Annales UMCS Informatica AI X, 2 (2010) 177-185
DOI: 10.2478/v10065-011-0022-7

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

WiMAX Networks – architecture and data security

Łukasz Kucharzewski*, Zbigniew Kotulski†

Institute of Telecomunications, Warsaw University of Technology,
Pl. Politechniki 1, 00-661 Warszawa, Poland.

Abstract – This document presents thorough information on the WiMAX technology, its detailed architecture and illustrates security mechanisms employed. The first part discusses basic properties and components of WiMAX network. Individual sub-layers of the network operation have been presented. The second part describes all security-related aspects and solutions employed to ensure secure data exchange: cryptographic keys generation and exchange, authentication processes and encrypted data exchange. The last part illustrates potential attacks, means of effective protection and methods for improving security in WiMAX networks.

1 The IEEE 802.16 Standard

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless radio data transmission technology based on the IEEE 802.16 and ETSI HiperMAN standards, designed to ensure Broadband Wireless Access (BWA) [1]. The technology is standardized by the IEEE association, whereas its organizational body is the WiMAX Forum which associates leading telecommunication operators and manufacturers of network hardware and components (Intel, AT&T, Samsung, Motorola, Cisco and others). Their main goal is to develop and promote the standard and to issue "WiMAX Certified^{TM}" certificates for the equipment from various hardware manufacturers. These certificates confirm compatibility with the adopted IEEE 802.16 standard [3].

The IEEE 802.16 standard was established in 2001 (Fig. 1) and kept evolving within subsequent years during which new changes and improvements were implemented.

*l.kucharzewski@tele.pw.edu.pl
†z.kotulski@tele.pw.edu.pl

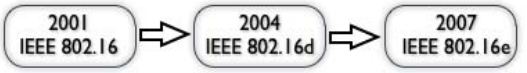

Fig. 1. WiMAX Network Standards.

Initially the technology was a subject to several constraints, mainly related to its utilized frequency band (the 10-66 GHz band) and Line of Sight (LOS) requirements. In the so-called Fresnel zone, the propagated energy was effectively attenuated, which caused breaks in data transmission and signal decay. In the IEEE 802.16d standard, approved in 2004 (based on prior 802.16a, 802.16b, 802.16c standards) the line of sight problem was solved by employing longer radio wavelengths in the frequency band below 11 GHz. Additionally several advanced mechanisms improving properties of radio antennas and HARQ (Hybrid Automatic Repeat Request) transmission control mechanisms were introduced to the physical layer. The development focused also on the implementation of Quality of Service (QoS) control mechanisms in order to reduce transmission lag and to introduce process prioritizing. The latest, approved IEEE 802.16e standard introduces mobility of users and terminals operating in the 2 – 6 GHz frequency band. This became possible due to the implementation of handover mechanism, known from mobile telephone networks, ensuring transparent switching of the whole transmission session state to another base station, which ensures better quality of the transmitted signal. This technique, combined with high data link bandwidths provides unlimited options for data transmissions, e.g. availability of Triple Play data packets. Additionally special mechanisms supporting equipment mobility have been introduced. These are: subscriber station's standby mode improving accumulated power management and idle mode which allows Subscriber Stations (SS) to receive broadcast messages from base stations without the need to log on to the network.

2 The WiMAX Architecture

The WiMAX network is a wireless network technology and as such its operating principle can be related and compared to the ISO OSI reference model. As a technology, which utilizes radio wave as a transmission medium, it spans over two bottommost layers of the ISO model: the physical layer and the Medium Access Control (MAC) layer (Fig. 2).

The main aim of WiMAX development was to ensure efficient data transmission. This is why the technology utilizes proven physical layer solutions supporting more effective data transmissions. The primary source of the improved data transmission capabilities was utilization of the Orthogonal Frequency Division Multiplexing (OFDM) data transmission technology. This is one of many modulation methods which utilizes multiple sub-carries orthogonal to each other, thus ensuring the optimal compensation of selective decays resulting from the fact that signal is transmitted over multiple paths. In this technology a single data stream is coded in multiple sub-carriers (256 sub-carriers in 802.16d). This technology allows high bandwidths to be achieved and the radio band to be better used. Orthogonal Frequency Division Multiple Access (OFDMA) is an improved version of the OFDM technology.

