International Journal of Scientific & Technical Development
(A Peer-Reviewed Bi-Annual Journal) ISSN: 2348-4047

VARIOUS SECURITY ISSUES INVOLVED IN PKM PROTOCOL

Dr. Rajeev Dahiya
Department of Computer Science and Engineering
Desh Bhagat University, Mandi Gobindgarh, Punjab,India

Abstract
Now a day's WiMAX is largely deployed by developed as well as developing countries to access Broadband Wireless. WiMAX deliver its services on high speed to the user without disconnectivity .IEEE 802.11 security issues has been taken in the account to design Privacy and key management protocol of IEEE 802.16. After major improvement in Privacy and Key Management protocol, PKM version 2 emerges in the market, but still several flaws exist in the Module. This paper is going to introduce threats in PKMv2 and critical Security issues that are needed to be rectified in Future.
Keywords: [WiMAX, IEEE 802.16, Security]

1. INTRODUCTION

Wireless Local area networks based on the IEEE 802.11/Wi-Fi standards have been an emerging standard in the communication environment and achieved a great success .However, when we can think about the wide area network, we see that in the developing countries for accessing the broadband wireless service is still up for grabs. By using Mesh technology we can expand the range of Wi-Fi from 100 meters to an entire metropolitan area, but still the performance of these mesh networks has yet to be tested. There is an emerging technology in the market, WiMAX. WiMAX, also called Worldwide Interoperability for Microwave Access, is a metro-area wireless technology defined in the IEEE 802.16 standards, is a solution for the "last mile" problem of wireless communication and promoted by the WiMAX Forum [14].WiMAX was designed to provide a broadband wireless access (BWA) service for metro areas. WiMAX has been finding a home among emerging markets that don't have a decent wired infrastructure. WiMAX uses Orthogonal Frequency Division Modulation (OFDM) technology, which has a lower power consumption rate. The first standard of 802.16 addressed the LOS communication in the 10–66GHz band. 802.16a extended its operation to include NLOS communication in the lower-frequency band of 2–11GHz. IEEE standard 802.16-2004 also supports mesh connectivity between subscriber stations. The development of IEEE 802.16e aims to provide mobility supports to its subscriber stations. [17] With the continuously growth on wireless communication in recent years, security is also a major issues for wireless network. Wireless networks are less secure as compared to wired networks due to their lack of physical infrastructure .So the protocols used for wired networks are not sufficient to provide adequate security to wireless network. So special attention should be paid to the security of wireless networks. IEEE 802.11 vulnerabilities and attacks have been taken into mind to fully protect WiMAX against critical attacks. The security protocol defined for the standard is ready to face the challenge in the open environment.

2. WiMAX Security Challenges

The IEEE 802.16-2004 standard defines operations at lower frequencies, thus reducing the hardware implementation complexity and the physical placement constraints. As a result, new security challenges emerge especially for the mesh mode, such as the trustworthiness of the next-hop mesh node. The IEEE 802.16e 2005 standard accommodates user mobility, hence facilitating attackers to easily stage an attack. With less constraint on physical location, the management messages become more vulnerable to attackers. Since WiMAX uses air interface for the transmission medium, both the PHY and MAC layers are readily exposed to security threats [14, 15].

2.1 Physical Layer Threats

Two principal threats to the WiMAX PHY are jamming and scrambling [11].

2.1.1 Jamming: 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. Resilience to jamming can be augmented by increasing the power of signals or increasing the bandwidth of signals via spreading techniques such as frequency hopping or direct sequence spread spectrum. The practical options include a more powerful WiMAX transmitter, a high gain WiMAX transmission antenna, or a high gain WiMAX receiving antenna. It is easy to detect jamming in WiMAX communications as it can be heard by the receiving equipment. Law enforcement can also be involved to stop jammers. Since jamming is fairly easy to detect and address, we believe that it does not pose a significant impact on both the WiMAX users and systems.

