2006

Security Issues of IEEE 802.16 (WiMAX)

Jamshed Hasan
Edith Cowan University

DOI: 10.4225/75/57b65b913476d
Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

Security Issues of IEEE 802.16 (WiMAX)

Jamshed Hasan
School of Computer and Information Science,
Edith Cowan University, Australia
jhasan@student.ecu.edu.au

Abstract

Worldwide Interoperability for Microwave Access (WiMAX) is going to be an emerging wireless technology for the future. With the increasing popularity of Broadband internet, wireless networking market is thriving. Wireless network is not fully secure due to rapid release of new technologies, market competition and lack of physical infrastructure. In the IEEE 802.11 technology, security was added later. Iin 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.

Keywords: authentication, authorization, base station, connections, encryption, IEEE 802.16, methods, mobile station, subscriber station, security, standards, WiMAX.

INTRODUCTION

IEEE 802.16 is the Standard to state the radio frequency of fixed Broadband Wireless Access (BWA).WiMAX is the trade name of "IEEE 802.16 Standard". IEEE 802.16 was first planned to offer the last mile for Wireless Metropolitan Area Network (WMAN) with the line of sight (LOS) of 30 – 50 km. It was designed to facilitate WISP's Backhaul, Broadband internet connectivity to proprietary and standards-based Wi-Fi mesh networks, hotspots, residences and businesses. It is featured with QoS for Voice and Video, real-time video conferencing and other services with up to 280 Mbps per base stations. Revised Standard 802.16-2004 provide extended support for non-line-of-sight (NLOS) in 2-11GHz spectrum with mesh connections for both fixed and nomadic users. Lastest IEEE 802.16e Standard, released on February 28, 2006 intends to facilitate mobility in 2-6GHz spectrum within a range of 2 - 5 km. It is expected to provide true broadband for roaming users, which enables the creation of a 'CPE-less' broadband internet, and facilitate access to broadband internet connection for laptops and PDAs with integrated WiMAX technology. Industry experts are forecasting that WiMAX will strengthen business competition between Telecomm industries (GMS, CDMA) and cable broadband companies. Moreover, WiMAX hotspots (IEEE 802.16e) are more likely to replace WiFi hotspots (Patton et al, 2004).

METHODS

The IEEE 802.16 standard is still "on paper" and some methods are under development. Time and scope are the constraints for this paper. Therefore, research has been done based on published materials, literature & journal study, and IEEE publications and mostly from website; however references has been provided wherever necessary. To understand the security aspects of IEEE 802.16 technology, it is required to provide an overview of this standard as a relevant work. In this paper, only MAC and Physical layer of the standard has been discussed shortly. "WiMAX" and "IEEE 802.16 standard" will be used as synonyms.

IEEE 802.16 PROTOCOL LAYER

Physical Layer

WiMAX uses OFDM technology. Orthogonal frequency-division multiplexing (OFDM) allows assigning sub-carriers to different users. It is resilient to multipath that helps to overcome multiple signals hitting the receiver.

In IEEE 802.16-2004 standard, the OFDM signal is divided into 256 carriers and IEEE 802.16e will use Scalable OFDMA. The IEEE 802.16 standard supports wide range of frequencies and the physical layer contains several forms of modulation and multiplexing (Boom, 2004). The modulation methods in the downlink (DL) and uplink (UL) are binary phase shift keying (BPSK), quaternary PSK (QPSK), 16-quadrature amplitude modulation (QAM), and 64-QAM.

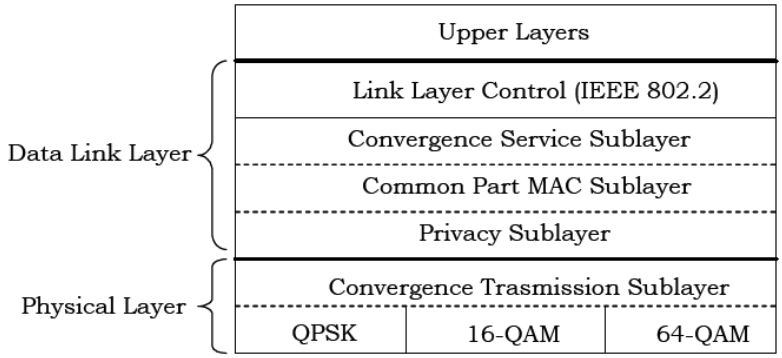

Figure 1: IEEE 802.16 Protocol Layer (IEEE, 2004)

The IEEE 802.16 supports two types of transmission duplexing: Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) and support both full and half duplex stations. TDD framing is adaptive, it has a fixed duration, which consists of one Uplink and one Downlink frame. BS sends the complete downlink subframe (DL-MAP, UL-MAP). Both Up and Down link transmission share same frequency but are separated on time. In FDD, while transmissions are still scheduled by DL-MAP and UL-MAP, uplink and downlink communications take place at the same time, but on different frequencies (Boom, 2004). Some device manufacturers produce, devices operating in unlicensed frequency bands which will use time-division duplexing (TDD) and devices using licensed frequency bands which uses either TDD or frequency-division duplexing (FDD) (INTEL, 2006).

