WiMax/802.16 Threat Analysis

Michel Barbeau
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario, Canada

ABSTRACT

This paper examines threats to the security of the WiMax/802.16 broadband wireless access technology. Threats associated with the physical layer and MAC layer are reviewed in detail. The likelihood, impact and risk are evaluated according to a threat assessment methodology proposed by the ETSI. Threats are listed and ranked according to the level of risk they represent. This work can be used to prioritize future research directions in WiMax/802.16 security.

Categories and Subject Descriptors

C.2.5 [**Computer-Communications Networks**]: Local and Wide-Area Networks —*Access schemes, High-speed*

General Terms

Security

Keywords

Wireless network, WiMax, 802.16, Threat analysis.

1. INTRODUCTION

This paper is about a broadband wireless access technology being defined, in a complementary way, by the IEEE and WiMax Forum. With respect to previous wireless access technologies, WiMax/802.16 proposes higher bandwidth IP-based mobile and wireless access, handover between networks of different technologies and management authorities and broadband in remote areas.

The IEEE 802.16 standard [9], published in 2002, defines the air interface for fixed point-to-multipoint broadband wireless access networks. Originally, line-of-sight transmission in the 10 G Hz to 66 G Hz range was supported. Two amendments have been published. The first amendment, the IEEE 802.16c standard [10], defines profiles of typical implementations. The second amendment, the IEEE 802.16a standard [11], consists of control enhancements, introduction of a mesh mode and support of additional frequencies. Together they added transmission in the 2 G Hz to 11 G Hz range, non line-of-sight, and licensed or unlicensed service. An overview of IEEE 802.16 can be found in Ref. [4]. A major update has been published in 2004 as the IEEE 802.16d standard [9]. It is a consolidation and an improvement of the IEEE 802.16 standard and the amendments 802.16c and 802.16a. An amendment to IEEE 802.16d has been drafted as the IEEE 802.16e [9] (completion of the draft is expected in 2005). It defines additional mechanisms to support mobile subscribers at vehicular speed and data authentication.

The role of the WiMax Forum [14] is to define profiles using the broad range of 802.16 available options, to address certification of implementations and to define additional mechanisms for networking such as user-network mutual authentication, integration with other kinds of wireless access technologies (WiFi/802.11, 2G/3G cellular) and transfer of security and quality of service state information during handovers.

This paper presents an analysis of the security threats to WiMax/802.16 security. The paper reflects to most recent work of the IEEE and WiMax Forum, including elements being drafted right now. Threats are analyzed with respect to their likelihood of occurrence, their possible impact on individual users and system and the global risk they represent.

The methodology used to conduct the treat analysis is introduced in Section 2. The analysis is presented in Section 3. We conclude with Section 4

2. METHODOLOGY

The threat analysis is conducted according to a methodology described in Ref. [6]. The methodology is summarized in Table 1. The evaluation is conducted according to three criteria: Likelihood, Impact and Risk. The *Likelihood* evaluates the possibility that attacks associated with the threat are conducted. Two factors are taken into account: the technical difficulties that have to be resolved by an attacker and the motivation for an attacker to conduct an attack. The likelihood is *Low* if a potential attacker has to resolve strong technical difficulties, with major unknowns, or there is a low motivation for conducting an attack of that type. The likelihood is *Possible* if there are technical difficulties, but solvable because the required information is available, or there are reasonable reasons for an attacker to conduct an attack. The likelihood is *Likely* if there is no technical difficulty that needs to be solved to conduct an attack or there is a high motivation for an attacker to launch an attack.

Q2SWinet'05, October 13, 2005, Montreal, Quebec, Canada.

The *Impact* criterion evaluates the consequences of an attack related to the threat. The impact is *Low* if an attack creates only annoyance to the user and consequences, if there are any, are reversible and can be repaired. If an attack is directed to a system serving several users, then possible outages are very limited in scope. For example, the number of affected users is limited or the outages are of short duration. The impact is *Medium* if the attack is directed to a single user and that user will experience a loss of service for a considerable amount of time. If the attack is directed to a system, then outages are limited in scope and there are possible financial losses, but limited. The impact is *High*, if an attack directed to a single user causes a loss of service for a long period of time. If an attack is directed to a system, then outages are for long periods of time and a large number of users are affected. In addition, there can be law violations or substantial financial losses.

