in: C. Zhang and H.-H. Chen (Editors), Mobile WiMax: Toward Broadband Wireless Metropolitan Area Networks, Wireless Networks and Mobile Communications Series, Volume 7, Taylor and Francis CRC Press, 2007.

Chapter 1

Analysis of Threats to WiMax/802.16 Security

Michel Barbeau and Christine Laurendeau
Carleton University

This chapter 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 an adaptation of the threat assessment methodology proposed by the European Telecommunications Standards Institute (ETSI). Threats are listed and ranked according to the level of risk they represent. This assessment can be used to prioritize future research directions in WiMax/802.16 security.[1]

1.1 Introduction

This chapter pertains to an emerging broadband wireless access technology being jointly defined by the IEEE and WiMax Forum [16]. Compared to previous wireless access tech-

[1] ©ACM, 2006. This is a revision of work published in Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks Q2SWinet (October 2005).

nologies, WiMax/802.16 offers wide bandwidth IP-based mobile and wireless access, handover across heterogeneous networks and management authorities and broadband service in remote areas.

The IEEE 802.16 standard [16] defines the air interface for fixed point-to-multipoint broadband wireless access networks. An overview of IEEE 802.16 can be found in [8]. The IEEE 802.16e [17] amendment defines additional mechanisms to support mobile subscribers at vehicular speed, as well as mechanisms for data authentication.

The role of the WiMax Forum [24] is to define profiles as subsets of the broad range of available options, to address the 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 chapter provides an analysis of the threats to WiMax/802.16 security. Threats are analyzed with respect to their likelihood of occurrence, their possible impact on individual users and on the system, and the global risk they represent.

The methodology employed to conduct the threat analysis is introduced in Section 1.2. The analysis is presented in Section 1.3. Section 1.4 concludes the chapter.

1.2 Methodology

The primary goal of a threat analysis is to determine the threats inherent to a given technology and ascertain the risk posed by each identified threat. With this information, efforts to devise countermeasures can be efficiently focused solely on the more critical threats.

There are two types of threat analysis methodologies, quantitative and qualitative. *Quantitative threat analysis methodologies* [12] [18] offer an objective means for estimating the risk posed by a threat by using the statistical probability of its occurrence. However, a significant drawback of this type of methodology lies in its reliance on historic data of past occurrences of a threat in order to predict future occurrences. In the case of emerging technologies such as WiMax/802.16, no such history of past events exists, therefore quantitative threat analysis methodologies cannot be applied. *Qualitative threat analysis methodologies* [4] [7] [10], on the other hand, allow for discrete, estimated values to be assigned to a variety of risk factors, including the likelihood of occurrence and impact on the victims. Although this type of methodology has no dependence on pre-existing historic data, it is more subjective than its quantitative counterpart. Risk factor values may vary according to the authors of the analysis and the information available. However, we believe that it is a nice tool for identifying security flaws and ranking them by order of importance. One example of a qualitative threat analysis methodology is the one put forth by the European Telecommunications Standards Institute (ETSI), which forms the basis for the method used here to assess the threats to WiMax/802.16 security.

The ETSI methodology was originally developed in 2003 to analyze the security threats to a meta-protocol named Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) [10]. This methodology allows for the risk posed by identified threats to be evaluated as critical, major or minor, depending on estimated values for the likelihood of occurrence of the threat and its impact upon a user or a system. As a guideline, a threat ranked as minor typically requires no countermeasures, a major one needs to be dealt with, and a critical threat must be addressed with the highest priority. In the ETSI methodology, a threat is ranked as critical under the following conditions: if it is likely and has high impact, if it is likely and has medium impact, and if it is possible and has high impact. A threat is only assessed as major if it is possible and has medium impact. We have found, through experience with the ETSI methodology [**?**] [**?**], that many threats are over-classified as critical when they are better ranked as major. As a result, we have adapted the ETSI methodology to assess the risks as depicted in Table 1.1. Our adaptation thus places the emphasis on the truly critical threats. The evaluation of the likelihood and impact risk factors is described in Sections 1.2.1 and 1.2.2.