2.1.2 Scrambling Scrambling is 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. The attacker, often behaved as a WiMAX SS, can reduce the effective bandwidth of the victims, other SSs, and accelerate the processing of its own data by selectively scrambling the uplink slots of other SSs. Unlike the random behavior of a WiMAX jammer, a scrambler needs to interpret WiMAX control information correctly and to generate noise during specific intervals. Hence, attacks from scrambling are intermittent, and thus exacerbate the detection task. Monitoring anomalies beyond the performance norm is a viable means to detect scrambling and scramblers.

2.2 MAC Layer Threats

MPDU is the data unit transmitted in the WiMAX MAC layer. As shown in Figure 2.A, MPDU uses different formats to carry different information. The common format of each MPDU consists of a MAC header, service data, and an optional cyclic redundancy check (CRC). The unencrypted generic MAC header format contains the specific encryption information in the MAC header. Encryption is applied to the MAC PDU payload. All MAC management messages shall be sent unencrypted to facilitate registration, ranging, and normal operation of the MAC. The WiMAX management messages are carried in the MPDU as illustrated in Figure 2.B. WiMAX encrypts neither the MAC headers nor the MAC management messages, with the purpose to enable various operations of the MAC layer. Therefore, an attacker, as a passive listener of the WiMAX channel, can retrieve valuable information from unencrypted MAC management messages. Eavesdropping of management messages may reveal network topology to the eavesdropper, posing a critical threat to SSs as well as the WiMAX system. WiMAX requires devicelevel authentication to tackle this problem. The main idea is to issue a WiMAX device with a Rivest-Shamir-Adleman (RSA)/X.509 digital certificate from the manufacturer. The digital certificate is employed for authentication and authority detection. The unauthenticated device is blocked from eavesdropping of the network.

Generic MAC header	**MAC SDU (service data unit) Payload**	**CRC**

Figure 2. A

Generic MAC header	**MAC management message**	**CRC**

Figure **2. B**

Identity theft is a severe threat to unlicensed services supported by WiMAX [11, 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. The Wirelessfidelity (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. In WiMAX, time division multiple access (TDMA) is adopted. To steal the identity, the attacker must transmit while the legitimate BS is transmitting, and the signal of the attacker must arrive at the targeted SSs with high enough strength to subside the signal of the legitimate BS in the background. Since the transmission is divided into time slots, the attacker has to interpret the time slot allocated to the legitimate BS successfully and detect the BS signal strength correctly, both of which make identity theft more difficult and challenging. Besides, mutual authentication has been introduced into the latest WiMAX standard, further reducing the likelihood of identity theft. In the following sections, we will elaborate the PKM protocols, the security management mechanism to effectively overcome identity theft and eavesdropping in WiMAX.

3. Privacy Key Management Protocol Version1

The security sublayer is defined at the bottom of the WiMAX MAC layer to provide access control and confidentiality across the broadband wireless network through encryption and key management. Figure 3.1 illustrates the protocol stack of the security components of the WiMAX system. The PKM protocol in the middle provides secure distribution of keying data from the BS to the SS. PKM manages the key exchange process and the procedure for applying the supported encryption and authentication algorithms to MPDUs. By specifying the synchronization of keying data between the BS and SS, PKM enforces the conditional access to a particular WiMAX connection

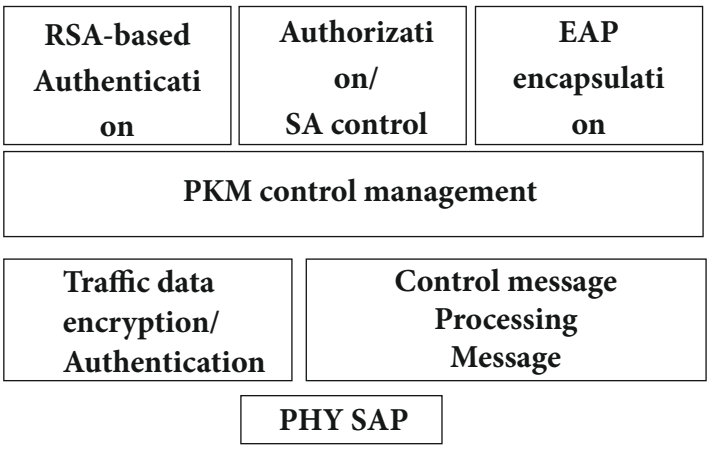

Figure 3.1 Protocol stack of the security sublayer.