Frame duration can be set to 0.5, 1 or 2 milliseconds. In TDD, the portion allocated for the downlink and portion allocated to the uplink may vary. The Uplink is time division multiple access (TDMA) where bandwidth is split into time slots. Each time slot is allocated to an individual MS being served by the BS. A downlink sub frame contains two parts. One part is for control information, which holds preamble for frame synchronization & maps and the other contains data. A Downlink map states the starting position and transmission attributes of the data bursts. An Uplink map states the allocation of the bandwidth to mobile station (MS) for their communication (Barbeau, 2005).

IEEE 802.16 MAC

802.16 MAC is connection oriented. The MAC Layer of IEEE 802.16 was designed for point to multipoint (PMP) broadband wireless access applications (IEEE, 2004). IEEE 802.16 standard is made up of a protocol stack with properly defined interfaces. There is a Base Station (BS) as the Access Points in 802.11 and several Subscribers Stations (SS). BS is basically wired, and it broadcasts to the Subsciber Stations (SS). In contrast to 802.11 CSMA/CA method, 802.16 uses Uplink and Downlink maps to confirm collision free access. SS uses Time Division Multiple Access (TDMA) to share the uplink, while BS uses TDM (Time Division Multiplexing). All these functions are done through UL-MAP and DL-MAP messages (Aikaterini, 2004).

MAC layer consists of three sub layers. Service Specific Convergence Sublayer (MAC CS), the MAC Common Part Sublayer (MAC CPS) and the privacy sublayer. The MAC CS sublayer is to converse with higher layers and transforms upper-level data services to MAC layer flows and associations. MAC CS has two types of sublayers: one is ATM convergence sublayer for ATM networks & services and the other one is Packet Convergence sublayer for packet data services for example, Ethernet, PPP, IP and VLAN (Aikaterini, 2004). The basic

function of CS Layer is that it receives data from higher layers, classifies data as ATM cell or packet and forwards frames to CPS layer (Liu, 2004).

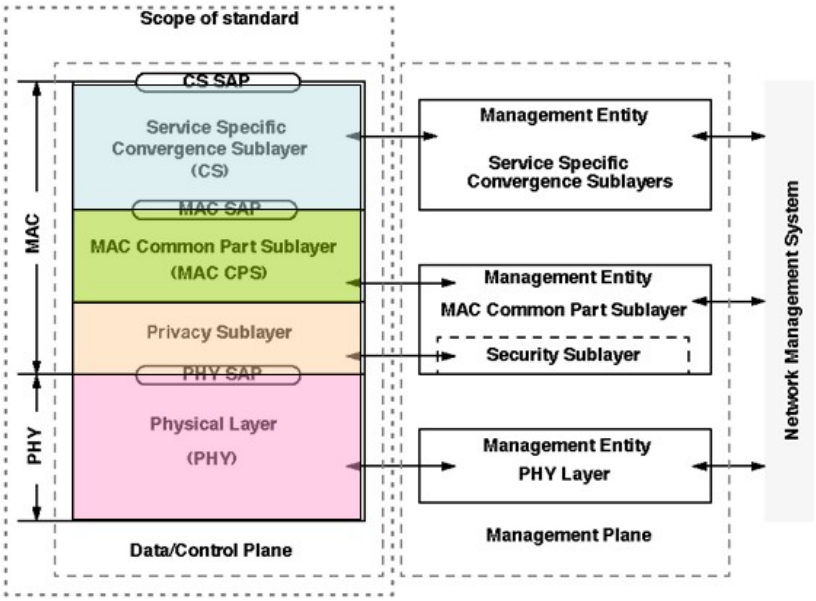

Figure 2: IEEE 802.16 MAC and Physical Layer (Liu, 2005)

The core part of the IEEE 802.16 MAC is the MAC CPS, which defines all methods for connection management, bandwidth distribution, request & grant, system access procedure, uplink scheduling, connection control, and automatic repeat request (ARQ). Communication between the CS (Convergence Sublayer) and the MAC CPS are maintained by MAC Service Access Point (MAC SAP). Creation, modification, deletion of connection and transportation of data over the channel are four the basic functions occuring in this communication process (Aikaterini, 2004).