Table 1.1: Risk as a function of the likelihood and impact.

	Impact		
Likelihood	**High**	**Medium**	**Low**
Likely	Critical	Major	Minor
Possible			
Unlikely			

1.2.1 Likelihood of Occurrence

The *Likelihood* risk factor denotes the possibility that attacks associated with a given threat are carried out. Three discrete levels of likelihood are defined: *Likely*, *Possible* and *Unlikely*. In order to evaluate the likelihood of a threat, two additional risk factors are taken into account: the motivation for an attacker to carry out the attack and the technical difficulties that must be resolved by the attacker in order to do so, as shown in Table 1.2.

A threat is *Unlikely* if there is little motivation for perpetrating the specific attack or if significant technical difficulties must be overcome. A threat is *Possible* if the motivation for an attacker is sufficiently high and the technical difficulties are few or solvable because the required theoretical and practical knowledge for implementing the attack is available. A threat is *Likely* if a user or system is almost assured of being victimized, given a high attacker motivation and lack of technical hurdles. The different values for motivation and technical difficulties are further described in the sequel.

Table 1.2: Likelihood as a function of attacker motivation and technical difficulty.

Motivation	**Difficulty**	**Likelihood**
High	None	Likely
	Solvable	Possible
Moderate	None	
	Solvable	
Low	Any	Unlikely
Any	Strong	

Attacker Motivation

The topic of what motivates a computer hacker to conduct attacks has been addressed in the literature in order to devise better countermeasures. In his insightful article [6], anthropologist Roger Blake adapts basic social stratification theory to suggest that hackers are motivated primarily by wealth, power and prestige, although these may be sought in the acquisition of knowledge rather than money. The financial gains to be made through the sale of private information or the disruption of a business rival's network, the power that private or secret information can afford an individual over others, and the prestige to be garnered before the hacker community are thus powerful motives for attacks.

Schifreen [21] proposes five possible motives for hackers:

- Opportunity: the temptation offered by systems with poor security mechanisms
- Revenge: attacks perpetrated by a disgruntled employee, for example
- Greed: financial gain through the sale of information, espionage or blackmail
- Challenge: the prestige obtained through trumping a security system
- Boredom: the lack of better activities to occupy the hacker's time

To these, Barber [5] adds:

- Vandalism: the defacing of corporate web sites
- Hacktivism: attacks conducted for making political, ecological or ethical statements
- Information Warfare: governments trying to influence foreign or domestic situations for their own interests

In our adaptation of the ETSI methodology, we assess the possibility of gain in terms of money and power to be somewhat more motivating than prestige. We therefore associate a *High* motivation with an attacker reaping significant financial or power-based gains, a *Moderate* motivation with limited gains or with creating mischief for the purpose of garnering prestige, and a *Low* motivation with little gain for the attacker.

Technical Difficulty

Technical difficulty refers to the technological hurdles encountered by an attacker in his attempts to implement a threat. It should be noted that such difficulties are dynamic in nature. What seems like an unsurmountable obstacle today may not be so in a few years' time.

For example, WiFi implementations based on the IEEE 802.11 standard's original specifications employ the Wired Equivalent Privacy (WEP) approach to security [14]. The standard's working group believed that WEP's security mechanisms posed strong technical difficulties to attackers. In 1999, the technical difficulty for attacks directed at WEP was *Strong*, and attacks were *Unlikely* to occur. However, it quickly became obvious that WEP had weaknesses. WEP's shortcomings were discovered by Fluhrer, Mantin, and Shamir and made public in 2001 [11]. The technical difficulty became *Solvable* and the likelihood of attacks rose to the level of *Possible*. In 2002, Stubblefield, Ioannidis, and Rubin implemented the attack [22]. Since that time, the attack has been well documented, and the associated software has been available, reducing the technical difficulty to *None* and upgrading the likelihood of the attack to *Likely*. WiFi Protected Access (WPA), WEP's successor, is currently believed to pose strong technical difficulties to attackers [23]. It remains to be seen whether this assumption stands the test of time.

