12-5-2006

An assessment of threats of the Physical and MAC Address Layers in WiMAX/802.16

Krishnun Sansurooah
Edith Cowan University

DOI: 10.4225/75/57b6601234773
4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

An assessment of threats of the Physical and MAC Address Layers in WiMAX/802.16

Krishnun Sansurooah
School of Computer and Information Science (SCIS)
Edith Cowan University Perth, Western Australia.
Email: ksansuro@student.ecu.edu.au

Abstract

This paper investigates the risks and vulnerabilities associated to the security of the WiMAX/802.16 broadband wireless technology. One of the other aspects of this document will be to review all the associated weaknesses to the Medium Access Control (MAC) layer and at the physical (PHY) layer. The risks and impacts are assessed according to a systematic approach. The approach or methodology is used is according to the European Telecommunication Standards Institute (ETSI). These threats are enumerated and classified accordingly to their risk levels.

Keywords

Wireless, Wi-Fi, WiMAX, 802.16, Potential threats, Wireless Broadband Access.

INTRODUCTION

In the modern era, high volume and open standard radio technology (802.11, 802.16, 802.30, Wi-Fi, WiMAX and future standards) offer exceptional benefits to network operators and users.

The 802.16 standard amended January 2006 by the Institute of Electrical and Electronics Engineers (IEEE) covers frequency bands in the range of 2 GHz and 11 GHz compared to the previous parameters of 10 GHz to 66 GHZ. The amended standard specified a metropolitan area networking (MAN) protocol that enhances and enables an alternative for cable, DSL, T1. The new 802.16a standard specifies a convention that establishes low latency application, such as voice and video. This protocol provides connectivity without having access to a direct line-of-sight (LOS) between subscribers and base station (BS).

This document defines wireless access technology being in association with WiMAX with respect to all the other wireless technologies such as IP-based mobile and wireless access.

According to the IEEE Communication Magazine (2002), the IEEE Standard 802.16 completed in the late 2001 and published on April 2002 defines on air interface requirement for the wireless networks. Air interface for fixed point-to-multipoint (P2MP) was possible by the completion of this specific standard. The IEEE 802.16 offers an alternative to cabled access networks, such in the instance of fiber optic, coaxial systems and digital subscriber line (DSL).

The IEEE Communication Magazine (2002), initially the LOS transmission was between the range of 10 GHz and 66 GHz but following two published amendments, namely IEEE 802.16c which defines profiles of typical implementations, and IEEE 802.16a, which consists of managed improvement and the development of a mesh mode. It also allowed capacity to carry additional frequencies. These subsequent amendments then enabled transmission in the range of 2 GHz to 11 GHz on a non line-of-sight (NLOS) transmission for both licensed and unlicensed services.

One of the major revisions was published in 2004 as IEEE 802.16d compiling and enhancing both IEEE 802.16a and IEEE 802.16c. This defined the added mechanism to maintain mobile subscribers at vehicular pace and also for data validation.

This document presents an in depth scrutiny of the spectrum of the security threats to the WiMAX/802.16. The aim of this paper is to reflect the most recent threats to the wireless access systems. All the vulnerabilities are assessed with respect to the probability of it happening, the resultant effect together with the actual feasible impact on individual users and the system, and the overall weakness it represents.

METHODOLOGY

To analyze the different threats planning around the IEEE Standard 802.16, a structured methodological approach needs to be considered in order to test and evaluate the probability of occurrences to happen, the impacts associated to those occurrences and finally, the risks involved. The best approach in conducting this measure is to adopt the European Telecommunication Standard Institute (ETSI). It is noted that the analysis is carried out according to the ETSI version 2003. Table 1 illustrates a clear summary of this methodology.

Table 1: Risk Assessment (WiMAX/802.16 Threat Analysis, 2005)

CRITERIA	*CASES*	*DIFFICULTY*	*MOTIVATION*	*RANK*
Probability	*Unlikely*	*Strong*	*Low*	*1*
	Possible	*Solvable*	*Reasonable*	*2*
	Likely	*None*	*High*	*3*
CRITERIA	*CASES*	*USER*	*SYSTEM*	*RANK*
Impact	*Low*	*Annoyance*	*Very Limited Outages*	*1*
	Medium	*Loss of Service*	*Limited Outages*	*2*
	High	*Loss of Service*	*Long time Outages*	*3*
Risk	*Minor*	*No Need for Countermeasure*		*1, 2*
	Major	*Threat Needs to be Handled*		*3, 4*
	Critical	*High Priority*		*6, 9*

Referring to the table above, the assessment is carried out according three factors; probability, impact, and the risks involved.