The Likelihood and Impact receive numerical values from one to three, indicated in the rightmost column in Table 1. For a given threat, the *Risk* value is defined as the product of the Likelihood value and Impact value. If the value of the risk is one or two, then the threat is considered to be minor and there is no need for countermeasures. If the risk is three of four, then the threat is major and needs to be handled. Finally, if the risk is six or nine, then the threat is critical and needs to be addressed in priority.

This type of analysis is subjective. Risk values may vary according to the author(s) of the analysis and information available to the author(s). We believe, although, that it is a nice tool for identifying security flaws and ranking them by order of importance. Hence, more emphasis could be put on countermeasures for threats which receive high priority.

3. ANALYSIS

A WiMax/802.16 wireless access network consists of base stations (BSs) and mobile stations (MSs). The BSs provide network attachment to the MSs. As a serving BS, an MS selects the one which offers the strongest signal. In this analysis, the subscriber plays the role of the user while a BS and a collection of served MSs play the role of system.

The protocol architecture of WiMax/802.16 is structured into two main layers: the medium access control (MAC) layer and physical layer, see Figure 1. The diagram also indicates interfacing points where service access points (SAPs) are formally defined by the standard. The central element of the layered architecture is the Common Part sub layer. In this layer, MAC protocol data units (PDUs) are constructed, connections are established and bandwidth is managed. The Common Part exchanges MAC service data units (SDUs) with the Convergence layer. The Common Part is tightly integrated with the Security sub layer. The Security sub layer addresses authentication, establishment of keys and encryption. The Security sub layer exchanges MAC PDUs with the Physical layer. The Convergence layer adapts units of data (e.g. IP packets or ATM cells) of higher level protocols to the MAC SDU format, and vice versa. The Convergence layer also sorts the incoming MAC SDUs by the connections to which they belong. The Physical layer is a two-way mapping between MAC PDUs and Physical layer frames received and transmitted through coding and modulation of RF signals.

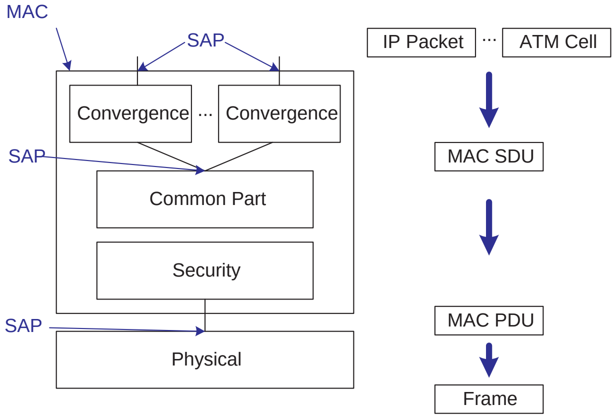

Figure 1: WiMax/802.16 layered architecture.

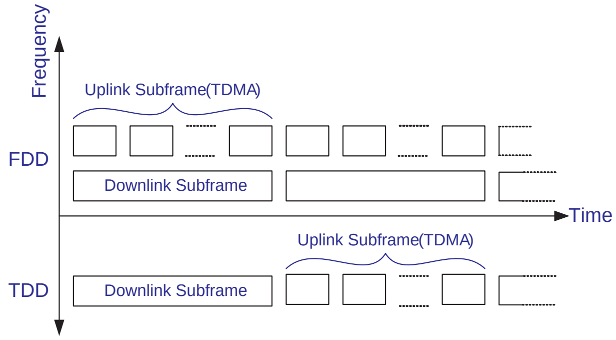

Figure 2: Framing.

We examine security threats at the Physical layer then at the MAC layer. The results of the analysis are consolidated in Table 3. When there is a pair of values (separated by a column), the first value ranks the case of an individual user while the second value ranks the case for a system. When there is only one value, both cases are the same.

3.1 Physical Layer Threats

At the physical layer, the flow of bits is structured as a sequence of frames of equal length, see Figure 2. There is a downlink subframe and an uplink subframe and two modes of operation: frequency division dulplex (FDD) and time division duplex (TDD). Figure 2 pictures these two modes. The horizontal axis represents the time domain while the vertical one represents the frequency domain. In FDD, the downlink subframe and uplink subframe are simultaneous, but don't interfere because they are sent on different frequencies. In TDD, the downlink subframe and uplink subframe are consecutive. A frame duration of 0.5, one or two milliseconds can be used.