The Privacy Sublayer is accountable for the encryption and decryption of data that is coming and leaving the Physical layer. It is also used for authentication and secure key exchange. It carries 56-bit DES encryption for traffic and 3-DES encryption for key exchanges (Aikaterini, 2004). In IEEE 802.16 network, the Base Station (BS) has 48-bit base station ID, which is not a MAC address and Service Station (SS) has 48-bit 802.3 MAC address (Liu, 2005).

From a security point of view, MAC CPS (Common Part Sublayer) and MAC PS (Privacy Sublayer) have wide responsibility. Note that in this paper MAC will refer to the MAC CPS Sublayer.

MAC Layer

The 16-bit connection identifier (CID) used in MAC PDU (Protocol Data Units), functions as a reference for all connections and is constantly granted bandwidth on demand (Eklund et al, 2002). There are two types of MAC connection: one is Management connection and the other is Transport connection. MAC layer connections are like TCP connections. For example the SS can have several connections to a BS for different services, like for network management or for data transport. In MAC, all associations use different parameters for priority, bandwidth and security. BS always assigns CID for SS. As soon as a SS joins a network, three different CIDs are allocated to it. Moreover, each CID has separate QoS requirements, which are used by different management connection levels: Primary (authentication and connection setup), Basic (used to transfer brief, time-critical MAC and Radio Link control messages) and Secondary Management connections (transfer standards-based management messages i.e. DHCP, TFTP, and SNMP). Both basic and primary management connections are created when a MS (Mobile station)/SS is joined to a BS network. Transport connections can be established on demand. They are used for user traffic flows, unicast or multicast transmission. Additional channels are also reserved by the MAC to send out uplink and downlink schedule. A single CID can carry traffic for many

different higher-layer sessions. The IEEE 802.16 MAC Layer is a stateful machine. It has series of state machines to determine the operation of individual process within the MAC structure (Boom, 2004).

Format of MAC Messages

MAC Protocol Data Units (MPDUs) contains exchange messages of BS MAC and SS MAC. It has three parts: a fixed length MAC header, which contains frame control information; a variable-length Payload (frame body) and a frame check sequence (FCS), which holds IEEE 32-bit CRC (Liu, 2005). Again, MAC header types are: MAC Service Data Unit (MSPU), where payloads are MAC SDUs/segments, i.e., data from the upper layer (CS PDUs). Second one is, Generic MAC header (GMH) where the payloads are MAC Management messages or IP packets encapsulated in MAC CS PDUs. Both are transmitted on management connections (Liu, 2005). The third one is Bandwidth Request Header (BRH) which is sent out without payload.

Except the Bandwidth Request PDUs, MAC PDUs may hold either MAC management messages or convergence Sublayer data- MSDU. For both GMH and MSDU, Header Type (HT bit) is always set to 0 (zero) while Bandwidth Request Header is set to 1 (one). The MAC header contains a flag, which indicates whether the payload of the PDU is encrypted or not (Barbeau, 2005).

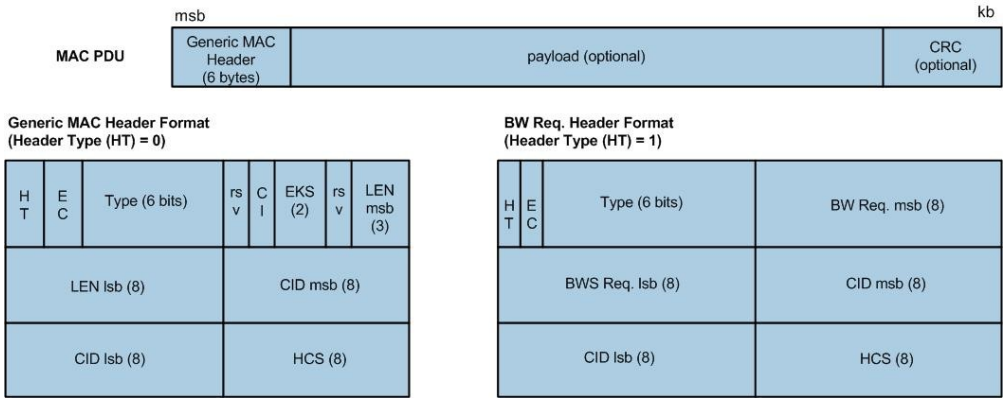

Figure 3: MAC PDU Field description (Liu, 2005)

According to IEEE Standard 802.16-2001, MAC header and all MAC management messages are not encrypted. This decision was made to "facilitate registration, ranging and normal operation of the MAC sublayer" as it allows generation of false management messages. Consequently, this leads to vulnerabilities, otherwise if encrypted, spoofing was difficult during BS and SS had exchanged encryption keys (Boom, 2004). In case of vulnerabilities in management messages, authentication will be exposed to eavesdropping, man in the middle attacks, active attacks and replay attacks. In the latest IEEE 802.16e standard, the payload of MAC PDUs is encrypted with DES in the CBC mode or AES in the CCM mode (IEEE, 2006). The amended 802.16e introduces an integrity protection mechanism for data traffic.