The probability evaluates the likeliness that attacks are associated to the threats conducted. When considering the probability of attacks to occur, the two factors to consider are:

1. The technical difficulties that need to be resolved by an attacker and,
2. The motivation for accomplishing it's attack

When the probability of attack is 'Low' there are either multiple technical barriers to overcome with unidentified uncertainties, and/or there is a low motivation factor for accomplishing an attack of that category.

The probability can be 'Possible' only if there are defined technical difficulties but manageable due to the availability of the necessary information, or if there are practical reasons for the hacker to construct then lead the attack.

A 'Likely' probability is to occur when there are no technical barriers to overcome thus providing the attacker with a high motivation to engage in an attack.

The impact factor analyzes and indicates the effects of an attack which is related to the threat. Depending on the severity of the attack, the impact may be classified as Low, Medium or High.

The impact is defined as 'Low' where there are reversible or repairable actions, the service disruption is short or the number of users affected a minimal.

A 'Medium' impact can affect only one user and have a consequential loss of usage over a period of time. In relation to the system, the impact is medium when the outage is restrained. A medium impact may cause limited financial setback.

When the loss of system usage is over a considerable length of time to a single user, defined as long to the organization, the impact is 'High'. A long outage of the system is high also. There may be numerous users unable to access the system, severe financial loss and/or illegal offences.

To enable objective analysis of the probability and the impact of the threat, the different categories as defined above can be numerically graded. When multiplying the grade of the probability and the impact level, the result is the valid risk. Any risk value of one or two is a minor threat with no real contingency planning required. Any risk valued as three of four is major and requires plans for business continuity. A risk to the value of six or greater is critical and immediate countermeasures are to be prioritized. Using the ETSI methodology as outlined above is impartial and non-biased. It is an objective approach to prioritize the preventative remedies.

ANALYSIS

A WiMAX/802.16 wireless access network consists of base stations (BS) and of mobile stations (MS). The MSs are networked by the BSs by searching for the strongest BS signal to attach to. A subscriber is a system user, while the BS and multiple MSs are the system.

The structure of WiMAX/806.12 consists of two core tiers, the Medium Access Control (MAC) and the Physical Layer (PHY). There are Service Access Points (SAPs) defined at different levels of the WiMAX architecture. MAC Protocol Data Units (PDUs) are formed in the Common Part sublayer which is at the central core of the system. After being assembled, the connections of MAC PDUs are created and bandwidth is administered. MAC Service Data Units (SDUs) are interchanged with the Convergence Layer enabled in the Common Part. The Security sublayer is firmly incorporated with the Common Part. The Security sublayer role is to authenticate and establish keys and encryption. MAC PDUs must be verified by the Security layer to enable successful exchange with the Physical Layer. Higher level protocol data units are transformed to and from the MAC SDU format at the Convergence Layer, which also directs the MAC SDUs to the appropriate connection. The Physical Layer has a dual direction mapping function between the MAC PDU and Physical layer RF transmissions.

Security threats at the Physical and MAC layers are investigated of which Table 3 illustrates the threat risk to user and system respectively (when there are two values listed) or indicating the same value for both (when there is only one value).

WIMAX & THE PHYSICAL LAYER

The first version of the 802.16 standard has a physical layer (PHY) specification for 10 to 66 GHz addressing LOS environment at high frequency bands, whereas the amendment version of 802.16a has been designed for systems operating on bands between 2 to 11 GHz. One of the major advantages of this difference between the two frequencies is that the latter allows and support NLOS operation in low frequencies, something that is not possible in higher bands. This has been made possible through the introduction of three new PHY layer specifications:

1. Single Carrier Modulation format.
2. 256 point Orthogonal Frequency Division Multiplexing (OFDM) format.

3. 2048 point Orthogonal Frequency Division Multiple Access (OFDMA). The OFDMA allows multiple accesses by acknowledging a subset of the multiple carriers to an individual receiver.

The table below (Table 2) illustrates a list of all the features and the benefits of the physical layer 802.16a

PHYSICAL LAYER DETAILS

According to IEEE Communications Magazine (2002), the PHY attribute defined for 10 to 66 GHz uses burst single carrier modulation with adaptive burst profiling that may be adjusted to the subscriber station (SS) separately each frame one at a time. At the physical layer, the flow of bits is organized as a sequence of frames of equal length.