Frames are of equal length. In TDD, the portion allocated for the downlink and portion allocated to the uplink may vary. The uplink is time division multiple access (TDMA), which means that the bandwidth is divided into time slots. Each time slot is allocated to an individual MS being served by the BS.

Table 1: Risk evaluation grid.

		Rationale		
Criteria	Cases	Difficulty	Motivation	Rank
Likelihood	Unlikely	Strong	Low	1
	Possible	Solvable	Reasonable	2
	Likely	None	High	3
		User	System	
Impact	Low	Annoyance	Very limited outages	1
	Medium	Loss of service	Limited outages	2
	High	Long time loss of service	Long time outages	3
Risk	Minor	No need for countermeasures		1, 2
	Major	Threat need to be handled		3, 4
	Critical	High priority		6, 9

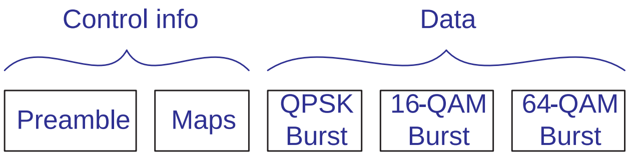

Figure 3: TDD downlink subframe.

A detailed representation of a TDD downlink subframe illustrates the burst nature of the transmission, see Figure 3. A downlink subframe consists of two main parts. The first part contains control information while the second part contains data. The control information consists of a preamble and maps. The preamble is for frame synchronization purposes. There are two maps. A downlink map announces the start position and transmission characteristics of the following data bursts. An uplink map announces the allocation of the bandwidth to the MSs for their transmission. The data part consists of a sequence of bursts. Each burst is transmitted according to a profile of modulation and a kind of forward error correction. They are sent in an increasing degree of demodulation difficulty. Hence, an MS may only receive the bursts while it has the capability to do it and ignores the bursts it cannot demodulate.

Since the security sub-layer is above it, the physical layer is unsecured (as pictured in Figure 1). WiMax/802.16 is vulnerable to physical layer attacks such as jamming and scrambling. Jamming is achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel. Jamming is either unintentional or malicious. The information and equipment required to perform jamming are not difficult to obtain. Poisel has published a book on the topic of jamming alone, i.e. how to build jamming systems and to counter systems which are by construction jamming resistant [12]. We believe that a jamming attack is likely to occur. Resilience to jamming can be augmented by increasing the power of signals or increasing the bandwidth of signals using spreading techniques, e.g. frequency hopping or direct sequence spread spectrum. Note that a number of options are available to raise the power of a signal, namely, a more powerful transmitter, a high gain transmission antenna and a high gain receiving antenna. Jamming is easy to detect with radio spectrum monitoring equipment. Sources are relatively easy to locate using radio direction finding tools. Law enforcement can be involved to stop jammers. Jammed segments of bandwidth, once detected, can also be avoided in a spread spectrum scheme. Since jamming is fairly easy to detect and to address, we believe that it can have a low impact on both the user and system. The risk associated to jamming is therefore major, at the most.

Scrambling is a sort of jamming, but for short intervals of time and targeted to specific frames or parts of frames. Scramblers can selectively scramble control or management information with the aim of affecting the normal operation of the network. The problem is of greater amplitude for time sensitive messages, which are not delay tolerant, such as the channel measurement report requests or responses. Slots of data traffic belonging to targeted users can be scrambled selectively, forcing them to retransmit. With the net result that they get less than their granted bandwidth. Selectively scrambling uplink slots of other users can theoretically reduce the effective bandwidth of the victims and accelerate the processing of the data of the attacker (if it is an another user). It is relatively more difficult to achieve scrambling than jamming because of the need, by the attacker, to interpret control information and to send noise during specific intervals. There are technical difficulties to address by an attacker, but they are solvable. The likelihood of occurrence is possible. Scrambling is more difficult to detect because of the intermittent nature of the attack and the fact that scrambling can also be due to natural sources of noise. Scrambling and scramblers can be detected by monitoring anomalies in performance criteria. This issue has been studied for WiFi/802.11 systems by Raya et al. [13]. The situation for WiMax/802.16 is much different and research is required for this case. The impact of scrambling is low. It results in annoyance to a limited number of users. Results are reversible, e.g. by retransmission. We believe that scrambling represents a minor risk at this time.