3.1 Security Procedure

WiMAX communications follow the security procedure defined in PKMv1 to ensure secure access of a connection. As shown in Figure 3.1, authentication is conducted as the first step of security enforcement prior to any data

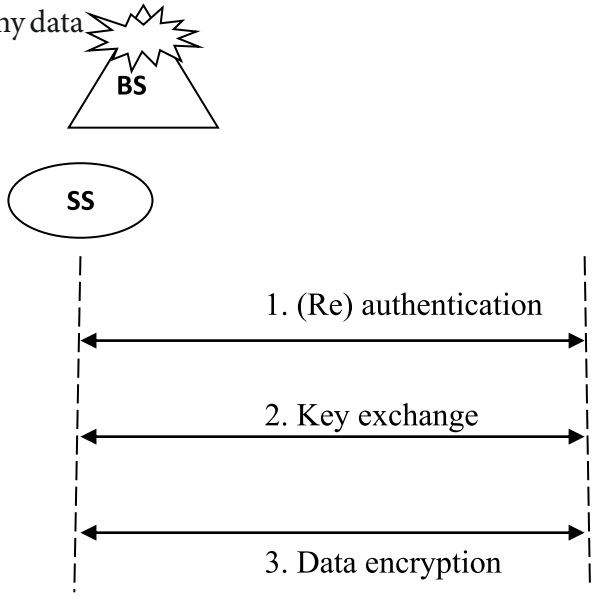

Figure 3.1 WiMAX security procedure. transmission. When an SS enters the WiMAX network, the BS verifies the SS identity, followed by the key exchange step. Once the SS identity is authenticated and a key is successfully established, the BS registers the SS into the network and the key is used to encrypt the data transmitted through the WiMAX connection. The remaining part of Section 3 will elaborate each step of the security procedure. 3.2 Authentication Authorization is the process for authenticating a client SS's identity by the BS. An SS starts authorization by sending an authentication

information message to the target BS, containing the SS manufacturer's X.509 certificate issued by the manufacturer or an external authority. [17]Following the authentication information message, an authorization request message is sent immediately to the BS to request for an authentication key, with the following information from the SS for security authentication:

• A description of the cryptographic algorithms that the requesting SS supports (the so-called security association [SA]) • The SS's basic CID, which is equal to its primary security association identifier (SAID) The detailed process of security authentication is shown in Figure 3.2. In the authentication process, WiMAX standards define the term "security association" to specify the set of security information a BS and its SS (or SSs) share. SA, identified with a SAID, is essentially the set of security information a BS and its SSs support for secure communications. It includes the cryptographic suites and keys for encryption. As illustrated in Figure 3.2, an SS informs the BS of its SAID. The BS validates the requesting SS's identity by determining the encryption algorithms and protocols it shares with the SS. The BS also determines whether the SS is authorized for basic unicast services and any other services provided by the WiMAX network. After verifying the requesting SS's identity, the BS activates an authentication key (AK) for the SS, encrypts it with the SS's public key, and sends it back to the SS in an authorization reply message. Authorization reply includes the AK encrypted with the SS's public key, a 4-bit key sequence number (used to distinguish between successive Aks), a key lifetime, and the identities and properties of the SA list the SS has been authorized to access. With the authentication process, the BS associates the SS's authenticated identity to a paying subscriber, and hence to the data services that the subscriber is authorized to access. With the AK exchange, the BS determines the authenticated identity of the client SS and the services the SS is authorized to access. Since the BS authenticates the SS, it protects against an attacker from employing a cloned SS, masquerading as a legitimate subscriber's SS.