The physical layer consists of a downlink subframe and an uplink frame and two modes of operation:

a) Frequency Division Duplex (FDD)

b) Time Division Duplex (TDD)

Table 2 Features and benefits of the 802.16 of Physical Layer (PHY) features. (Worldwide Interoperability for Microware Access Forum, n.d)

FEATURES	*BENEFITS*
256 point ODFM	*Built in support for addressing multipath in outdoor LOS & NLOS environment*
Adaptive Modulation and variable error connection encoding per RF burst	*Ensure a robust RF link maximizing the number of lists for each subscriber unit*
TDD & FDD duplexing support	*Address varying worldwide regulation where one or both may be allowed*
Flexible Channel Sizes (eg 3.5, 5, 10 MHz)	*Provides the flexibility necessary to operate in many frequency bands with ranging channel requirement around the world*
Designed to support smart antenna system	*Smart antenna system are becoming more affordable and as those costs come down their ability to suppress interference and increase system gain will become important to Band Wireless Access (BWA)*

Reed-Solomon GF(256) is the type of Forward Error Correction (FEC) used which has a variable block size and error fixing capabilities stated by the IEEE Communication Magazine (2002). Coupled with an inner block convolution code, the FEC steadily broadcast crucial information such as frame control and initial access.

The FEC solutions are integrated with Quadrature Phase Shift Keying (QPSK), 16-state Quadrature Amplitude Modulation (16-QAM) and 64-state QAM (64-QAM) to configure burst profiles of different strength and effectiveness. However, when the last FEC block is left empty, that block can be truncated. When truncating occurs, both the downlink and the uplink which is managed by the BS is exclusively broadcast to the downlink map (DL-MAP) and to the uplink map (UL-MAP) as shown in Figure 1 below.

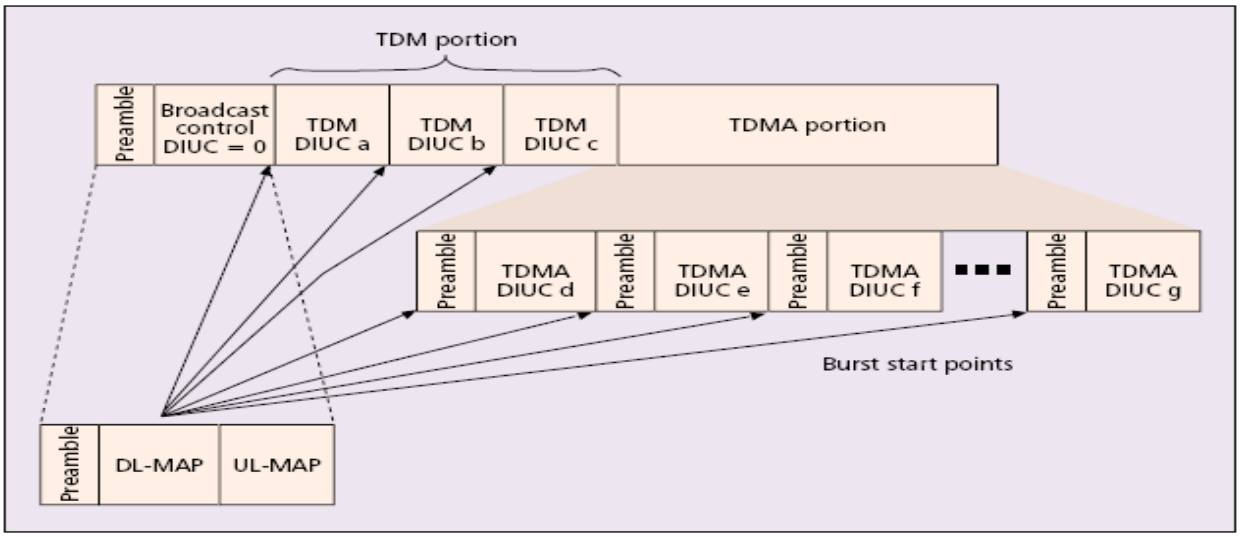

Figure 1. Detailed downlink subframe structure.(IEEE Communication Magazine, 2002)

The system operates a frame of 0.5, 1 or 2 ms which is separated into physical slots for the aim of both bandwidth identification and allocation. A physical slot is characterized as a 4 QAM symbol.

In the FDD variant, the uplink and downlink subframe are timed simultaneously but transmitted on different frequencies whereas in the TDD variant of the physical later, the uplink subframe follows the downlink subframe on the same carrier frequency as shown in the figure below.