3.2 MAC Layer Threats

The MAC layer is connection oriented. There are two kinds of connections: management connections and data transport connections. Management connections are of three kinds: basic, primary and secondary. A basic connection is created for each MS when it joins the network. It is used for short and urgent management messages. The primary connection is also created for each MS at the network entry time, but it is used for delay tolerant management messages. There is a third management connection, the secondary, which is used for IP encapsulated management messages (e.g. DHCP, SNMP, TFP).

Transport connections can be provisioned or can be established on demand. They are use for user traffic flows. Unicast or multicast can be used for transmission.

A security association (SA) is a concept that captures the security parameters of a connection: keys and selected encryption algorithms. The basic and primary management connections don't have SAs. Although, integrity of management messages can be secured (as discussed in the sequel). The secondary management connection can have, on an optional basis, a SA. Transport connections always have SAs,

The security model is pictured in Figure 4. The security keys and associations established between an MS and a BS during the authorization step at network entry are discussed in the sequel. Rectangles picture entities. Lines represent relations with cardinalities at the termination points. Preexisting elements are pictured with solid lines while dynamically established elements are drawn using dashed lines. There are three types of SAs, namely, the primary SA, static SA and dynamic SA. Each SA has an identifier (SAID). It also contains a cryptographic suite identifier (selected algorithms), Traffic Encryption Keys (TEKs) and initialization vectors. There is one primary SA for each MS. The primary SA is established when the MS is initialized. The scope of the primary SA is the secondary management connection. The primary SA is shared exclusively between an MS and its BS. Static SAs are created by the BS during the initialization of an MS. There is a static SA for the basic unicast service. An MS may have subscribed to additional services. There are as many additional static SAs as there are subscribed additional services. Dynamic SAs are created on the fly when new flows are opened and they are destroyed when their flow is terminated. Static SAs and dynamic SAs can be shared among several MSs, when multicast is used.

Core data entities are the X.509 certificate, AK (Authorization Key), KEK (Key Encryption Key) and HMAC Key (message authentication key). Every MS is preconfigured with an X.509 certificate. The X.509 certificate is persistent. It contains the Public Key (PK) of the MS. The MS uses it for its authentication with the BS. All other keys are established during authorization. They are subject to an aging process. They must be refreshed on a periodic basis through reauthorization. The BS determines the AK and passes it to the MS, encrypted using the PK. The AK has a sequence number (from zero to 15) and a lifetime. For the purpose of smooth transitions, two AKs may be simultaneously active with overlapping lifetime. The lifetime of an AK ranges from one day to 70 days, with a default value of 7 days. The MS uses the AK to determine the KEK and HMAC Key. The sequence number of the AK implicitly belongs to the HMAC Keys as well. KEKs are used to encrypt TEKs during their transfer.

The network entry of an MS consists of the following steps:

- Downlink scanning and synchronization with a BS.
- Downlink and uplink description acquisition; available uplink channel discovery.
- Ranging.
- Capability negotiation.
- Authorization, authentication and key establishment.
- Registration.

During scanning, the MS looks up for downlink signals by going through the available frequencies. It does search for downlink subframes. Whenever a channel is found, it gets the downlink and uplink description. The MS obtains the downlink map and uplink map in the physical frame headers (they tell the structure of the subframes in terms of bursts). The downlink/uplink channel descriptors are obtained as MAC management messages (they tell the properties of the bursts in terms of data rate and error correction). During ranging, the MS synchronizes its clock with the BS and determines the level of power required to communicate with the BS. Ranging is done in a special channel called the *ranging interval*, which is contention-based multiple access. The basic connection and primary connection are assigned during ranging. Capabilities, e.g. in terms of supported security algorithms, are negotiated on the basic connection. Authorization and authentication can be device list-based, X.509 certificate-based or EAP-based. It is discussed in more details in the sequel. The registration results in the establishment of a secondary management connection and provisioned connections.

We examine the MAC layer threats with respect to confidentiality and authentication. A MAC layer PDU consists of a MAC header, a payload and an optional CRC. The payload may consist of user traffic of management messages. The MAC header contains a flag, which indicates whether the payload of the PDU is encrypted or not. MAC headers themselves are not encrypted and all MAC management messages shall be sent in the clear. According to the standard, this is for facilitating the operation of the MAC layer. Each transport connection (the term used to refer to a MAC layer connection dedicated to user traffic) has either one SA (which applies to both the uplink and downlink) or two SAs (one for the uplink and another for the downlink).