The EKS (Encryption Key Sequence) field is used to make sure that the BS and SS are synchronized in their use of Traffic Encryption Keys (TEK) and Initialization Vectors (IV). When a SS joins a BS network, it follows a multi-step process. And when the SS detects an active connection it transmits its presence to BS through a Range Request (RNG-REQ) message. The SS and BS continue their conversation via RNG-REQ and RNG-RSP messages using newly assigned basic CID by BS. BS replies with REG-RSP message describing the supported capabilities. SS acknowledges the REG-RSP with REG-ACK message (Boom, 2004).

Privacy Sublayer:

Two main protocols work in this security sublayer, one is an encapsulation protocol for encrypting packet data across the fixed BWA, and the other is a Privacy and Key Management Protocol (PKM) providing secure distribution of keying data from BS to SS. It also enables BS to impose conditional access to network services.

The PKM protocol uses, RSA public-key algorithm, X.509 digital certificates, and strong encryption algorithm to carry out key exchanges between SS and BS (Xu et al, 2006). This Privacy protocol is based on the PKM protocol of the DOCSIS BPI+ specification; it has been enhanced to accommodate stronger cryptographic methods such as AES to fit into the IEEE 802.16 MAC. (Eklund et al, 2002).

The entire security of IEEE 802.16 is in the privacy sublayer. The function of this sublayer is to provide access control and confidentiality of the data link. Security Associations (SA) is identified by SAID, which contains, Cryptographic suite (i.e., encryption algorithm) and Security Info (i.e., key, IV). The basic and primary management connections do not have SAs. The secondary management connection can have an optional SA. Transport connections always have SAs.

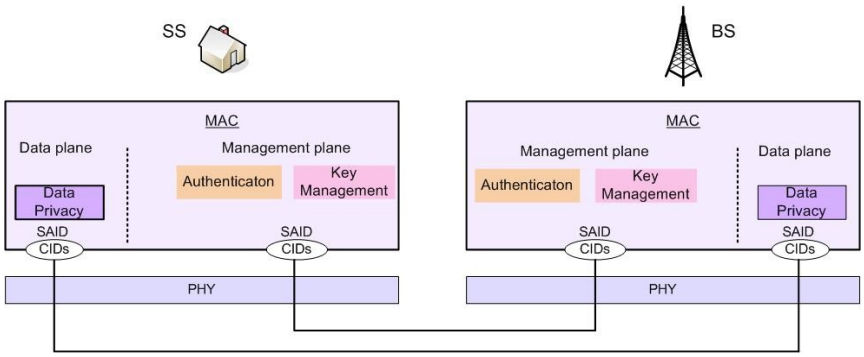

Figure 4: IEEE 802.16 Security Associations (SA), (Aikaterini, 2004)

Data SA (Security Associations)

Data SA has a 16-bit 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. When the current key expires, TEK a 2-bit key identifiers is used. A 64-bit initialization vector (IV) is used for each TEK. The lifetime of TEK is between 30 minutes to 7 days. There are three types of data SA: Primary SA is used during link initialization, static SAs are configured on the BS and dynamic SAs are used for transport connections when needed. The primary SA is shared between an MS and its BS. Static SAs and dynamic SAs can be shared among several MSs (Mobile stations) during multicast. During the connection process, SA first starts a data SA using a connection request function. A SS generally has two or three SAs, one is the secondary management connection and one is for both uplink and downlink connections; it may use separate SAs for uplink and downlink channels (Johnston & Walker 2004). BS ensure that each SS has access only to SA its authorized.

Authorization SA (Authentication)

The authorization SA has a 60-bit authorization key (AK) and a 4-bit quantity to identify the AK. To identify SS, it uses an X.509 certificate. The lifetime of AK ranges from 1 to 70 days, default is 7 days. Key encryption key (KEK) has a 112-bit 3DES key for distributing TEKs (Temporal encryption key) and a list of authorized data SAs. It uses a downlink & uplink HMAC (Hash function-based message authentication code) key providing data authenticity of key distribution messages from the BS to SS and SS to BS respectively. An authorization SA state is shared between a particular BS & SS. Base stations use authorization SAs to configure data SAs on the SS (Johnston & Walker 2004).