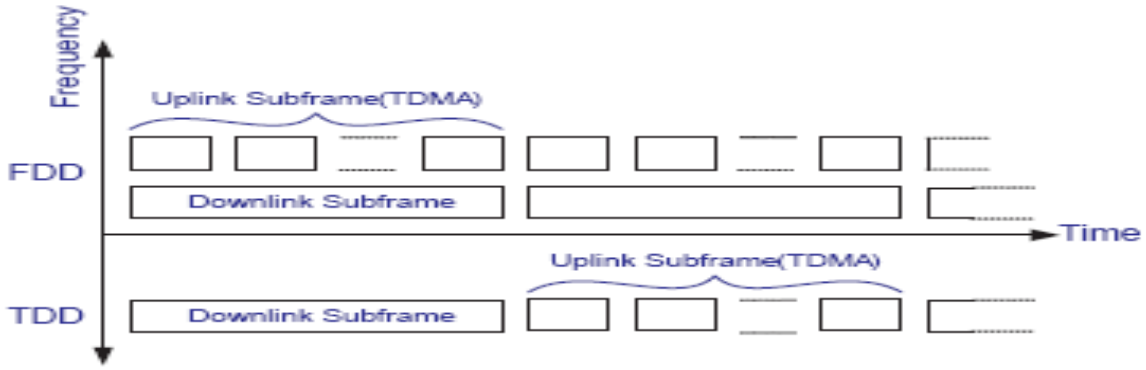

Figure 2. Framing of both TDD and FDD .(WiMAX/802.16 Threat Analysis, 2005)

A comprehensive illustration of a TDD downlink subframe which is defined in figure 3 denotes the burst characteristic of the transmission. There are two main parts to a downlink subframe. The first part holds the frame control section that contains the DL-MAP for the current downlink frame as well as the UL-MAP for a specified time while the second part contains the data. In addition, this section also contains control information consisting of preamble, being the frame synchronization purpose. The downlink map reveals the commencement point and transmission features of data burst whereas the uplink map reveals the allotment of the bandwidth to the MS for the transmission. Each burst is sent in reference to a profile of modulation and a type of FEC which is sent in an

expanding flow of demodulation frequency. Therefore the MS can only accept the bursts while it has the competency of doing so and rejects those that cannot be demodulated.

Figure 3. Detailed Time Division Duplex (TDD) downlink subframe. .(WiMAX/802.16 Threat Analysis, 2005)

PHYSICAL LAYER THREATS

The security sublayer is positioned just above the physical layer enabling it to be unsecured as shown in Figure 4.

Jamming and scrambling can be the form of attack to the PHY as the WiMAX 802.16 is defenseless. Jamming is an interruption of the frequency such as intense noise. It can either be intended or accidental. Resistance to jamming can be increased by raising the signal frequency or intensifying the bandwidth using precise spreading techniques e.g. sequence spread spectrum and frequency hopping. Increasing the power of the signal can be achieved easily by means of using a more powerful transmitter or a high gain transmission antenna and a high gain receiving antenna.

Scrambling is similar to jamming but this happens at small time period and is focused to certain frames or parts of frames. Scramblers can intently effect control or management information with the rationale of disturbing the networks normal operation. This is of grave concern for time sensitive messages which do not have built-in time delay. Examples of this are channel measurement reports requests or responses. Intentional scrambling of data traffic of particular users can cause them to retransmit. 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.