The format of the payload is pictured in Figure 5. When applicable, before encryption, each packet is given a unique identity as a new four-byte packet number (which is increased from one data unit to another). Note that, for the sake of uniqueness, there are separate ranges of values for the uplink and downlink. The 802.16e uses Data Encryption Standard (DES) in the CBC mode or Advanced Encryption Standard (AES) in the CCM mode to encrypt the payload of MAC PDUs. Protection of integrity of 802.16 data traffic did not exist before 802.16e. The 802.16e introduces an integrity protection mechanism for data traffic. CBC-MAC (as a component of AES-CCM) is used to protect the integrity of the payload of MAC data units.

Table 3 provides values for the eavesdropping threat, first for management messages, then for user traffic. Management messages (never encrypted) can provide valuable information to an attacker (e.g. to verify the presence of a victim at its location before perpetrating a crime). They can be intercepted by a passive listener within communication. There are no serious technical difficulties to resolve by an attacker. It is likely to occur. From the user perspective, eavesdropping of management messages may result in limited financial loss, if it results in the execution of a crime. From the point of view of a system, eavesdropping in itself may not create outages. Although, it might be used by a competitor to map the network. Hence, eavesdropping of management messages is a critical threat for users and a major threat to a system. Eavesdropping of traffic is a minor threat and there is no need for countermeasures.

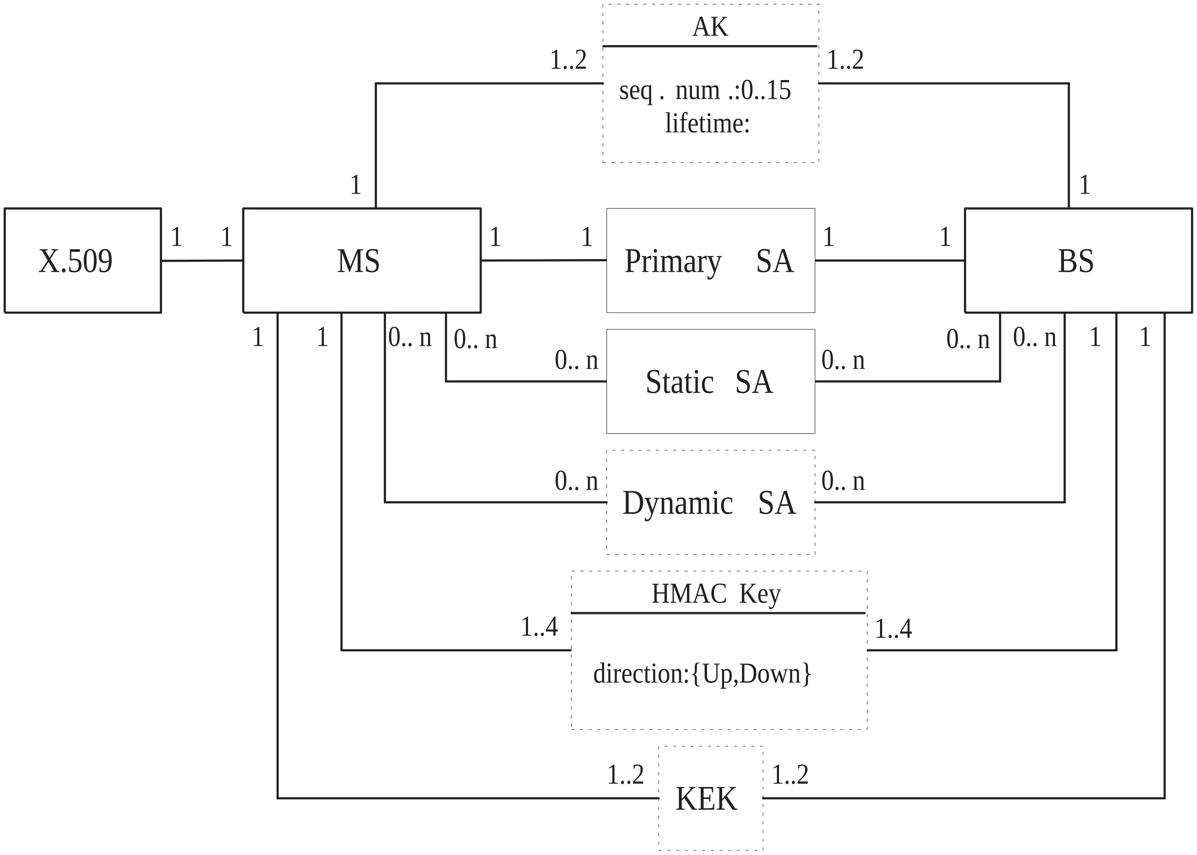

Figure 4: Security model.