In our WiMax/802.16 threat analysis, we assign a *Strong* technical difficulty to threats to security mechanisms which currently may not be defeated because some theoretical elements for perpetrating an attack upon them are missing. A *Solvable* technical difficulty is associated with a security mechanism which may be countered or has been defeated in a related technology. A technical difficulty of *None* is assigned when a precedent for the attack already exists.

1.2.2 Impact on User and System

The *Impact* criterion evaluates the consequences for a user or a system if a given threat is carried out. Possible values for the impact are listed in Table 1.3.

Low Impact. From the single user's point of view, the impact of a threat is rated as *Low* if an attack results in only annoyance and the consequences, if there are any, are reversible and can be repaired. From the point of view of a system serving several users, a threat is ranked with *Low* impact if the possible outages are very limited in scope, for example with few users affected for a short duration.

Medium Impact. For the user, the impact is *Medium* if a loss of service occurs for a short amount of time. For a system, the consequences of a *Medium* impact threat consist of outages that are limited in both scope and possible financial losses.

High Impact. A threat carries a *High* impact for a user if an attack causes a loss of service for a considerable period of time. If targeted at a system, an attack associated with a *High* impact threat results in outages over a long period of time with a large number of users affected, possibly accompanied by law violations or substantial financial losses.

Table 1.3: Impact from the user or system point of view.

Low	Annoyance or very limited outage
Medium	Short-term loss of service or outage
High	Long-term loss of service or outage

1.3 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. An MS selects for its serving BS the one which offers the strongest signal. In this analysis, the subscriber plays the role of the user, while a BS and the collection of MSs represent a system.

The protocol architecture of WiMax/802.16 is structured into two main layers: the medium access control (MAC) layer and physical layer, as depicted in Figure 1.1. 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, which is tightly integrated with the Security 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, which adapts units of data (e.g. IP packets or ATM cells) from higher level protocols to the MAC SDU format, and vice versa. The Convergence layer also sorts the incoming MAC

SDUs by the connection to which they belong. The Security sub layer addresses authentication, establishment of keys and encryption, and exchanges MAC PDUs with the physical layer. The physical layer is a two-way mapping between MAC PDUs and the physical layer frames received and transmitted through coding and modulation of RF signals.

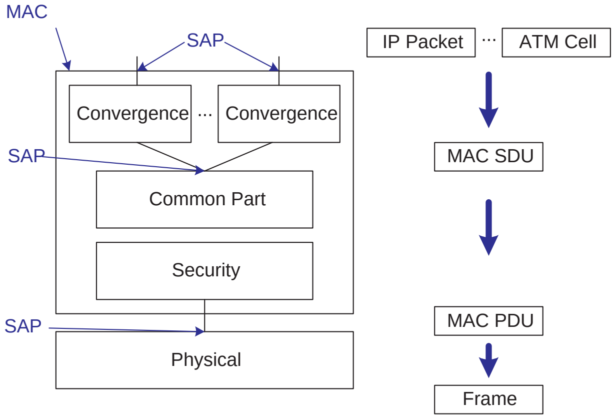

Figure 1.1: WiMax/802.16 layered architecture.

In our analysis, we examine the security threats first at the physical layer, then at the MAC layer. The results of the analysis are consolidated in Table 1.5.

1.3.1 Threats to the Physical Layer

In this section, we describe the frame structure used in the WiMax/802.16 physical layer and assess the possible threats therein.

Frame Structure

At the physical layer, the flow of bits is structured as a sequence of frames of equal length, as shown in Figure 1.2. There is a downlink subframe and an uplink subframe, and two modes of operation: frequency division duplex (FDD) and time division duplex (TDD). Figure 1.2 depicts 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 with each other because they are sent on different

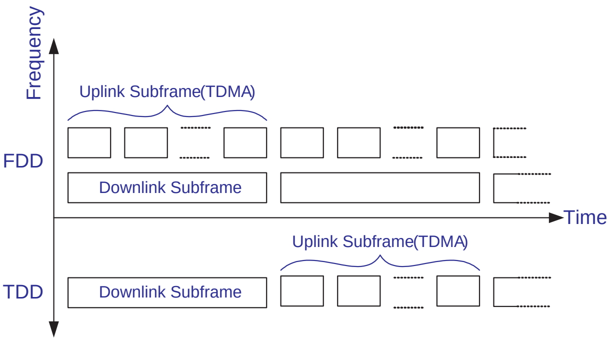

Figure 1.2: Physical layer framing.