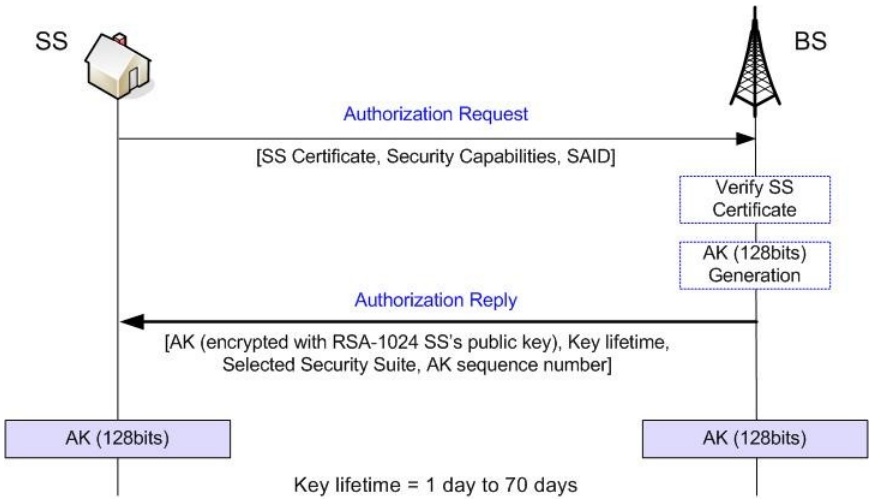

Figure 5: IEEE 802.16 Authentications, (Wongthavarawat, 2005)

SS authentication uses X.509 certificate (Privacy Key Management (PKM) authorization protocol and encryption) negotiate security capabilities between BS and SS, which establish security association (SAID) through Authentication Key (AK) exchange. AK serves as authorization token, which is encrypted using public key (RSA) cryptography. Authentication is done when both SS and BS possess AK (Wongthavarawat, 2005).

Data Key Exchange

Data encryption requires data key called Transport Encryption key (TEK), which uses AK from authentication process to derive Key Encryption Key (KEK) and Message Authentication Key (HMAC key). TEK is generated by BS randomly. TEK is encrypted with 3DES (use 112 bits KEK), RSA (use SS's public key) and AES (use 128 bits KEK). Key Exchange message is authenticated by HMAC-SHA1, which provides Message Integrity and AK confirmation (Wongthavarawat, 2005).

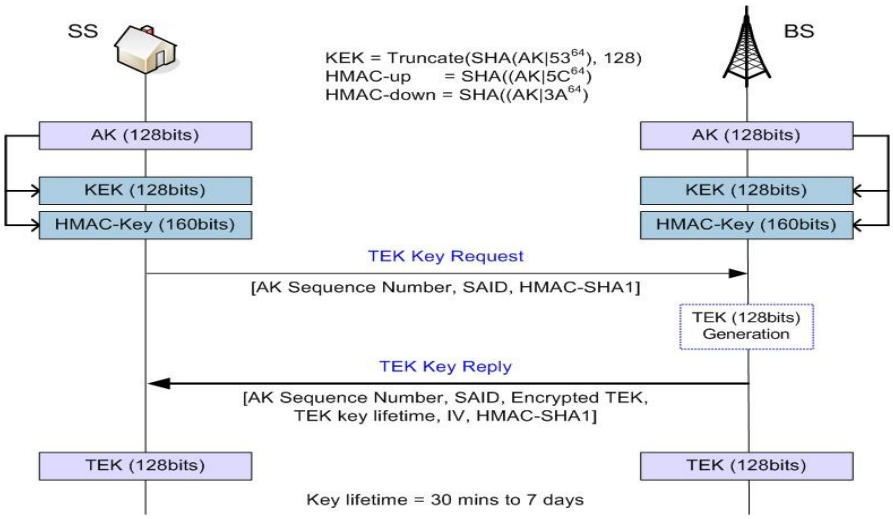

Figure 6: IEEE 802.16 IEEE 802.16 Data Key Exchange , (Wongthavarawat, 2005)

SECURITY RISKS & VULNERABILITIES

In wireless networks, confidentiality is a primary concern for secure transmission. Resistance to interception and eavesdropping are other common threats. Message authentication is for integrity of the message and sender authentication. Availability guarantees that the services are not prevented from access by DoS attack. Anti-replay identifies and disrepute any message that is a repeat of a past message (Xu et al, 2006).