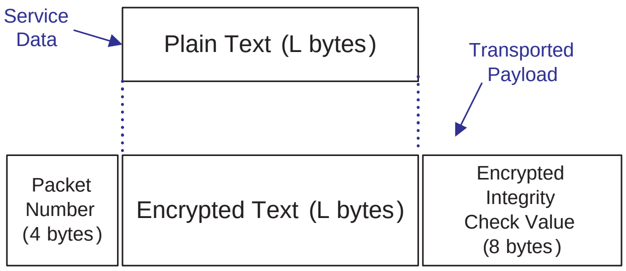

Figure 5: Payload format.

The applicable kinds of authentication in WiMax/802.16 are listed in Table 2. There is device level authentication. It is useful for detecting stolen devices and blocking their access to the network. It is a RSA/X.509 certificate-based authentication. The certificate can be programmed in a device by its manufacturer. It is unilateral, i.e. BSs are not authenticated.

The standard IEEE Std 802.16-2001 [9] (Page 172) says *identity can be verified via the X.509 digital certificate*. This wording suggests that it is possible to disregard the X.509 certificate and base access control on a predetermined list of devices, for instances.

Any weakness in authentication is an enabler for the BS or MS masquerading threat. Specific techniques are the identity theft and rogue BS attack. Identity theft consists or reprogramming a device with the hardware address of another device. This is a well know problem in unlicensed services such as WiFi/802.11, but has been under control in cellular networks because it had been made illegal and more difficult to execute with subscriber ID module (SIM) cards. It is interesting to note that a recent case of CDMA phone cloning in India has been documented [8]. The address can be stolen over the air by intercepting management messages. A *rogue BS* is an attacker station that imitates a legitimate BS. The rogue BS confuses a set of MSs trying to get service through what they believe being a legitimate BS. The exact method of attack depends on the type of networks. In a WiFi/802.11 network, which is carrier sense multiple access, the attacker has to capture the identity of a legitimate access point (AP), to build a message using the legitimate AP's identity, to wait until the medium is idle and to send the message. It appears to be one of the top security threats in WiFi/802.11 networks [5]. In a WiMax/802.16 network, it is more difficult to do because of the time division multiple access model. The attacker must transmit while the legitimate BS is transmitting. The signal of the attacker, however, must arrive at the targeted receiver MS(s) with more strength and must put the signal of the legitimate BS in the background, relatively speaking. Again, the attacker has to capture the identity of a legitimate BS and to build a message using that identity. The attacker has to wait until a time slot allocated to the legitimate BS starts. The attacker must transmit while achieving a *receive signal strength*, a value in dBm, higher than the one of the legitimate BS. The receiver MSs reduce their gain and decode the signal of the attacker instead of the one from the legitimate BS.

Mutual authentication at user-network level has been introduced in WiMax/802.16. Mutual authentication, when available, occurs after scanning, acquisition of channel description, ranging and capability negotiation. It is based on the Extensible Authentication Protocol (EAP) [2]. EAP is a generic authentication protocol. For WiMax/802.16, EAP can be actualized with specific authentication methods such as EAP-TLS (X.509 certificate-based) [3] or EAP-SIM [7].

There are three options for authentication: device list-based, X.509 based or EAP-based. If device list-based authentication is used only, then the likelihood of a BS or MA masquerading attack is likely. Impact can be high. The risk is therefore high and there is a need for countermeasures. If X.509-based authentication is used, the likelihood for a user (a MS) to be the victim of BS masquerading is possible because of the asymmetry of the mechanism. For a system, it is unlikely. The impact for a user is high because it can lead to loss of service for long periods of time. The impact for a system is medium, because it can lead to limited financial loss (due to theft of air time). In the case of a user, the risk is critical and countermeasures are needed. For a system, the risk is minor and there is no need for countermeasures.

If EAP-based authentication is used, we believe that at this time it is safe to say that the likelihood of a BS or MS masquerading attack is possible. Some of the EAP methods are being defined; security flaws are often uncovered in *unproven* mechanisms. Aboba maintains a Web page about security vulnerabilities in EAP methods [1]. The impact is the same as for the X.509 certificate-based authentication. The risk is critical for a user and major for a system. It is a good idea to allow a second line of defense to play safe with EAP-based authentication.