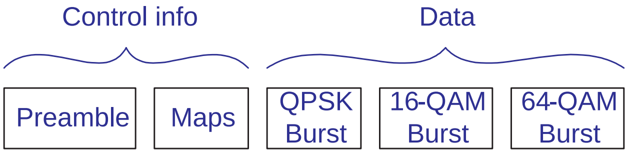

Figure 1.3: TDD downlink subframe.

frequencies. In TDD, the downlink subframe and uplink subframe are consecutive in time. A frame duration of 0.5, one or two milliseconds can be used.

All frames are of equal length. In TDD, the portion allocated for the downlink and the 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.

A detailed representation of a TDD downlink subframe illustrates the burst nature of the transmission and can be found in Figure 1.3. A downlink subframe consists of two main parts: the control information and the data. The control information consists of a preamble and maps. The preamble is used for frame synchronization purposes. There are two maps: a downlink map describes the start position and transmission characteristics of the following data bursts, and an uplink map disseminates 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 so and ignores the bursts it cannot demodulate.

Threats

Since the security sub-layer is above it, as represented in Figure 1.1, the physical layer is unsecured. 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. Since the attacker's aim is to creating mischief, the motivation can be rated as moderate. In terms of technical difficulty, the information and equipment required to perform jamming are not difficult to obtain. Poisel published a book on the topic of jamming alone, describing how to build jamming systems and counter systems which are by construction jamming resistant [19]. We therefore assess the difficulty to be very low, leading us to rate a jamming attack as possible, according to Table 1.2. Resilience to jamming can be augmented by increasing the power of signals or increasing the bandwidth of signals using spreading techniques, namely frequency hopping or direct sequence spread spectrum. Note that a number of options are available to raise the power of a signal, for example by using a more powerful transmitter, a high gain transmission antenna or 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, and 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 a user because of the limited loss of service and a medium impact on a system because of the short-term outages of limited scope and number of users. According to Table 1.1, the risk associated with jamming is therefore minor for a user and major for a system.

Scrambling is a sort of jamming, with similar motivation factors, that is carried out 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 the 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 another user). It is relatively more difficult to achieve scrambling than jamming because of the attacker's need to interpret control information and to send noise during specific intervals. There are technical difficulties for an attacker to address, but they are solvable. With the attacker motivation ranked as moderate because it is limited to creating mischief and with the technical difficulty solvable, the likelihood of occurrence of scrambling 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. [20]. The situation for WiMax/802.16 is much different, and further research is required for this case. The impact of scrambling is low because it results in annoyance to a limited number of users and the consequences are reversible, for example by retransmission. We believe that scrambling represents a minor risk at this time.

1.3.2 Threats to the MAC Layer

This section begins with an overview of the WiMax/802.16 MAC layer, including a description of its connections, the process used by an MS for joining the network and the MAC security model. We then proceed to discuss the threats to confidentiality and authentication.

MAC Layer Connections

The MAC layer is connection oriented. There are two kinds of connections: management connections and data transport connections.

Management connections are of three types: basic, primary and secondary. A basic connection is created for each MS when it joins the network and is used for short and urgent management messages. The primary connection is also created for each MS at the network entry time, but is used for delay tolerant management messages. The third management connection, the secondary one, 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 used for user traffic flows. Unicast or multicast can be used for transmission.