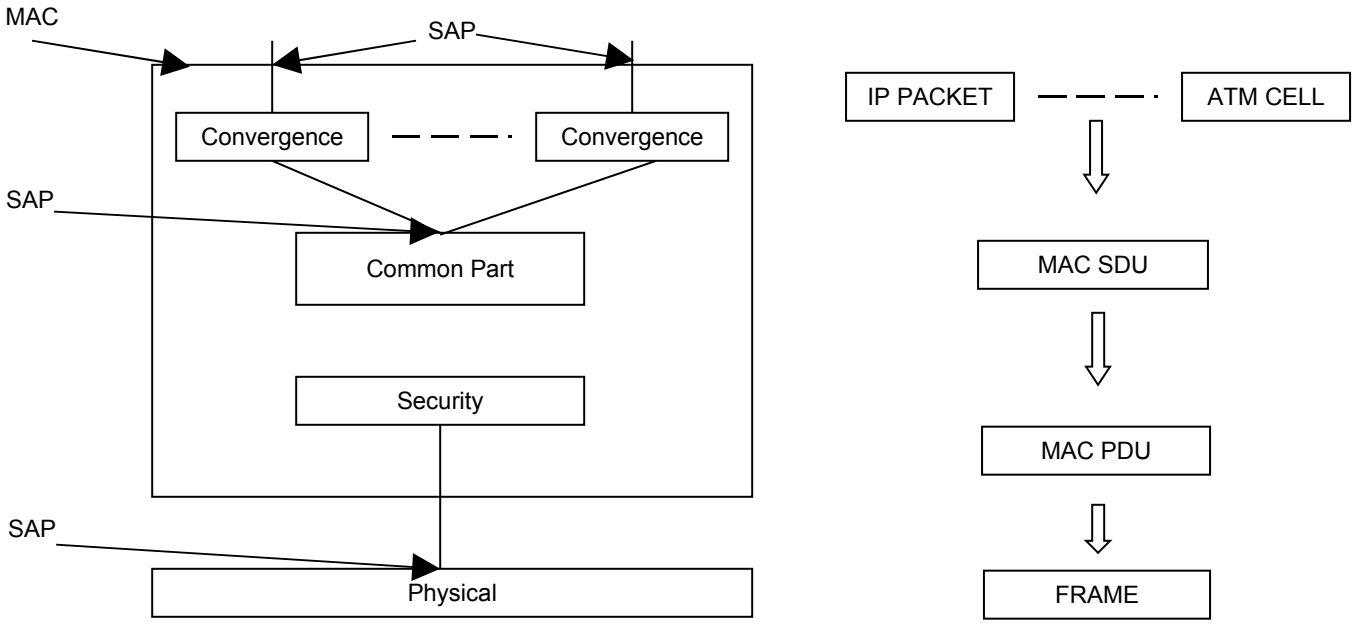

Figure 4. WiMAX 802.16 Layered Architecture .(WiMAX/802.16 Threat Analysis, 2005)

The risk of scrambling is low in comparison to jamming because the attacker has to interpret control information and involves sending noise over the network at specific time interval. The impact of scrambling is low nevertheless results are reversible for example, by retransmission. Jamming is easier to detect, in comparison to scrambling, with the use of a radio spectrum monitoring equipment. The risks associated with jamming are actually quite high as shown in Table 4.

MEDIUM ACCESS CONTROL (MAC) LAYER DETAILS

The Medium Access Control (MAC) normally embeds a service-specific convergence sublayer that interacts to higher levels above the core MAC common part sublayer that includes the key MAC function. The privacy sublayer sits under the common part sublayer.

SERVICE-SPECIFIC CONVERGENCE LAYER

IEEE Standard 802.16 describes two common service-specific convergence sublayers for mapping services to and from the 802.16 MAC connections. The Asynchronous Transfer Mode (ATM) convergence layer is dedicated to ATM facilities whereas the packet convergence layer is accountable for mapping conventions and protocols. The crucial role of the sublayer is to organize Service Data Units (SDUs) to the accurate MAC connection, to facilitate and provide Quality of Service (QoS), and to establish bandwidth allocation. As well as these basic functions, the convergence sublayer also has the ability to achieve highly intricate tasks such as the reconstruction and suppression payload header to boost airlink performance.

COMMON PART SUBLAYER DETAILS

The 802.16 MAC is set up to sustain a P2MP framework with a central BS managing several independent sectors simultaneously. On the downlink, data to SS, are normally multiplexed in TDM way and for the uplink is shared between the SS are multiplexed in TDMA way.

Given that the 802.16 MAC is connection oriented, it provides a vehicle for requesting bandwidth association of QoS and traffic limits, routing and sending information to the correct convergence sublayer. The connection used is usually fixed with a 16-bit connection identifier (CID).

Table 3 demonstrates the features and benefits of the 802.16 of MAC Layer. (Worldwide Interoperability for Microware Access Forum, n.d)

FEATURES	*BENEFITS*
TDM / TDMA Scheduled Downlink/Uplink frames	*Efficient bandwidth usage*
Scalable from 1 to 100 of subscribers	*Allows cost effective deployments by supporting enough subs to deliver robust business case.*
Connection-oriented	*1) Per Connection QoS* *2) Faster packet routing and forwarding*
QoS supportContinuous GrantReal Time Variable Bit RateNon Real Time Variable Bit RateBest Effort	*1) Low latency for delay sensitive services (TDM Voice, VoIP)* *2) Optimal transport for VBR traffic(e.g., video)·*
Automatic Retransmission request (ARQ)	*Improves end-to-end performance by hiding RF layer induced errors from upper layer protocols*

Support for adaptive modulation	*Enables highest data rates allowed by channel conditions, improving system capacity*
Security and encryption (Triple DES)	*Protects user privacy*
Automatic Power control	*Enables cellular deployments by minimizing self interference*

Each SS has a typical 48-bit MAC address which purpose is to primarily identify the equipment of which the primary addresses used in the system are the CIDs. On joining to the network the SS is allocated three separate management connections reflecting the three different QoS level. These are:

1. Basic Connection

   Basic connection is used for the transmission of short time-critical MAC and radio-link control (RLC) messages.

2. Primary Management Connection

   Primary management connection transmits longer and more delay-tolerant communication such as the one used in verification, validation and set of connections.

3. Secondary Management Connection

   Secondary connection management is used for the transfer of standards-base management messages. Examples of such are Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP) and the Simple Network Management Protocol (SNMP).

Transport connections are conveyed only in one direction to ease the QoS of both downlink and uplink subframes and traffic parameters which are normally paired.

MAC PDU FORMATS

The MAC PDU is the data unit transferred between the MAC layers of the BS and it SSs. It consists of a fixed length MAC header, a variable-length payload and an optional cyclic redundancy check (CRC).

