and is targeted to specific WiMAX frames or parts of frames. WiMAX scramblers can selectively scramble control or management messages with the aim of affecting the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit.

Another typical attack against the PHY layer, so called *water torture attack* [6], pushes a SS to drain its battery or consume computing resources by sending bogus frames. This type of attack against a mobile station could be even more destructive than a typical Denial-of-Service (DoS) attack against a wired machine because portable devices are likely to have limited resources.

In the *mesh* mode, 802.16 is also vulnerable to a replay attack in which an attacker maliciously resends valid frames that the attacker has intercepted in the middle of forwarding (relaying) process.

The PHY layer attacks can be prevented or mitigated by several trivial countermeasures. Increasing the power of signals can resist jamming attacks. For this, monitoring equipment can be used to detect radio jamming, and upon an abnormal state of radio spectrum the power of signals is increased in order to override malicious signals. According to [10], the bandwidth of signals can be increased by using spreading techniques such as frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). A sophisticate mechanism discarding bogus frames is needed to avoid running out of battery or computational resources by the water torture attack mentioned earlier. The latest 802.16 standard adds support for mobility of SS. This could make 802.16/WiMAX more vulnerable to these attacks against the PHY layer because an attacker does not necessarily have to reside in a fixed point and monitoring the anomaly becomes more difficult. Though intended scrambling is more complex than jamming, the probability for scrambling to occur is possible due to natural noise interruption and the availability periods of the attack. These attacks can be unveiled by analyzing discrepancies in the systems performance.

B. MAC Layer Threats and Vulnerabilities

There are several significant shortcomings of 802.16 security implemented at the MAC layer. To ultimately set up secure transport connections, 802.16 exploits a sequential two-way transactions for controlling, authorization, and authentication. The first problem is that, during the basic and primary connection, MAC management messages are sent in plain-text and not properly authenticated. Thus, the management message can be hijacked over the air and forged by an attacker in the middle. By doing so, the attacker can prepare for further attacks. Secondly, 802.16 uses the X.509 certificate, the standard for PKI, that defines a certification path validation to identify a genuine SS. It uses RSA encryption with SHA-1 hashing. Typically, a SS's certificate is pre-configured by the manufacture and persistent on the machine. Thus, the certificate could be stolen and tampered by an adversary unless it is kept secret.

Many serious threats arise from its authentication scheme. WiMAX supports unilateral device level authentication [10], which can be implemented in a similar way as Wireless-fidelity (Wi-Fi) MAC filtering based on the hardware device address. Therefore, address sniffing and spoofing make a SS masquerade attack possible. In addition, the lack of mutual authentication makes a MITM attack from a rogue BS possible. However, a successful MITM attack is difficult because of the time division multiple access (TDMA) model in WiMAX. The attacker must transmit at the same time as the legitimate BS using a much higher power level in order to "hide" the legitimate signal. Furthermore, WiMAX supports mutual authentication at user network level based on the generic EAP [11]. EAP variants, EAP- TLS (transport layer security) (X.509 certificate based) [12] and EAP- SIM [13], are supported.

Eavesdropping of management messages is a critical threat for users and a major threat to a system. For

example, an attacker could use this vulnerability to verify the presence of a victim at its location before perpetrating a crime. Additionally, it might be used by a competitor to map the network. Another major vulnerability is the encryption mode based on data encryption standard (DES). The 56 bit DES key is easily broken with modern computers by brute force attack. Furthermore, the DES encryption mode includes no message integrity or replay protection functionality and is thus vulnerable to active or replay attacks. The secure AES encryption mode should be preferred over DES [14]. Eavesdropping mostly affects the transfer of information and rarely causes system outage. The assessment of the eavesdropping threat is minor to the system but high for the user. Countermeasures for minor threats are not required.

The masquerading threat of the BS or SSs is enabled when authentication weaknesses are present. Identity theft and Rogues BS are specific techniques of masquerading. Identity theft is a severe threat to unlicensed services supported by WiMAX [10,15]. A fake device can use the hardware address of another registered device by intercepting management messages over the air. Once succeeded, an attacker can turn a BS into a rogue BS. A rogue BS can imitate a legitimate BS by confusing the associated SSs. Those SSs try to acquire WiMAX services from the rogue BS, resulting in degraded service or even service termination. Only for comparison, the Wi-Fi network employs carrier sense multiple access (CSMA), and thus identity theft has become one of the top security threats. The reason is that the attacker can easily capture the identity of a legitimate access point (AP) by listening to the CSMA process, which readily reveals information on the AP identity. The attacker can then construct a message by using the legitimate AP's identity, wait until the medium is idle, and distribute the malicious message.