According to Xu, Matthews and Huang (2006), there are some typical attacks on authentication protocols. One common attack is Message replay attack on authentication and authenticated key formation protocols. They added, "If the messages are exchanged in an authentication protocol that do not carry proper freshness identifiers, then an opponent can easily get himself authenticated by replaying messages copied from a legitimate authentication session". Man-in-the-middle attack usually associated in a communication protocol where common when mutual authentication is missing. Other known attacks that are likely to occur include parallel session attack, reflection attacks, interleaving attacks, attacks due to type flaw, attacks due to name omission, and attacks due to misuse of cryptographic services.

Physical Layer & Privacy Sublayer

In IEEE 802.16 standard, Privacy Sublayer resides on the top of Physical layer. Therefore, 802.16 networks are vulnerable to physical layer attacks for example, jamming and scrambling. Jamming is done by instigating a source of strong noise to significantly lessen the capacity of the channel, thus denying services (DoS) to all parties. However, jamming is detectable with radio analyzer devices. Scrambling is another kind of jamming, but it takes place for a short interval of time aimed at specific frames. Control or management messages could be scrambled, but it is not possible with delay sensitive message i.e., scrambling Uplink slots are relatively difficult, because attacker has to interpret control information and to send noise during a particular interval (Barbeau, 2005).

The main objective of the Privacy Sublayer was to protect service providers against theft of service, rather than guarding network users. It is noticeable that the privacy layer only guards data at the OSI layer two (data link), whereas it does not ensure end-to-end encryption of user data. Moreover, it does not protect physical layer from being intercepted (Boom, 2004). It is necessary to include technologies to secure physical layer and higher layer security for a converged routable network.

Identity theft is another threat, which is reprogramming a device with the hardware address of another device. The address can be stolen over the air by intercepting management messages. A rogue BS is an attacker station which act as a legitimate BS. It confuses a set of SSs/MSs when attempting to get service through what they believe being a legitimate BS. It is difficult in 802.16 network because of time division multiple access (TDMA) model. In this case, the attacker must transmit while the real BS is transmitting, with more signal strength and place the real BS's signal in the background, moreover attacker has to capture the identity and wait until a time slot of legitimate BS starts (Barbeau, 2005).

In wireless world some threats are generic; IEEE 802.16 is not an exception. A classic threat arises from the water torture attack, in which an attacker sends a series of frames to drain the receiver's battery. In addition, attacker with a properly positioned RF receiver can intercept messages sent through wireless, and thus a confidentiality mechanism in the design is required. Present security mechanisms do not address well in IEEE 802.16a Mesh modes network, which lead into new security threats, such as the trustworthiness of the next-hop mesh node. Introducing mobility in IEEE 802.16e standard will make the attacker's life comfortable. As the physical location of the attacker is not an issue, management messages are more vulnerable than in IEEE 802.11. Therefore, it is necessary to maintain a secure connectivity while a mobile SS shifts between BSs (Johnston & Walker, 2004).

With a properly configured RF transmitter, an attacker can write to a RF channel, forge new frame and capture, mutate, and re-transmit frames from authorized edge. The design must ensure a data authenticity technology. It is also possible to resend a valid, already-sent frame unmodified. In case of long distance transmission, radio interference and distance could permit an attacker to reorder and selectively forward frames, in a situation where

two authorized edges are not able to contact directly with each other. Therefore, the design must detect replayed frames (Johnston & Walker, 2004).

Mutual Authentication

Two types of certificate are classified by IEEE 802.16 standard: one is for manufacturer certificates and the other is for SS certificates. There is no provision for BS certificates. A manufacturer certificate identifies the manufacturer of an IEEE 802.16 device. It can be a self signed certificate or issued by a third party. A SS certificate identifies a particular SS and includes its MAC address in the subject field. Manufacturers typically create and sign SS certificates. In general the BS uses the manufacturer certificate's public key to verify the SS certificate, and hence identify the device as genuine. This design assumes that the SS maintains the private key corresponding to its public key in a sealed storage, preventing attackers from easily compromising it. The big flaw of the IEEE 802.16 security design is the lack of a BS certificate. The only way to defend the client against forgery or replay attack is to provide a scheme for mutual authentication (Johnston & Walker 2004). It's supported by Wongthavarawat (2005), "No mutual authentication is provided, which is vulnerable to rogue BS man-in-the-middle attack and SS certification is a limited authentication method." In 802.16e, EAP can be actualized with specific authentication methods such as EAP-TLS (X.509 certificate-based) (Barbeau, 2005).