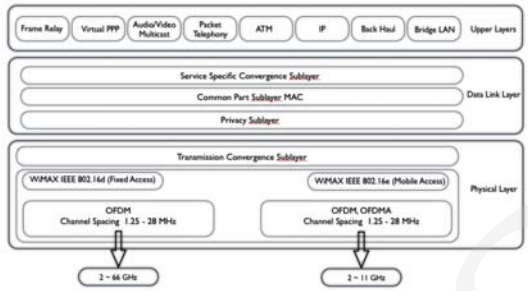

Fig. 2. WiMAX Network Architecture.

The OFDM frequency distribution and multiple user access is accomplished by means of assigning different users to different subchannels. In order to better support mobile users, the technology also modulates the transmitted signal power based on the quality of the data transmission channel. The physical layer provides five operating options which are selected depending on the frequency band and modulation techniques used. These are:

(1) WirelessMAN-SC (single carrier (SC) modulation, 10-66 GHz band).
(2) WirelessMAN-Sca (SC modulation, NLOS, <11GHz band).
(3) WirelessMAN-OFDM (OFDM modulation, <11GHz band).
(4) WirelessMAN-OFDMA (OFDMA modulation, <11 GHz band, terminal mobility).
(5) WirelessHUMAN (<11GHz band license-free).

The Transmission Convergence Sublayer lies between the physical layer and MAC layer. Its purpose is to convert variable length of MAC protocols data units to fixed-length units used in the physical layer. This sublayer is only used in the case of the WirelessMAN-SC option.

The MAC layer establishes and manages many different connections using a single physical medium. This layer consists of the following key sublayers:

(1) Service-Specific Convergence Sublayer (CS).
(2) MAC Common Part Sublayer (MAC CPS).
(3) Privacy Sublayer (PS).

The service-specific convergence sublayer accepts traffic and converts higher protocol data units to data units, which are compatible with the MAC layer specifications. It can also employ the Payload Header Suppression (PHS) mechanisms.

The MAC CPS layer is responsible for system access, bandwidth allocation for individual services and connection set-up and management. It also verifies Quality of Service (QoS) which is used by the physical layer for data transmission and queuing.

The security sublayer is responsible for ensuring adequate security level of communicating nodes. For this purpose it uses, for example, digital certificates and encryption algorithms. It supports such services as authentication, secure exchange of encryption keys and transmission encryption.

3 WiMAX Security

The security architecture has been defined in a dedicated Privacy Sublayer (PS)to ensure appropriate level of security for the parties involved in a transmission. This sublayer ensures parties' authentication as well as transmitted data integrity and confidentiality (Fig. 3). As early as in the 802.16 standard design stage, appropriate transmission security techniques and methods were considered. This was intended to prevent reoccurrence of numerous errors made during the 802.11 standard implementation.

Security Association (SA) is a container of key information utilized for ensuring secure communication between a Subscriber Station (SS) and a Base Station (BS). There are two types of SA: Data SA and Authorization SA. Data SA protects communication between one or more SSs and a BS. Data SA contains the elements listed in a Table 1 below. There are three types of Data SA: primary, static and dynamic. Primary SA is set by SS while setting up a connection with the base station. Static SAs are made available by base stations. Dynamic SAs are created and removed as needed to ensure secure communication (VoIP, VoD, etc.).

Table 1. Data SA payload.

16-bit SA identifier (SAID).
Encryption cipher to protect the data exchanged over the connection.
Two TEKs: one for current operation and another when the current key expires.
Two 2-bit key identifiers, one for each TEK.
TEK lifetime. The minimum value is 30 min and the maximum value is 7 days (default is 2 days).
Initialization vector for each TEK.
Data SA type indicator (primary, static, dynamic).

Authorization SAs contain the elements listed in Table 2, which are shared by the base station and the subscriber station. They are used by base stations to configure Data SA intended for a subscriber station.

Table 2. Authorization SA payload.

X.509 certificate identifying the subscriber station.
160-bit authorization key.
4-bit authorization key identifier.
Authorization key lifetime. The minimum value is 1 day and the value maximum is 70 days (default is 7 days).
Key encryption key (KEK) for distributing TEKs.
Downlink hash function-base message authentication code (HMAC) key.
Uplink HMAC keys.
List of authorized data SAs.