Network Entry

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 for downlink signals by going through the available frequencies and searches for downlink subframes. Whenever a channel is found, the MS gets the downlink and uplink description. It obtains the downlink map and uplink map in the physical frame headers, and these maps describe the structure of the subframes in terms of bursts. The downlink/uplink channel descriptors are obtained as MAC management messages, and they describe 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 using a special channel called the *ranging interval*, which uses contention-based multiple access. The basic connection and primary connection are assigned during ranging. Capabilities, for example the supported security algorithms, are negotiated on the basic connection. Authorization and authentication can be device list-based, X.509 certificate-based or EAP-based. This is discussed in more detail in the sequel. The registration step results in the establishment of a secondary management connection and provisioned connections.

Security Model

The security keys and associations established between an MS and a BS during the authorization step at network entry are discussed in this section.

A MAC layer PDU consists of a MAC header, a payload and an optional CRC. The payload may consist of user traffic or 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 are sent in the clear. According to the standard, this facilitates the operation of the MAC layer. 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 the 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. Each transport connection, a term used to refer to a MAC layer connection dedicated to user traffic, has either one SA for both the uplink and downlink, or two SAs, one for the uplink and another for the downlink.

The security model is depicted in Figure 1.4. Rectangles depict entities. Lines represent relations with cardinalities at the termination points. Preexisting elements are shown 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, and it is shared exclusively between an MS and its BS. Static SAs are created by the BS during the initialization of an MS. For example, there is a static SA for the basic unicast service. However, an MS may have subscribed to additional services, and there are as many additional static SAs as there are subscribed additional services. Dynamic SAs are created dynamically when new traffic flows are opened, and they are destroyed when their flow is terminated. Static SAs and dynamic SAs can be shared among several MSs, for example when multicast is used.

Core security 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 and 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, and they are subject to an aging process, so 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 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.

Threats to Confidentiality

The format of the MAC PDU payload is depicted in Figure 1.5. When applicable, before encryption, each packet is given a unique identifier 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 packets. The IEEE 802.16e standard 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. This standard introduces an integrity protection mechanism for data traffic which did not previously exist. CBC-MAC (as a component of AES-CCM) is used to protect the integrity of the payload of MAC data units.

Table 1.5 provides values for the *eavesdropping* threat, first for management messages, then for user traffic. Management messages, which are never encrypted, can provide valuable