[11, 14]

Figure 3.2 The authentication process. PKMv1 mandates the use of X.509 digital certificates together with the RSA public-key encryption algorithm to conduct authentication. [11, 12]

3.3 Key Exchange There are five kinds of keys used to secure WiMAX communications: AK, key encryption key (KEK), downlink hash function-based message authentication code (HMAC) key, uplink HMAC key, and traffic encryption key (TEK). AK is activated by a BS during the authentication process. As the shared secret between the SS and the BS, AK is used to secure subsequent key exchanges in PKMv1. As shown in Figure 3.3, a 128-bitAKis used to generate the 128-bit KEK by the BS. KEK is used for TEK encryption and distribution. The KEK is derived from the AK by the following formula:

KEK =Truncate_128{SHA1[(AK|0
44)Θ5364]} (3.a)

In Equation 3.a, AK concatenates with 044 and XORs 5364 as denoted by (AK| 044)È5364. The result is hashed by the secure hash algorithm SHA1, the most commonly used hash function defined by the secure hash standard

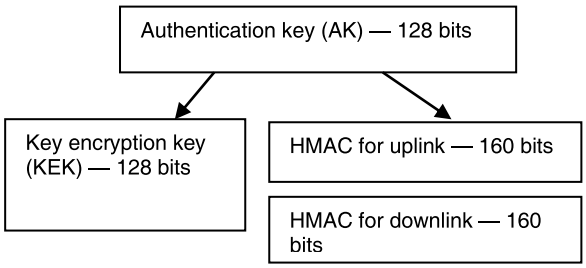

Figure 3.3 The key derivation process. Truncate_128(.) retrieves the first 128 bits of the hash result as the KEK and discards the rest of the bits. The downlink HMAC key and uplink HMAC key provide data authenticityof key distribution messages from the BS to the SS and from the SS to the BS, respectively. They are both generated from the AK in a similar way as defined by Equation 3.a. The TEK exchange process relies on the downlink HMAC key and the uplink HMAC key to secure the exchanging messages.

3.4 Data Encryption

Upon the completion of authentication and initial key exchange, data transmission between the BS and the SS starts by using the TEK for encryption. Figure 3.4 depicts the process, where data encryption standard with cipher block

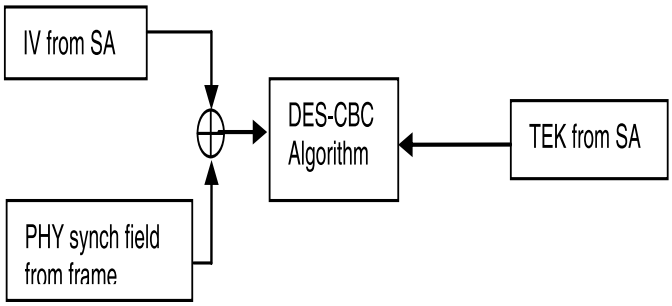

Figure 3.4 WiMAX MPDU encryption process.

changing (DES-CBC) encryption enciphers the MPDU payload field. Neither the header nor the CRC is encrypted to support diverse services. As exemplified in Figure 3.4, when the security sublayer generates an MPDU, it checks the SA associated with the current connection and acquires the initialization vector (IV). The MPDU IV is generated by XORing the SA IV with the synchronization field in the PHY frame header. The DESCBC algorithm then encrypts the MPDU plaintext payload by employing the generated MPDU IV and the authenticated TEKs.

3.5 Challenges

PKMv1 uses a client/server model for traffic key management, where an SS is the client, requesting keying material, and a BS is the server, responding to the requests. The major challenge comes from the unilateral authentication. PKMv1 ensures that individual SS clients receive only keying material authorized by the BS, the BS authenticates an SS during each process but not vice versa. This implies that an SS is not capable of detecting a rogue BS. As discussed in Section 2.2, the impact of a rogue BS includes identity theft, degraded throughput, and even service termination. PKMv2 overcomes this by introducing mutual authentication, enabling the SS to authenticate the BS as well [14, 17].

4. Privacy Key Management Protocol Version2

PKMv2 is defined in IEEE 802.16e-2005 and it requires mutual authentication between SS and BS, a major deviation from PKMv1. PKMv2 also has more enhanced security features such as new key hierarchy for AK derivation and extensible authentication protocol (EAP) [14]. The following part of this section will introduce these significant changes.