The WiMAX Standard employs proven and robust cryptographic algorithms. Data confidentiality is ensured by symmetric Data Encryption Standard (DES), by Triple DES (3DES), Advanced Encryption Standard (AES) and asymmetric Rivest, Shamir, Adleman (RSA) algorithms. In order to ensure integrity of transmitted data, Keyed-Hash Message Authentication Code (HMAC) and Cipher-Based Message Authentication Code (CMAC) mechanisms are used. The authorization and authentication processes are implemented based on the Privacy Key Management (PKM) protocol which utilizes asymmetric encryption as well as on public key certificates. This protocol is also involved in the key management mechanism which is performed as an immediate consequence of a device logging on to the network and SS authentication [12].

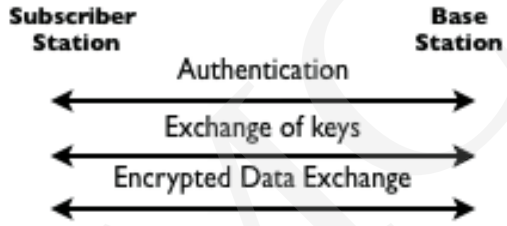

Fig. 3. Exchange of information between stations.

This protocol is based on the so-called Security Associations (SA). This is a state specific and unique for each connection, describing its cryptographic properties, such as values and validities of used cryptographic keys and used algorithms. There are two versions of the PKM protocol. The PKMv1 is used to protect nomadic networks (including LOS and NLOS connections), whereas the other – PKMV2 is used to protect WiMAX networks with mobility support (IEEE 802.16e) [4, 5].

3.1 PKM v1 Protocol

This protocol uses asymmetric ciphers (primarily RSA) to validate identity of stations. A subscriber station commences the authentication process with presentation of the station's certificate issued by its manufacturer (Fig. 4). Optionally it may also send the hardware manufacturer certificate. Following certificate validation, the base station generates an Authorization Key (AK) which is sent back to the subscriber station encrypting it with a public key obtained from the subscriber station's certificate. The subscriber station decrypts it using its private key. In this way both parties obtain cryptographic material necessary for link protection. The PKMv1 protocol skips user data authentication ensuring only its privacy. The Transmission Encryption Key (TEK), which is generated at a later stage, similarly to AK is determined by the base station.

Each new association is assigned with an individual encryption key. The key ensuring secure transmission of the TEK key is the Key Encryption Key (KEK) generated based on the AK key as well as Hash Message Authentication Code Key for Downlink (HMAC-KEY-D) and Hash Message Authentication Code Key for Uplink (HMAC-KEY-U) keys. The purpose of

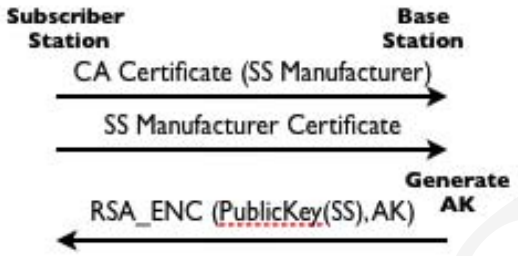

Fig. 4. Station Authentication Process.

the KEK is to encrypt messages that are used to transfer the TEK keys. On the other hand, HMAC family of keys are used to generate authentication checksums in control messages. These checksums are calculated using the Secure Hash Algorithm (SHA-1) function. Key transmission messages are encrypted with 3DES algorithm in a mode, in which each 64-bit data block is encrypted independently. It is worth mentioning here that each security association consists of two TEKs (the current and a spare one). Traffic decryption can be performed using both of these keys, whereas only the current key permits data encryption. The standard recommends that Transmission Encryption Keys are pseudo-random sequences and fails to clearly specify their generation methods. For purposes of user protection, the PKMv1 protocol of the IEEE 802.16d standard utilizes advantages of the AES block algorithm operating in a special mode called Counter Mode with Cipher Block Chaining Message Authentication Code (CCM) [11].