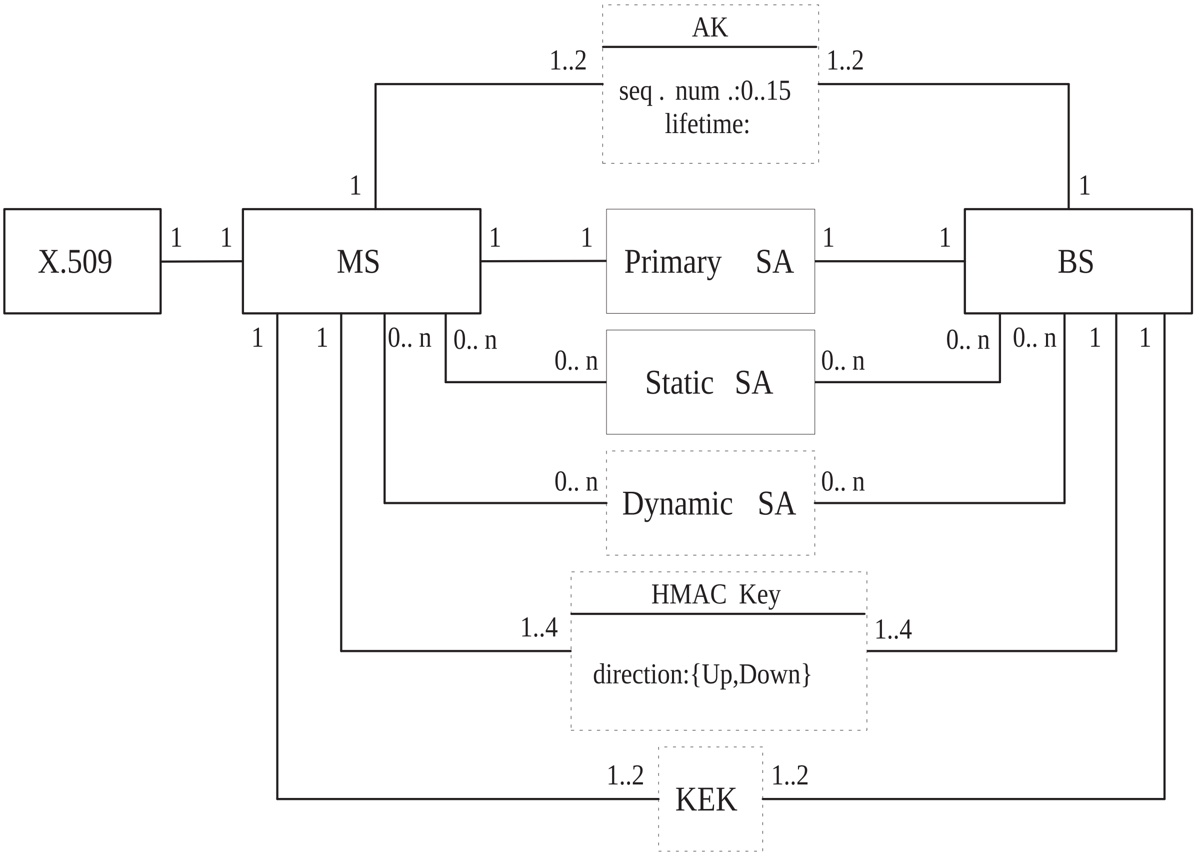

Figure 1.4: Security model.

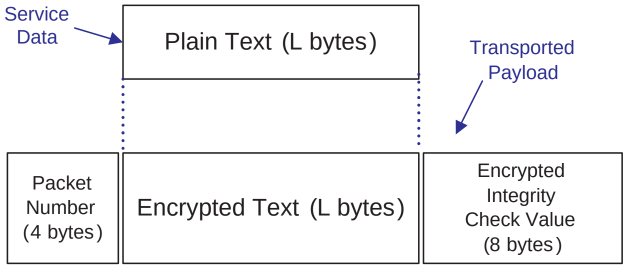

Figure 1.5: MAC layer PDU payload format.

information to an attacker, for example to verify the presence of a victim at his location before perpetrating a crime. This provides a high motivation for an attacker. The messages can be intercepted by a passive listener within communication range, so there are no serious technical difficulties to resolve by an attacker. The threat is therefore likely to occur. From the user perspective, eavesdropping of management messages may result in limited financial loss if a crime is committed, resulting in an attack of medium impact. From the point of view of a system, eavesdropping in itself may not create outages, but it might be used by a competitor to map the network, making it a threat of high impact. Hence, eavesdropping of management messages is a major threat for users and a critical one for a system.

Eavesdropping of data traffic is an unlikely threat because of the strong security measures provided by encryption, which presently pose unsurmountable technical difficulties. As a result, the threat is minor to both users and system, and there is no need for countermeasures.

Threats to Authentication

The kinds of authentication in WiMax/802.16 are listed in Table 1.4. There is device level authentication, which is RSA/X.509 certificate-based and is useful for detecting stolen devices and blocking their access to the network. The certificate can be programmed in a device by its manufacturer. This type of authentication is unilateral, i.e. BSs are not authenticated.

The IEEE 802.16 standard states that *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. In this case, a BS will grant network entry only to MSs featured on a pre-configured list, while an MS is configured with its network identifier and joins a BS only if it belongs to that network.

Any weakness in authentication is an enabler for the *BS or MS masquerading* threat, which may result in important gains for an attacker in terms of misappropriation of resources such as air time from another user or from a system. We therefore rate the attacker's motivation as high. Specific techniques for this threat include identity theft and the rogue BS attack.

Identity theft consists of reprogramming a device with the hardware address of another device. This is a well known problem in unlicensed services such as WiFi/802.11, but has been under control in cellular networks because it has 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 [15]. 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 to be a legitimate BS. The exact method of attack depends on the type of network. In a WiFi/802.11 network, which uses carrier sense multiple access, the attacker has to capture the identity of a legitimate access point (AP), build a message using the legitimate AP's identity, wait until the medium is idle and send the message. This appears to be one of the top security threats in WiFi/802.11 networks [9]. In a WiMax/802.16 network, this is more difficult to accomplish 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 MSs 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 build a message using that identity. The attacker has to wait until a time slot allocated to the legitimate BS starts. The attacker must then transmit while achieving a *receive signal strength*, a value in dBm, higher than that 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 the 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], which 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 [13].