4.1 Mutual Authentication

To enable mutual authentication between SS and BS, the authorization process follows these steps:

(a) The BS authenticates the client Ss's identity.

(b) The SS authenticates the BS's identity.

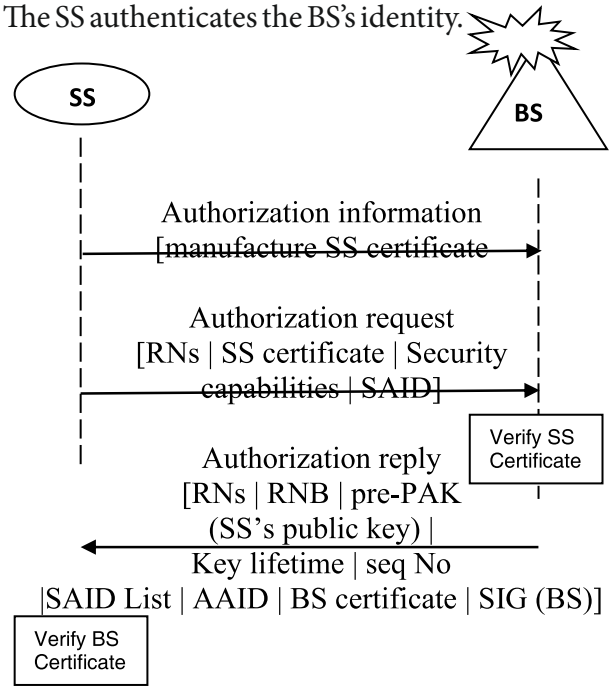

FIGURE 4.1 The mutual authorization process between an SS and the BS. (c) The BS provides the authenticated SS with the AK, and then a KEK and message authentication keys are derived from this AK. (d) The BS provides the authenticated SS with the identities (the SAIDs) and properties of SAs from which the SS can obtain the encryption key information for subsequent transport connections. Similar to PKMv1, the SS sends an authorization request message to the target BS, requesting an AK immediately after sending the authentication information message. The authentication information message is the same as that in PKMv1. As compared to the authorization request message in PKMv1, an SS running PKMv2 adds a 64-bit random number NS in the authorization request message. This NS is returned in the authorization reply message from the BS to the SS in securing the authentication process. PKMv2 also adds a 64-bit random number NB, the BS's X.509 certificate, and BS's signature in the authorization reply message. The random numbers NS and NB are included in the exchange, and both the SS and BS can check the replied numbers to ensure the time freshness of the message, and thus to prevent the replay attack..

4.2 Authorization Key Derivation

The PKMv2 key hierarchy defines the key category and the algorithms used to generate keys. The authentication and authorization processes generate source key materials. These keys form the roots of the key hierarchy and will be used to derive other keys to ensure management message integrity and to transport the traffic encryption keys. All PKMv2 key derivations are based on the Dot16KDF algorithm. PKMv2 supports two authorization schemes with mutual authentication. The RSA-based authorization process and the EAP-based authentication process. The AK will be derived by the BS and the SS from the PAK via the RSA-based authorization procedure and the PMK via the EAP-based authorization procedure.

5. Future Work

Although the PKMv2 protocols improve WiMAX security by adopting new features such as mutual authentication and flexible key management, there are still flaws rooted in the WiMAX standard itself. First, since the MAC management messages are transmitted without encryption, valuable information can be given away to attackers. For example, an attacker can passively listen to the communications between an SS and a BS, intercept the management messages, verify the presence

FIGURE 4.1 The mutual authorization process between an SS and the BS. (c) The BS provides the authenticated SS with the AK, and then a KEK and message authentication keys are derived from this AK. (d) The BS provides the authenticated SS with the identities (the SAIDs) and properties of SAs from which the SS can obtain the encryption key information for subsequent transport connections. Similar to PKMv1, the SS sends an authorization request message to the target BS, requesting an AK immediately after sending the authentication information message. The authentication information message is the same as that in PKMv1. As compared to the authorization request message in PKMv1, an SS running PKMv2 adds a 64-bit random number NS in the authorization request message. This NS is returned in the authorization reply message from the BS to the SS in securing the authentication process. PKMv2 also adds a 64-bit random number NB, the BS's X.509 certificate, and BS's signature in the authorization reply message. The random numbers NS and NB are included in the exchange, and both the SS and BS can check the replied numbers to ensure the time freshness of the message, and thus to prevent the replay attack..