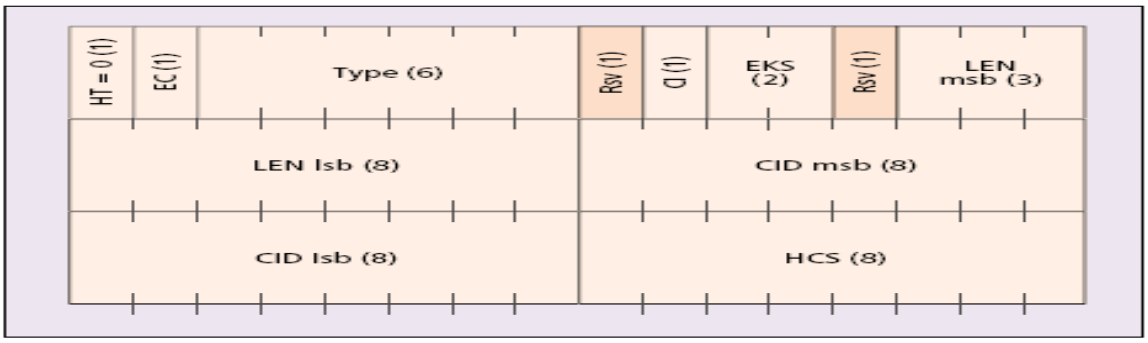

Figure 5. Format of a MAC PDU generic header. (IEEE Communications Magazine, 2002)

Apart from the bandwidth request an important aspect of the MAC PDU is that no payload exists but contains the MAC convergence sublayer data or the management of messages.

There are three possible types of MAC Subheaders in the MAC PDU:

1. Grant Management Subheaders: These SSs uses the Grant Management Subheader to deliver bandwidth requirements to its BS.
2. Fragmentation Subheaders: This is the section holding data notifying the existence and the direction in the payload of any fragment of the SDUs.
3. The Packing Subheaders: This section enables multiple SDUs to consolidate into a single PDU.

TRANSMISSION OF MAC PDUs

The IEEE 802.16 MAC layer sustains several high-layer data units such as IP and ATM. Inward bound MAC SDUs are configured to the MAC PDU format at the Convergence layer. Fragmentation, the division of MAC SDUs, or/and packing, the combining of single MAC PDUs into a single MAC PDU payload, before being transferred over a single or multiple connections with regards to the MAC protocol may occur.

Both fragmenting and packing of the bandwidth allocation occurs to enhance the effectiveness, efficiently and the feasibility of both. These processes can be activated by a downlink connection by the BS or an uplink connection by the SS.

RADIO LINK CONTROL

The highly sophisticated technology of the 802.16 PHY demands that burst profile transmissions occur via an advanced Radio Link Control (RLC), whilst continuing to function traditionally i.e. power control and ranging. The RLC operates by broadcasting at regular intervals, the burst profiles chosen for the uplink and downlink of the BS. Factors such as rain region and equipment capabilities affect which burst profiles are used on a channel. Downlink bust profiles are tagged with a Downlink Interval Usage Code (DIUC) and the uplink are tagged with an Uplink Interval Usage Code (UIUC).

During the first connection, the SS complete initial power handling and varying using ranging request (RNG-REQ) messages transmitted in maintenance windows. The SS also request to be served in the downlink through a particular burst profile by transmitting its choice of DIUC to the BS.

CHANNEL ACQUISITION

Manual configuration is not required to find the operating channel as the MAC protocol includes an automatic initialization procedure. Once installed, the SS begins scanning its frequency. It can sometimes already be programmed to link with an identified BS. This programming is particularly beneficial in dense environments where the SS might not be able to easily distinguish the target BS if a secondary BS antenna is in close proximity or due to selective.

After selecting the channel(s) to endeavor data exchange, the SS attempts to synchronize to the downlink transmission by locating the intermittent frame preambles. Once the physical layer is synchronized, the SS searches for the frequently broadcast DCD or UCD message that facilitates the SS to learn the modulation of the FEC schemes used on the carrier.

SS AUTHENTICATION & REGISTRATION

Each SS includes an X.509 digital certificate which is manufacturer-issued and factory-installed as well as the manufacturer's certificate. The connection of the 48-bit MAC address of the SS and its RSA key is permitted due to the SS sending Authorization Request and Authorization Information messages to the BS seeking verification of the certificates. At this stage the network also identifies the SSs authorization permissions. To complete network approval of the SS, the BS replies to the request with an Authorization Reply carrying an Authorization Key (AK) encrypted with the SSs public key.

Successful authorization allows the BS to secure all following communication during connection. A secondary management connection of the SS is launched when network registration is completed. The registration process also verifies connection setup ability, MAC operation capabilities and the IP version.