There are three options for authentication: device list-based, X.509 based or EAP-based. If only device list-based authentication is used, identity theft by device address reprogramming is greatly facilitated, and the likelihood of a BS or MS masquerading attack is likely because there are few technical difficulties to solve. The impact for a user is high because it can lead to loss of service for long periods of time and the user can be billed for another user's communication fee. The impact for a system is medium because it can lead to limited financial loss or theft of resources. The risk is therefore critical for a user and major for a system, and there is the 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 and the solvable technical difficulties. The strong technical difficulties in MS masquerading render it an unlikely threat to a system. The impact is the same as for the device list-based authentication. Therefore, in the case of a user, the risk is assessed as major, 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 the likelihood of a BS or MS masquerading attack is possible. Some of the EAP methods are still being defined, and security flaws are often uncovered in *unproven* mechanisms. The technical difficulties in carrying out an attack are therefore best estimated as solvable. Aboba maintains a Web page about security vulnerabilities in EAP methods [1]. The impact is the same as for the device list and X.509 certificate-based authentication, so the risk is ranked as major for both a user and a system. It is a good idea to allow a second line of defense to play safe with EAP-based authentication.

The *modification of MAC management messages* poses a moderate motivation for an attacker because it stems from the goal to create mischief and results in limited gains. In terms of technical difficulty, MAC management messages are never encrypted and not always authenticated. If an authentication mechanism is used for MAC layer management messages, it is negotiated at network entry. The scope of management messages to which authentication is applicable is limited in earlier versions of IEEE 802.16, but has been extended in version *e*. Hence, with earlier versions of the IEEE 802.16 standard, the management messages are not subject to integrity protection.

Weaknesses in management message authentication open the door to aggressions such as the man in the middle attack, active attack and replay attack. However, the following authentication mechanisms are available: the hashed message authentication code (HMAC) tuple and the one-key message authentication code (OMAC) tuple. The OMAC is AES-based and includes replay protection. The HMAC authentication originally specified in the IEEE 802.16 standard did not provide a counter to protect against replay attacks, but version *e* does, so we distinguish both possibilities in our analysis. The technical difficulty in defeating the four different possibilities for authentication is as follows: *None* where no authentication is used, *Solvable* for the HMAC case with no replay protection, and *Strong* for both cases where the HMAC with replay protection or the OMAC defense is used. The likelihood of the management message modification threat is therefore possible for the first two cases and unlikely for the latter two. 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 therefore ranked as major for both cases where no authentication or HMAC without the replay counter is used, and minor for both the HMAC with the replay counter and the OMAC cases. As a result, it might be safe to allow a second line of defense against this type of attack.

Authentication of traffic messages also presents a moderate motivation for an attacker because it is an attack rooted in creating mischief. The *modification of data traffic* is very unlikely to occur if AES is used because of the strong technical difficulties encountered, and possible if AES is not used, given the lack of technical difficulty in carrying out an attack. We believe that such an attack has the potential to create short-term consequences for the user and system, resulting in a medium impact. If AES is not used, then this is a major threat, otherwise it is minor.

There is the potential for denial of service (*DoS*) attacks based on the fact that authen-

Table 1.4: 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

tication operations of devices, users and messages trigger the execution of long procedures. A DoS attack can be perpetrated by flooding a victim with a high number of messages to authenticate. With a moderate motivation on the part of the attacker bent on creating mischief, and with little technical difficulty to solve, this threat is possible. The impact is medium for a system, but could be high for a user because of lower computational resources available for handling a large influx of invalid messages. The DoS threat is therefore assessed as major for both users and system.