Finally, there is a potential for DoS attacks because authentication operations trigger the execution of long procedures. For example, a DoS attack could flood a MS with a high number of messages to authenticate. Due to low computational resources, the MS will not be able to handle a large amount of invalid messages, rendering the DoS attack successful. The impact of this attack is classified as medium to the system as only time is affected at that level, but can be high for the user as it causes delays in the system responding to the individual's requests.

IV. Conclusion

In this paper we have studied the security solutions, vulnerabilities and threats of IEEE 802.16 (WiMAX). It can be seen that WiMAX provides a robust user authentication, access control, data privacy and data integrity using sophisticated authentication and encryption technology. WiMAX has both a sophisticated set of security protocols in its security suite and advanced bandwidth allocation mechanisms, which makes it a suitable candidate for enterprise applications.

On the other hand, it was found that WiMAX is subject to critical threats including jamming, eavesdropping and modification of management messages, masquerading as BS, and DoS attacks.

Even though some issues are no longer valid since the recent amendments and security solutions in 802.16, some remain unsolved and need to be carefully reviewed to avoid the same mistake as 802.11/Wi-Fi.

References

[1] IEEE Std. 802.16e, air interface for fixed and mobile broadband wireless access systems. IEEE Standard for local and Metropolitan Area Networks, February 2006.

[2] P. Chandra, *Securing WLAN links: Part 3. Telogy networks.* (2002, July 30) - Retrieved October 23, 2007, from http://www.CommsDesign.com.

[3] J. Hasan, *Security Issues of IEEE 802.16 (WiMAX)*, School of computer and Information Science, Edith Cowan University, Australia, 2006.

[4] IEEE Std. 802.16-2004, IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, October 2004.

[5] S. Adibi, G. B. Agnew,T. Tofigh, *End-to-End (E2E) Security Approach in WiMAX: Security Technical Overview for Corporate Multimedia Applications*, 747-758, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.

[6] D. Johnston and J. Walker, *Overview of IEEE 802.16 Security*, *IEEE Security & Privacy*, magazine May/June 2004.

[7] S.Adibi, G. B. Agnew, *End-to-End Security Comparisons Between IEEE 802.16e and 3G Technologies*, 364 - 378, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.

[8] S. Adibi, B. Lin, P.-H. Ho, G.B. Agnew, S. Erfani, *Authentication Authorization and Accounting (AAA) Schemes in WiMAX*, University of Waterloo, Broadband Communication Research Centre (BBCR) , appears in: Electro/information Technology, 2006 IEEE International Conference on 7-10 on pages: 210-215, May 2006.

[9] S. Adibi, G. B. Agnew, *Extensible Authentication (EAP) Protocol Integrations in the Next Generation Cellular Networks*, 776-789, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.

[10] M. Barbeau, *WiMax/802.16 Threat Analysis*, Proceedings of the 1th ACM Int. Workshop on Quality of Service & Security in Wireless and Mobile Networks, Q2SWinet '05, ACM Press, pp. 8-15, 2005.

[11] B.Aboba,, L.Blunk, J.Vollbrecht,, J.Carlson, & H. Levkowetz., *Extensible authentication protocol (EAP)* (IETF RFC 3748), 2004.

[12] B.Aboba, , & D.Simon,. *PPP EAP TLS authentication protocol* (IETF RFC 2716, 1999.

[13] H. Haverinen, & J. Salowey, *Extensible authentication protocol method for GSM subscriber identity modules (EAP-SIM)* (Internet draft [work in progress]). Internet Engineering Task Force, 2004.

[14] S. Chatzinotas, J. Karlsson, G. Pulkkis, K. Grahn, *Evaluation of Security Architectures for Mobile Broadband Access*, 759-775, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.

[15] Ernst and Young, *The necessity of rogue wireless device detection*, White Paper 2004.