CRYPTOGRAPHIC METHODS

Before encryption, each packet number is allocated a distinctive numeric character as a new 4-byte packet number. The 802.16e applies Data Encryption Standard (DES) in the Cipher Block Chaining (CBC) mode and the Advanced Encryption Standard (AES) in the CCM to encrypt the payload of the MAC PDU.

MAC LAYER THREATS

Table 4 lists the values of eavesdropping, an undetected listener of the communication, for management messages and user traffic separately. 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.

Table 4 point up a summary of the threats

THREAT	***ALGORITHM USED***	***PROBABILITY***	***IMPACT***	***RISK***
Jamming *Scrambling*		*3* *2*	*1* *1*	*3* *2*
Eavesdropping Management Message		*3:3*	*2:1*	*6:3*
Eavesdropping Traffic	*DES – CBC* *AES – CCM*			
BS or MS Masquerading	*Device List* *X.509 certificate-based* *EAP*	*3* *2:1* *2:2*	*3* *3:2* *3:2*	*9* *6:2* *6:4*
Management Message Modification	*NO MAC* *SHA –1 MAC* *AES MAC*	*3* *2* *1*	*3* *3* *3*	*9* *6* *3*
THREAT	***ALGORITHM USED***	***PROBABILITY***	***IMPACT***	***RISK***
Data Traffic Modification	*Without AES* *With AES*	*3* *1*	*1* *1*	*3* *1*
DOS on BS or MS	*EAP, SHA –1, AES, MAC*	*3:3*	*3:2*	*9:6*

The masquerading threat of the BS or Ms is enabled when authentication weaknesses are present. Identity theft and Rogues BS are specific techniques of masquerading.

Identity theft takes place when the original hardware address is reprogrammed with the address of a different device. This problem is widespread for unlicensed services such as WiFi/802.11, but has since been curbed with the release of subsequent technology such as subscriber ID module (SIM) cards on cellular networks.

Another form of masquerading is when the original BS is being imitated by a rogue BS i.e. an external deceitful man-in-the-middle attacker. The MS's are unable to differentiate between the legitimate BS and the rogue BS while considering the type of network on which the attack is being conducted, which determines the method of attack.

On a WiFi/802.11 network which has carrier sense multiple access, the attacker attains the identity of the legal access point (AP) then sends a message during idle time. The WiMAX/802.16 network is a time division multiple access model meaning the attacker's rogue BS transmission must arrive to the MS at the same time the legitimate BS transmits but stronger to fade the signal of the genuine BS. Just as with the previously identity theft, the attacker

builds a message using the hardware address of the original BS. The attacker waits for the original BS to commence transmission and sends the rogue message whilst acquiring a receive signal at higher decibels than the original BS. The unsuspecting MS deciphers the signal of the rogue BS.

The advanced technology of WiMAX/802.16 has introduced the capability of mutual authentication. This occurs after the network entry steps of scanning, acquisition of channel description, ranging and capability negotiation. Mutual authentication is based on the generic Extensible Authentication Protocol (EAP). For WiMAX/802.16 EAP can be achieved with exact authentication systems such as EAP-TLS (X.509 certificate-based) or EAP-SIM according to B. Aboban and D. Simon (1999) and H. Haverinen and J. Salousy (2004) respectively. They also note that three options of authentication are:

1. Device list-based
2. X.509 certificate-based
3. EAP-based

The probability of a BS or MA masquerading attack is likely to occur when using only a device list-based with a high impact, thus requiring countermeasures due to the high risk.

The X.509 certificate-based authentication limits the masquerading threat to a system but a high impact for the user because loss of service can take place for a lengthy time period. The system impact is classified as medium as possible financial loss, due to theft of air time, is limited. For a user the risk is critical and countermeasures are essential but not for the system.

In the case of an EAP-based authentication being used, a BS or MS masquerading attack is possible. The impact of the system is medium and high for the user classifying the risk as major for the system and critical for the user, similar to the X.509 certificate-based authentication. With EAP-based authentication it is advisable to have a secondary line for business continuity.

By the nature of how the system is designed, MAC management messages are not encrypted and sometimes not validated. The possible authentication methods available are:

1) Hashed Message Authentication Code (HMAC)
2) One-key Message Authentication Code (OMAC)
3) Unique to the OMAC method is that it is AES-based and has a feature where by the message has replay protection.

The various types of attacks that are probable due to weaknesses in the MAC management system authentication can be man-in-the-middle (MITM) attack, replay attack, passive and active attacks. Either of these attacks is classified as high as they affect the channels of communication. This is precisely the reason for suggesting that a second line of defense is essential for the operations.

Authentication procedures are lengthy encouraging the potential for denial of service (DoS) attacks. This is a form of attack which inundates the system with copious amounts of messages. 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.