1.4 Conclusion

An analysis of the threats to the security of the WiMax/ 802.16 broadband wireless access networks was conducted. Critical threats consist of eavesdropping of management messages and BS masquerading. Major threats include jamming, MS masquerading, management message and data traffic modification, and DoS attacks. Countermeasures need to be devised for networks using the security options with critical or major risks. An intrusion detection system approach can be developed to address some of the threats, but more research is needed in this direction.

Table 1.5: Analysis summary from the user and system points of view.

Threat	Algorithm(s)	Likelihood	Impact	Risk
Jamming		Possible	*User:* Low	Minor
			System: Medium	Major
Scrambling		Possible	Low	Minor
Eavesdropping of management msgs		Likely	*User:* Medium	Major
			System: High	Critical
Eavesdropping of data traffic	DES-CBC, AES-CCM	Unlikely	Medium	Minor
BS or MS masquerading	Device list	Likely	*User:* High	Critical
			System: Medium	Major
	X.509 device auth.	*User:* Possible	High	Major
		System: Unlikely	Medium	Minor
	EAP	Possible	*User:* High	Major
			System: Medium	
Management message modification	No MAC	Possible	High	Major
	HMAC w/o counter			
	HMAC w/counter	Unlikely		Minor
	OMAC			
Data traffic modification	Without AES	Possible	Medium	Major
	With AES	Unlikely		Minor
DoS on BS or MS		Possible	*User:* High	Major
			System: Medium	

1.5 Acknowledgments

The authors 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 authors gratefully acknowledge the financial support received from the following organizations: Alcatel Canada, Automobile of the 21st Century (AUTO21), Mathematics of Information Technology and Complex Systems (MITACS) and Natural Sciences, and Engineering Research Council of Canada (NSERC).

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 authenti-

cation 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.J. Alberts and A.J. Dorofee. OCTAVE Criteria, Version 2.0. www.cert.org/octave/pubs.html, 2001.

[5] M. Barbeau. WiMax/802.16 Threat Analysis. *Proceedings of the 1st ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet)*, 2005.

[6] R. Barber. Hackers Profiled - Who Are They and What Are Their Motivations. *Computer Fraud & Security*, 2001(2):14–17, February 2001.

[7] R. Blake. Hackers in the Mist. www.eff.org/Net_culture/Hackers/hackers_in_the_mist.article, 1994.

[8] Club de la securité des systèmes d'information français (CLUSIF) Methods Commission. MEHARI V3 Concepts and Mechanisms. www.clusif.asso.fr/en/clusif/present, 2002.

[9] 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.

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

[11] 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.

[12] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography: 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001. Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 2259, 2001.

[13] F.J. Groen, C. Smidts, and A. Mosleh. QRAS - The Quantitative Risk Assessment System. *Reliability Engineering and System Safety*, 91(3):292–304, March 2006.

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

[15] IEEE, Computer Society. ANSI/IEEE Std 802.11 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Piscataway, NJ, 1999.

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

[17] 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 802.16-2004, 2004. (Revision of IEEE Std 802.16-2001).

[18] LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1. IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004), 2006.

[19] C. Laurendeau and M. Barbeau. Threats to Security in DSRC/WAVE. *Proceedings of the 5th International Conference on Ad Hoc Networks (ADHOC-NOW)*, 2006.

[20] E. Paté-Cornell. Finding and Fixing System Weaknesses: Probabilistic Methods and Applications of Engineering Risk Analysis. *Risk Analysis*, 22(2):319–334, 2002.

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

[22] 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.

[23] R. Schifreen. What Motivates a Hacker. *Network Security*, 1994(8):17–19, August 1994.

[24] A. Stubblefield, I. Ioannidis, and A. Rubin. Using the Fluhrer, Mantin and Shamir Attack to Break WEP. Proceedings of the 2002 Network and Distributed Systems Security Symposium, 17–22, 2002.

[25] WiFi, Alliance, Wi-Fi, Prottected Access (WPA) Enhanced Security Implementation Based on IEEE P802.11i Standard, Version 3.1. August, 2004.

[26] WiMax Forum. www.wimaxforum.org, 2006.