3.2 PKMv2 Protocol (IEEE 802.16e standard)

Version 2 of the PKM protocol was developed in response to numerous shortcomings in the protection system used in the previous version of the protocol. The PKMv2 standard bases on the techniques adopted in the IEEE 802.11i standard. Contrary to the first version of the protocol, the authentication stage in the second version has been implemented based on the Extensible Authentication Protocol (EAP). The network infrastructure has been also extended with an Authentication, Authorization, Accounting (AAA) server supporting the EAP on the network side. The result of these operations is a unique cryptographic material, generated independently by mutually authenticating parties. The DES and AES algorithms have been used to ensure link privacy. The PKMv2 protocol assumes that both subscriber and base stations should have a certificate. Terminal authentication (Fig. 5) starts with optional presentation of a manufacturer's certificate to the base station. Then the base station sends an authentication request containing a certificate issued by its manufacturer and a generated random number (RAND_SS). Having verified the certificate, the base station responds with a message containing its own X.509 certificate encrypted with the subscriber station's public key (Pre-Primary Authorization Key /Pre-PAK/), the RAND_SS number received in the previous message and with its generated RAND_BS number. Next, the subscriber station verifies

the validity of the certificate received, check correctness of the previously generated random number and deciphers the Pre-PAK key [11].

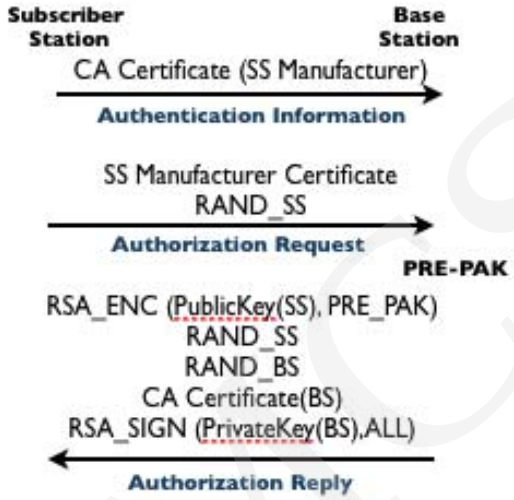

Fig. 5. Station and network authentication process in PKMv2.

As mentioned previously, the PKMv2 protocol is based on the EAP to authenticate end users. Implementation with this protocol requires special elements of the network architecture:

- Supplicant – is the application on the side of the subscriber station which is responsible for EAP-based authentication,
- AAA server with database of activated users in the network and authentication methods used,
- Authenticator – a network element constituting a network access point which blocks the whole traffic except for EAP authentication messages until authentication success message is received from the AAA server.

The result of user authentication process is the Master Session Key (MKE) generated independently by the supplicant and by the authentication server which sends it further to the base station.

3.3 WiMAX Security Assessment

The WiMAX technology is a relatively young technology permitting wireless access to broadband data transmission. Despite employment of the latest security mechanisms it has certain loopholes. Also we can assume that the development of this technology did not involve so much time and effort as other wireless technologies. LOS networks are susceptible to Man In the Middle (MITM) attacks. In the attack of this type, an aggressor takes over the user connection, using for this purpose a bogus base station, coupled with a properly activated terminal. Next, transmitted user data are decrypted by the bogus base station, monitored,

modified by the intruder and then sent to the users' home network. The AK determined in this way by the bogus base station constitutes an input to a database of encryption and authentication keys. In this total control over the attacked user data may be gained. A higher level of protection could be achieved by using a good base station random network generator, which would generate random keys resistant to cryptographic analysis attempts. Initially the risk of MITM attacks in LOS networks was considered insignificant, as the first IEEE 802.16 standard assumed only the communication using physical layers which required line of sight visibility of transmitter and receiver. This required the attacker to position itself exactly on the signal path between the transmitter and the receiver, at a considerable elevation. During standardization of further versions of the technology, which permitted multi-path propagation, the risk of this type of attacks grew significantly [4].

The PKMv2 protocol implements numerous improvements, which eliminates the risk of such attacks. It also introduces mobile users support. If proven cryptographic techniques are used, it seems that opportunities for a successful attack are precluded. However, there are several loopholes which, if effectively used, could pose a threat to data exchange between parties. Hence the following types of attacks are plausible:

- Rogue base stations.
- DoS attacks.
- Man-in-the-middle attacks.
- Network manipulation with spoofed management frames.