CONCLUSION

The air interface as documented in the IEEE Standard 802.16 supports the development and operation of standard-based network environment. After evaluating the analysis carried out on the threats to the security of the WiMAX/802.16 broadband wireless access network, it can be summarized that the most crucial threats include

eavesdropping of management messages, BS or MS masquerading, and appropriate consideration should be given to the modification of management messages and denial of service attacks.

The obvious threats that are to be considered are jamming and data traffic modification when AES is not preferred. An approach of securing the WiMAX/802.16 is to make use of a Wireless Intrusion Detection System (WIDS) which can help in addressing some of the issues. Yet, WiMAX/802.16 being a new field of wireless is bound to have more research conducted on this technology.

REFERENCES

Aboba, B. (2005). The unofficial 802.11 security web page - security vulnerabilities in EAP methods, URL www.drizzle.com/aboba/IEEE/ Accessed 15/04/2006.

Aboba, B. and Simon, D. (1999). PPP EAP TLS authentication protocol. The Internet Engineering Task Force - Request for Comments: 2716.

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and Levkowetz, H. (2004). Extensible authentication protocol (EAP). The Internet Engineering Task Force - Request for Comments: 3748.

Barbeau, M. (2005). WiMax/802.16 Threat Analysis, URL http://www.scs.carleton.ca/~barbeau/Publications/2005/iq2-barbeau.pdf Accessed 30/04/2006.

Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks (n.d). URL http://www.ieee802.org/16/tge/contrib/C80216e-04_406.pdf Accessed 04/05/2006.

Eklund, C., Marks, R., Stanwood, K., and Wang, S., (2002). IEEE standard 802.16: A technical overview of wireless man air interface for broadband wireless access. *IEEE Communications Magazine*, 40(6):98–107.

Ernst and Young, (2004). The necessity of rogue wireless device detection. White Paper,

ETSI. Telecommunications and internet protocol harmonization over networks (TIPHON) (2003) Release 4; protocol framework definition; methods and protocols for security; part 1: Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.

Haverinen, H. and Salowey, J. (2004). Extensible authentication protocol method for GSM subscriber identity modules (EAP-SIM). Work in progress,.

IEEE P802.16a/D3-2001: “Draft Amendment to IEEE Standard for Local and Metropolitan Area Networks — Part 16: Air Interface for Fixed Wireless Access Systems — Medium Access Control Modifications and Additional Physical Layers Specifications for 2–11 GHz,”.

IEEE 802.16.2-2001, “IEEE Recommended Practice for Local and Metropolitan Area Networks — Coexistence of Fixed Broadband Wireless Access Systems,”

IEEE 802.16-2001, “IEEE Standard for Local and Metropolitan Area Networks — Part 16: Air Interface for Fixed Broadband Wireless Access Systems,”

IEEE Standard 802.16 : A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access. Retrieved 22/04/2006 from http://www.grouper.ieee.org/groups/802/16/docs/02/c80216-02_05.pdf

IEEE Standard 802.16 - 2001, 2002 LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. Local and metropolitan area networks - Part 16: Air interface for fixed broadband wireless access systems. IEEE Standard 802.16 - 2001, 2002. Draft revision of IEEE Std. 802.16-2001. (n,d)

IEEE Standard 802.16c, (2002). LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. Local and metropolitan area networks - Part 16: Air interface for fixed broadband wireless access systems - amendment 1: Detailed system profiles for 10-66 ghz.

IEEE Standard 802.16a (2003). LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. Local and metropolitan area networks - Part 16: Air interface for fixed broadband wireless access systems - amendment 2: Medium access control modifications and additional physical layer specifications for 2-11 ghz.

Schindler, E. (2006). The WiMAX Evolution: Bring in the Standards Suspects, URL http://business.itbusinessnet.com/articles/viewarticle.jsp?id=39170 Accessed 01/05/2006

Sequans communication (n.d). Building High-Performance 802.16 Solutions for BWA Networks, URL from http://www.sequans.com/site/images/sqn_fast_facts_FIN.pdf Accessed 29/05/2006.

Top seven security problem with 802.11 wirelesses. (n.d), URL

http://wp.bitpipe.com/resource/org_1067352081_810/AirMagnet_Security_WhitePaper.pdf?site_cd=bp Accessed 12/05/2006

WiMAX (n,d). A Study of Mobility and a MAC-layer Implementation in GloMoSim, URL http://www.cs.umu.se/education/examina/Rapporter/CarlbergDammander.pdf Accessed 17/04/2006

WLAN Security – What Hackers Know That You Don't In (n,d), URL http://wp.bitpipe.com/resource/org_1028180222_467/WLAN_Security-What_Hackers_Know_That_You_Dont_In-Network.pdf?site_cd=bp Retrieved 28/04/2006 from

COPYRIGHT