MAC management messages are never encrypted and not always authenticated. There are authentication mechanisms for MAC layer management messages: the hashed message authentication code (HMAC) tuple and one-key message authentication code (OMAC) tuple. The OMAC is AES-based and includes replay protection, while to HMAC doesn't. The authentication mechanism for MAC layer management messages to be used is negotiated at network entry. The scope of management messages to which authentication is applicable is limited in earlier versions of 802.16 (has been extended in version *e*). Hence, with earlier versions of 802.16 the management messages are no subject to integrity protection. Weaknesses in management messages authentication open the door to aggressions such as the man in the middle attack, active attack and replay attack. The likelihood of the management message modification threat is likely, possible or unlikely if no authentication, HMAC or OMAC is used respectively for management messages. In all cases, the impact of an attack of that type can be high because it might affect the operation of the communications. The risk is at least major for all the cases and it might be safe to allow a second line of defense against this type of attack in all the cases.

Authentication of traffic messages has been discussed. The modification of traffic is very unlikely to occur if AES is used, likely otherwise. We believe that such an attack can create annoyance. If AES is not used, then it is a major threat. Otherwise, it is minor.

There is a potential for denial of service (DoS) attacks created by the fact that authentication operations (of devices, users and messages) trigger the execution of long procedures. A DoS attack can be executed by flooding a victim with a high number of messages to authenticate. This is likely to occur.

The impact is medium on a system, but could be high on a user because of lower computational resources available for handling an large influx of invalid messages.

4. CONCLUSION

An analysis of the threats to the security of the WiMax/ 802.16 broadband wireless access networks has been conducted. Critical threats are eavesdropping of management messages, BS or MS masquerading, management message modification and DoS attack. Major threats are jamming and data traffic modification (when AES is not applied). Countermeasures need to be devised for networks using the security options with critical or major risks. An intrusion detection system approach can be used to address some of the threats. More research is needed in this direction.

5. ACKNOWLEDGMENTS

The author would like to thank Jean-Marc Robert and Vinod Kumar Choyi of Alcatel Canada for helpful comments on an early version of this work. The author graciously acknowledges the financial support received from the following organizations: Natural Sciences and Engineering Research Council of Canada (NSERC) and Mathematics of Information Technology and Complex Systems (MITACS).

6. REFERENCES

[1] B. Aboba. The unofficial 802.11 security web page - security vulnerabilities in EAP methods. www.drizzle.com/ aboba/IEEE/, May 2005.

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

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

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

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

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

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

[8] F. T. Information. Mobile cloning, March 2005.

[9] 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.

[10] 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 802.16c-2002, 2002.

[11] 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. IEEE Standard 802.16a-2003, 2003.

[12] R. Poisel. *Modern Communications Jamming Principles and Techniques*. Artech House Publishers, 2003.

[13] M. Raya, J.-P. Hubaux, and I. Aad. Domino: A system to detect greedy behavior in IEEE 802.11 hotspots. In *Proceedings of the 2nd International Conference on Mobile Systems, Applications and Service (MobiSys)*, pages 84–97, Boston - MA, 2004.

[14] WiMax Forum. www.wimaxforum.org/home, 2005.

Table 2: Authentication in WiMax/802.16.

Kind	Mechanism
Device	Device list RSA/X.509 certificate
User level	EAP + EAP-TLS (X.509) or EAP-SIM (subscriber ID module)
Data traffic	AES-CCM CBC-MAC
Physical layer header	None
MAC layer header	None
Management messages	SHA-1 based MAC AES based MAC

Table 3: Analysis summary.

Threat	Algorithm(s)	Likelihood	Impact	Risk
Jamming		3	1	3
Scrambling		2	1	2
Eavesdropping management messages		3:3	2:1	6:3
Eavesdropping traffic	DES-CBC, AES-CCM	1	1	1
BS or MS masquerading	Device list	3	3	9
	X.509 dev. Auth.	2:1	3:2	6:2
	EAP	2:2	3:2	6:4
Management message modification	No MAC	3	3	9
	SHA-1 MAC	2	3	6
	AES MAC	1	3	3
Data traffic modification	Without AES	3	1	3
	With AES	1	1	1
DoS on BS or MS	EAP, SHA-1, AES MAC	3:3	3:2	9:6