Policies and profiles for WiMAX PKI are defined in WiMAX Forum. X.509 certificates and their associated keys are used to identify and authenticate the identity of devices and servers in a WiMAX network. Additional user authenticity acknowledgement mechanisms would certainly improve the level of security of parties connected to WiMAX network. Users would be required to register in a global database to obtain a network-unique identifier and secret PIN code. Additional critical services could be protected by generating an additional security key. Also a unique user id could be assigned in order to identify certificates and their associated information.

At the current stage of the technology development no significant errors have been discovered in the WiMAX network protocols and mechanisms, which could be exploited for successful attacks. Certainly we will hear about many such security loopholes when WiMAX networks become common on the telecommunication market. Sources of such errors may be related to end user hardware loopholes, problems with intrusion detection systems as well weaknesses of peripheral equipment connected to the WiMAX network.

To conclude, it is necessary to point out that the overall key agreement and exchange mechanism, necessary for data transmission encryption, is very complicated. X.509 standard certificates protect users against third parties attempting to spoof their terminals. Frequent renewal of encryption keys also improves the overall security level and deters potential intruders from attempted attacks.

References

[1] IEEE, 802.16a-2004 IEEE Standard for local and metropolitan area networks part 16: air interface for fixed broadband wireless access systems (2004).

[2] IEEE 802.16e-2005 IEEE Standard for local and metropolitan area networks part 16: air interface for fixed and mobile broadband wireless access systems amendment for physical and medium access control layers for combined fixed and mobile operation in licensed bands (2005).

[3] Andrews J., Ghosh A., Muhamed R., Fundamentals of WiMAX understanding broadband wireless networking (Prentice Hall, 2007).

[4] Ahson S., Ilyas M., WiMAX standards and security (Aurebach Publications, Taylor & Francis Group, 2008).

[5] Deepak Pareek, WiMAX taking wireless to the MAX (CRC Press, Taylor & Francis Group, 2006).

[6] Zhang Y., Handbook of research on wireless security (Idea Group Publishing, 2008).

[7] Yang F., Zhou H., Zhang L., Feng J., An improved security scheme in WMAN based on IEEE standard 802.16, Proc. of International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM (2005): 1191–1194.

[8] Eklund C., Marks R., Ponnuswamy S., Stanwood K., van Waes N.J.M, WirelessMAN®: inside the IEEE 802.16™ standard for wireless metropolitan area networks (IEEE Standards Information Network, IEEE Press, 2006).

[9] Hasan J., Security issues of IEEE 802.16 (WiMAX) Proc. of 4th Australian Information Security Management Conference (Edith Cowan University, Western Australia, 2006).

[10] Pawłowski M., Matusz P., Woźniak J., WiMAX – nowy standard szerokopasmowych sieci bezprzewodowych 1, Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne 7 (2005): 245–251.

[11] Zawadzki P., Podsystem bezpieczeństwa sieci WiMAX, Przegląd Telekomunikacyjny (2-3)(2007): 67–72.

[12] Cabaj K., Mazurczyk W., Szczypiorski K., Bezpieczeństwo bezprzewodowych sieci WiMAX, Enigma 2007 – XI Krajowa Konferencja Kryptografii i Ochrony Informacji (Warszawa, 2007): 371–326.

[13] Jurkowski K., Nowoczesne technologie: WiMAX jako alternatywa sieci GSM, GPRS I UMTS, MCS thesis, University of Łodz (unpublished, 2007).

[14] Velez F., Carvalho V., Santos D. et al., Aspects of cellular planning for emergency and safety services in mobile WiMAX networks, 1st International Symposium on Wireless Pervasive Computing (Portugal, 2006): 6.

[15] Narayana P., Chen R., Zhao Y. et al., Automatic vulnerability checking of IEEE 802.16 WiMAX protocols through TLA+, 2nd IEEE Workshop on Secure Network Protocols (USA, 2006): 44–49.

[16] Huijie L., Guangbin F., Jigang Q., Xiaokang L., GDKA: A Group-Based Key Distribution Algorithm for WiMAX MBS Security (Springer-Verlag, Berlin, 2006): 310–318.

[17] Taeshik S., Wook C., An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, (Springer-Verlag, Berlin, 2007): 88–97.