4.2 Authorization Key Derivation

The PKMv2 key hierarchy defines the key category and the algorithms used to generate keys. The authentication and authorization processes generate source key materials. These keys form the roots of the key hierarchy and will be used to derive other keys to ensure management message integrity and to transport the traffic encryption keys. All PKMv2 key derivations are based on the Dot16KDF algorithm. PKMv2 supports two authorization schemes with mutual authentication. The RSA-based authorization process and the EAP-based authentication process. The AK will be derived by the BS and the SS from the PAK via the RSA-based authorization procedure and the PMK via the EAP-based authorization procedure.

5. Future Work

Although the PKMv2 protocols improve WiMAX security by adopting new features such as mutual authentication and flexible key management, there are still flaws rooted in the WiMAX standard itself. First, since the MAC management messages are transmitted without encryption, valuable information can be given away to attackers. For example, an attacker can passively listen message is the same as that in PKMv1. As compared to the authorization request message in PKMv1, an SS running PKMv2 adds a 64-bit random number NS in the authorization request message. This NS is returned in the authorization reply message from the BS to the SS in securing the authentication process. PKMv2 also adds a 64-bit random number NB, the BS's X.509 certificate, and BS's signature in the authorization reply message. The random numbers NS and NB are included in the exchange, and both the SS and BS can check the replied numbers to ensure the time freshness of the message, and thus to prevent the replay attack..

4.2 Authorization Key Derivation

The PKMv2 key hierarchy defines the key category and the algorithms used to generate keys. The authentication and authorization processes generate source key materials. These keys form the roots of the key hierarchy and will be used to derive other keys to ensure management message integrity and to transport the traffic encryption keys. All PKMv2 key derivations are based on the Dot16KDF algorithm. PKMv2 supports two authorization schemes with mutual authentication. The RSA-based authorization process and the EAP-based authentication process. The AK will be derived by the BS and the SS from the PAK via the RSA-based authorization procedure and the PMK via the EAP-based authorization procedure.

5. Future Work

Although the PKMv2 protocols improve WiMAX security by adopting new features such as mutual authentication and flexible key management, there are still flaws rooted in the WiMAX standard itself. First, since the MAC management messages are transmitted without encryption, valuable information can be given away to attackers. For example, an attacker can passively listen to the communications between an SS and a BS, intercept the management messages, verify the presence

of the victim SS from the management message content, and then perpetrate a crime. Second, the key management mechanism depends on the 2-bit EKS field to identify the TEK being used. The value of this field wraps from 3 to 0 on every fourth key, and thus it is easy for an attacker to interject reused TEKs [12].

Third, the original DES-CBC algorithm uses a random IV to secure the encryption, while in PKMv1 and PKMv2 the IV is generated as the XOR result of the SA's IV and the PHY synchronization field. This kind of predictable IV impairs data security. Moreover, the DESCBC algorithm can only secure a limited length of data. It has been shown that DESCBC loses its security after encrypting 232 data blocks using the same TEK with each block containing 64 bits. Since each TEK has its lifetime, DES-CBC cannot secure data when the incoming data length during the TEK's lifetime is longer than 64×232 bits [14].As more valuable broadband services are enabled in WiMAX, more security concerns will emerge. For example, the mesh mode defined in WiMAX is more vulnerable to security threats than the traditional PMP mode. With each node being capable of forwarding traffic to its adjacent nodes,

critical problems such as malicious neighbors and authorization node spoofing challenge the user privacy and system operation tremendously.