Unclear Definitions

IEEE 802.16 design failed to explicitly define the authorization SA, for instance, state of the SA never differentiates one authorization SA instance from another, which is vulnerable to replay attacks. This will become a significant issue when IEEE 802.16e will facilitate mobility and roaming. Also, SS cannot identify reused data SAs. Thus the encryption scheme is vulnerable to attack via encryption key reuse. In addition, the authorization SA does not contain the BS identity; hence the SS cannot differentiate authorized from unauthorized BSs. Here we can assume that, hiding it from SS prevents key management and encryption, from protecting the SS from forgery and replay attacks. One solution against the replay vulnerability is to include a random value generator from the BS and SS to the authorization SA. In the latest IEEE 802.16e standard, this modification could happen. The protocols presume that no parties with different public or private key pairs are certified to employ same MAC address, condition must be explicitly defined that all certified MAC address is unique to avoid MAC masquerading problem (Johnston & Walker, 2004).

Data Privacy

In IEEE 802.16, it uses DES in CBC mode for data privacy. DES in CBC (Cipher Block Chaining) mode uses 56-bit DES key (TEK) and CBC-IV (Initialization Vector). CBC mode requires a random initialization vector to secure the Scheme (RSA, 2004). Continued with previous discussion Wongthavarawat (2005) said, that CBC-IV is predictable i.e, *CBC-IV = [IV Parameter from TEK exchange] XOR [PHY Synchronization field]* and 56 bit key is not secure based on today's computing and fails to provide strong data confidentiality, hence it is vulnerable to Bruce force attack to recover the original plaintext. In addition, there is no provision for message integrity detection, which increases the possibility of active attack. Another statement from Johnston and Walker, (2004) "Because the SA initialization vector is constant and public for its TEK, and because the PHY synchronization field is highly repetitive and predictable, the MPDU initialization vector is also predictable. IEEE 802.16 provides no data authenticity."

IEEE 802.16e adopted AES-CCM using 128bit key (TEK) as a new data cipher, which ensures message integrity check and replay protection using Packet Number (PN). Transmitter construct a unique nonce as a per-packet encryption randomizer, guarantee uniqueness and adds data authenticity mechanism (Wongthavarawat, 2005).

Key Management

In IEEE 802.16 standard it has key management protocol problem, which is its use of TEK sequence space; it uses sequence number to differentiate messages. The protocol recognizes each TEK with a 2 bit sequence number, enfolding the sequence number from 3 to 0 on every fourth rekey as an issue of replay attack; if replay

works, SS could not be able to detect this. Johnston and Walker (2004) said, “Encryption reuses the TEK and initialization vector in the encryption, exposing both the TEK and the subscriber data”

Other Vulnerabilities

In the data SA definition, an AK can last for up to 70 days, whereas a TEK lifetime can be as short as 30 minutes, allowing an attacker to interject reused TEKs. A data SA can consume up to 3,360 TEKs over the AK’s lifetime requiring the SAID space to grow from 2 to at least 12 bits. IEEE 802.16 design means the SS must trust that the BS always generates a new AK, which is another weakness as the BS contributes all of the bits in an AK so that BS’s random number generator must be perfect, if biased the AK and TEKs could be exposed.

In IEEE 802.16, it does not mention that authenticating the BS to the SS allows the PKM protocol vulnerable to forgery attack. For example SS cannot verify that any authorization messages it receives were coming from authorized BS. The BS respond to SS using public information, so any rogue BS can create a response. As we discussed earlier, the protocol’s failure allows participants to distinguish one instance of the protocol from another, therefore, the authorization protocol subjects the SS to replay attacks.

CONCLUSION

The new IEEE 802.16e standard has changed several security mechanisms like, generating each per-frame IV (Initialization Vector) randomly, replaying protection using Packet Number (PN). It will use AES (Advanced Encryption Standard) as a main encryption method and introduce a flexible authentication method based on the Extensible Authentication Protocol i.e., EAP-TLS, EAP-TTLS, PEAP, EAP-SIM, which extends the authentication to AAA server. AES-CCM mode is a new data link cipher for data authenticity mechanism, which is specified by NIST (National Institute of Standards and Technology). The standard also, replaces Triple-DES key wrapping in the PKM protocol with the AES-ECB mode and facilitates low cost re-authentication during roaming. Further research is required to find out security threats and vulnerabilities in the IEEE 802.16e standard.

Security mechanism is an expensive process; it requires extensive level of research, performance evaluation and implementation outcomes. The IEEE 802.16e will open the door for wireless mobility, vulnerability as well, because there are be no constraints for an attacker. In such a situation, more issues like, BS to BS key management, roaming user authentication & voice migration will arise. IEEE 802.16 (WiMAX) has the capability to attain success in wireless communication arena. Though, wireless vendors have already marketed their WiMAX product, this technology is still under development; and need more academic research and time to achieve a maturity level. Therefore, business organization, service provider and IT professionals should take great care before deployment of this new technology.