6 Conclusions

Driven by both the IEEE and the industrial forum, WiMAX is gaining more support from service providers as the solution for broadband wireless access. WiMAX is inevitably exposed to more security threats from the open-air channel to support both the LOS and NLOS spectra with flexible user mobility. This paper focuses on the PKM protocols, which play an important role to secure the connection and transmission across BWA. The processes of user authentication, key exchange, and data encryption have been reviewed with the emphasis on certificate verification, key derivation, and MDPU payload encrypment, respectively. Nevertheless, new security features in the latest standard have been covered and some open issues of WiMAX security are highlighted for future exploration.

References

[1] Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka [2007] "Security Vulnerabilities and Solutions in Mobile WiMAX", KDDI R&D Laboratories, 2-1-15, Ohara, Fujimino-shi, Saitama 356-8502, Japan.

[2] Arkoudi-Vafea Aikaterini [2006]"SECURITY OF IEEE 802.16" Department of Computer and Systems Science, Royal Institute of Technology.

[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, Extensible Authentication Protocol (EAP), The Internet Engineering Task Force—Request for Comments: 3748, June 2004.

[4] Christian Hoymann, Michael Dittrich, Stephan Goebbels [2007] "Dimensioning Cellular Multihop WiMAX Networks" Chair of Communication Networks (ComNets), RWTH Aachen University, Pages:150 – 157.

[5] David Teyao Chen [2007] "On the Analysis of Using 802. 16e WiMAX for point -to-Point Wireless Backhaul" Networks Advanced Technologies, Networks & Enterprise Business Motorola Inc. 1441 W. Shure Drive, Arlington Heights, IL 60004,USA.

[6] Dusit Niyato, Ekram Hossain, and Jefferey Diamond [2007] "IEEE 802.16/WIMAX-BASED BROADBAND WIRELESS ACCESS AND ITS APPLICATION FOR TELEMEDICINE/E-HEALTH SERVICES" Trlabs and University of Manitoba.

[7] Ender Yuksel [2007] "Analysis of the PKMv2 Protocol in IEEE 802.16e- 2005 Using Static Analysis "Technical University of Denmark Informatics and Mathematical Modelling Building 321, DK-2800 Kongens Lyngby, Denmark.

[8] E. Sedoyeka1, Z. Hunaiti1, M. Al Nabhan2 and W. Balachandran [2008]" WiMAX Mesh Networks for Underserved Areas" Anglia Ruskin University, Brunel University. Pages: 1070 – 1075.

[9] IEEE Std. 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, 2001.

[10] IEEE Std. 8802.16e-2005, IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed and Mobile Broadband Wireless

Access Systems, IEEE, 2006. [11] Kejie Lu, Yi Qian, Hsiao-Hwa Chen, Shengli Fu [2008]" WiMAX Networks: From Access to Service Platform" National Institute of Standards and Technology, University of North Texas. IEEE Volume 22, Page(s):38 – 45.

[12] Leonardo Maccari, Matteo Paoli, Romano Fantacci [2007]"Security analysis of IEEE 802.16" Department of Electronics and Telecommunications - University of Florence Telecommunication Network Lab Florence, Italy. Pages 1160 –1165.

[13] M. Barbeau, WiMax/802.16 threat analysis, Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks, pp. 8–15, October 2005.

[14] Qiang Ni, Alexey Vine, Yang Xiao, Andrey Turlikov [2007]" Investigation of Request Mechanisms under Pointto- Multipoint Mode of WiMAX Bandwidth Networks.

[15] Sen Xu Manton Matthews Chin-Tser Huang "Security Issues in Privacy and Key Management Protocols of IEEE 802.16" Department of Computer Science and Engineering, University of South Carolina, SC 29208, USA.

[16] Suthida Wattanachai [2006]" Security Architecture of the IEEE 802.16 Standard for Mesh Networks" Department of Computer and Systems Sciences Stockholm University / Royal Institute of Technology.

[17] Yongqiang Zhang [2008] "Vertical Handoff between 802.11 and 802.16 Wireless Access Networks" Electrical and Computer Engineering, Waterloo, Ontario, Canada.