REFERENCES

Aikaterini, A.V. (2004). *SECURITY OF IEEE 802.16*, retrieved on 1st May, 2006 from http://www.dsv.su.se/research/seclab/pages/pdf-files/2006-x-332.pdf

Barbeau, M. (2005). *WiMax/802.16 Threat Analysis,* retrieved on 1st May, 2006 from

http://www.scs.carleton.ca/~barbeau/Publications/2005/iq2-barbeau.pdf

Boom, D.D. (2004). *Denial of Service Vulnerabilities in IEEE 802.16 Wireless*

Networks, retrieved on 1st May, 2006 http://www.ieee802.org/16/tge/contrib/C80216e-04_406.pdf

Barry, A., Healy, G., Daly, C., Johnson, J. & Skehill, R.J. (2006). *Overview of Wi-Max IEEE 802.16,* retrieved on 1st May, 2006 from

http://www.mais-project.it/documenti_pubblico/IIIsemester/r4.1.2.pdf

Chou, H. (2004). *802.16 & 802.11 Security Overview,* retrieved on 1st May, 2006 from

http://lee-1.com/hlchou/802.16e%20Security_1.2.pdf

Eklund, C., Marks,R.B., Stanwood, K.L., & Wang, S.(2002) *IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access,* retrieved on 1st May, 2006 from

Guice, R.J. & Munoz, R.J. (2004). *IEEE 802.16 Commercial off the shelf (cots) Technologies as a compliment to ship to objective Maneuver Communications,* retrieved on 1st May, 2006 from http://web1.nps.navy.mil/~budden/lecture.notes/r-wan/Guice_Munoz_thesis.pdf

IEEE, (2006). *Part 16: Air Interface for Fixed Broadband Wireless Systems,* retrieved on 1st May, 2006 http://standards.ieee.org/getieee802/download/802.16-2004.pdf

IEEE, (2001), *IEEE Standard 802.16-2001,* retrieved on 1st May, 2006 from, http://standards.ieee.org/getieee802/download/802.16-2001.pdf

Intel, (2005). retrieved on 1st May, 2006 from http://download.intel.com/technology/itj/2004/volume08issue03/vol8_iss03.pdf

Johnston, D., Walker, J. (2004). *Overview of IEEE802.16 Security*, retrieved on 1st May, 2006 from http://mia.ece.uic.edu/~papers/WWW/Bubbles/segment/WiMax_Security.pdf

Liu, F. (2004). *IEEE 802.16 WiMAX* , retrieved on 1st May, 2006 from http://www.seas.gwu.edu/~cheng/388/LecNotes2006/80216WiMAXSecurity.ppt

Parekh, S. (2006) *IEEE 802.16 / WiMAX*, retrieved on 1st May, 2006 from

http://walrandpc.eecs.berkeley.edu/228S06/L6.pdf

Patton, K.B., Aukerman, R., & Shorter J.D. (2004) *Wireless technologies, Wireless Fidelity (wi-fi) & Worldwide Interoperability for Microwave Access (WiMAX),* retrieved on 1st May, 2006 from

http://www.iacis.org/iis/2005_IIS/PDFs/Patton_Aukerman_Shorter.pdf

RSA, (2004). *RSA Cryptography Standard, RSA Public Key Cryptography*

Standard #1 v. 2.0, retrieved on 1st May, 2006 from www.rsasecurity.com/rsalabs/pkcs/pkcs-1/

Wongthavarawat, K. (2005). *IEEE 802.16 WiMax Security,* retrieved on 1st May, 2006 from

http://www.nectec.or.th/nac2005/documents/20050328_SecurityTechnology-05_Presentation.pdf

WiMAX Forum, (2006). *Fixed, nomadic, portable and mobile applications for 802.16-2004 and 802.16e WiMAX networks,* retrieved on 1st May, 2006 from http://www.wimaxforum.org/news/downloads/Applications_for_802.16-2004_and_802.16e_WiMAX_networks_final.pdf

Xu, S., Matthews, M. & Huang, C. (2006). *Security Issues in Privacy and Key Management Protocols of IEEE 802.16,* retrieved on 1st May, 2006 from http://www.cse.sc.edu/~huangct/acmse06cr.pdf

Yaghoobi, H. (2003). *802.16 Broadband wireless access: the next big thing in*

Wireless, retrieved on 1st May, 2006 http://cnscenter.future.co.kr/resource/rsc-center/presentation/intel/fall2003/F03USWNTS111_OS.pdf

COPYRIGHT