Denial of Service Vulnerabilities In the 802.16 Protocol

Siddharth Maru, Timothy X Brown
Dept. of Electrical and Computer Engineering
University of Colorado, Boulder, CO 80309 – 0530
{siddharth.maru,timxb}@colorado.edu

ABSTRACT

This paper examines the denial of service attacks that an 802.16 Broadband Wireless Access network is susceptible to at the physical and medium access control layers. In our threat model, we assume that the attacker is external to the network i.e. the attacker cannot associate with the network and send packets as a participant; nor can the attacker decrypt encrypted data. However, the attacker is able to analyze the unencrypted parts of the management traffic and observe the timing, size and source of traffic. Further, the attacker can send jamming signals that disrupt a specific packet and cause its contents to be discarded. In this scenario we analyze the vulnerabilities. We find that the attacker can prevent or hinder communication with little effort by disrupting certain important control packets. We detail these attacks and their effects. This analysis also suggests the mitigation techniques to be employed to reduce or eliminate such attacks.

Keywords

IEEE 802.16, denial of service, broadband wireless access, jamming, encryption, sensing, traffic analysis.

I. INTRODUCTION

WiMAX which is based on the IEEE 802.16 standard [1-4] is envisioned to provide fixed as well as mobile broadband wireless access. It provides an alternative to the wired broadband technologies such as cable and DSL. IEEE 802.16 refers to a suite of protocols designed to provide fixed, mobile, or meshed broadband wireless access whereby a Base Station (BS) provides high speed radio connectivity to subscriber stations (SS). However, the radio medium is open to intruders who can overhear, insert and interfere with packets to disrupt communication. Hence, like most other wireless technologies, WiMAX has security vulnerabilities which, if it were possible to create a significant disruption in communication with little effort from the attacker, could threaten its widespread deployment. In this paper, we consider transmitted packets disrupted by sending short bursts of noise. This noise would be strong enough to prevent the detection of the particular packet at the receiver. Such a disruptive attack is known as jamming and the effort expended by the attacker is expressed in terms of the jamming gain. As defined in [7], jamming gain is the increase in attacker's efficiency from exploiting features of the victim network relative to continuous jamming. Because jamming gain depends on specific implementations and the 802.16 documentation does not specify many key parameters, we will provide only qualitative jamming gain assessment. The aim here is to identify ways in which an attacker can exploit vulnerabilities in the specifications to cause a delay or disruption in services provided to the user of the network, so called denial of service, and to further identify mitigation techniques.

1.1 THE THREAT MODEL

In our threat model, we assume that the attacker is external to the network: i.e. the attacker cannot associate with the network and send packets as a participant; nor can the attacker decrypt encrypted data. However, the attacker is able to analyze the unencrypted parts of the traffic and observe the timing, size and source of frames. Further, the attacker can send jamming signals that disrupt a specific packet and cause its contents to be discarded. The precise jamming mechanism is not important here. Rather we try to understand what can be gained by intelligently analyzing the network traffic and jamming only a subset of traffic. The attacker's goal is to disrupt communication between the BS and SS. In carrying out attacks, we distinguish eight capabilities that might be required.

1) Attacker can jam packets to the SS.
2) Attacker can send packets to the SS (without actually associating with the network e.g. replay attack).
3) Attacker can receive packets from the SS.
4) Attacker can detect that packets have been sent from the SS.
5) Attacker can jam packets to the BS.
6) Attacker can send packets to the BS (without actually associating with the network).
7) Attacker can receive packets from the BS.
8) Attacker can detect that packets have been sent from the BS.

Siddharth Maru is a student at the University of Colorado, Boulder, CO 80309 USA (phone: 510-717-2928; e-mail: siddharth.maru@colorado.edu).

Timothy X Brown is with the Electrical and Computer Engineering Department, University of Colorado, Boulder, CO 80309 USA. (e-mail: timxb@colorado.edu).

WICON 2008, November 17-19, 2008, Maui, Hawaii, USA.

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849

1.2 PRIOR WORK

Others have looked into the vulnerabilities in the 802.16 standard. Barbeau [5] has looked into quantifying the impact of various kinds of attacks on an 802.16 network with the aim of identifying the significant ones. He found that the critical threats were eavesdropping of management messages, management message modification and denial of service (message flooding at the BS or SS). Boom [6] has looked into denial of service vulnerabilities of the 802.16 standard. Attacks discussed include the replay attack, the auth invalid attack and the RNG-RSP attack. Macari L. et al [9] have analyzed some critical issues in the family of IEEE 802.16 standards. In one of the attacks they claim that an attacker can reduce bandwidth assigned to its neighbors, with the aim of obtaining more resources for himself (a form of denial of service). Nasreldin M. et al [10] have tried to rank the various security threats in WiMax based on the level of risk they present. Arkoudi A. [11] has looked into the vulnerabilities of 802.16 in general to determine whether IEEE 802.16 is a secure protocol. He looks into attacks such as RNG-RSP attack and the Auth Invalid attack and suggests some enhancements to the 802.16 protocol. Krishnun S. [12] too has attempted to enumerate and classify security threats to 802.16 according to their risk levels. He identifies jamming and data traffic modification as the key threats. However, though others have identified jamming as a significant threat, the specifics of what packets to jam and the effort required have not been looked into in detail.

1.3 PAPER CONTRIBUTIONS

This paper contributes a detailed account of the important messages to be jammed to cause denial of service. We summarize a range of denial of service vulnerabilities in the 802.16 protocol. Based on our analysis, we then provide suggestions to avoid such attacks. These suggestions are classified into those that do and do not require modifications to the 802.16 protocol specifications.

We begin with an overview of the 802.16 components relevant to our analysis in Section II. We follow this up with a look at the source of the vulnerabilities and a brief discussion of the MAC management messages that give rise to these vulnerabilities in Section III. Armed with this information and the basic cause of vulnerabilities, we construct and analyze DoS attacks. We do this by looking at the DoS attacks at the physical layer in Section IV and those at the MAC layer in Section V. We then look at certain specific attacks which can result in high jamming gain in greater detail in the later sections. Section VI discusses the vulnerabilities and attacks on the Network Entry and Initialization Mechanism. Section VII discusses the DOS Traffic attacks. Section VIII discusses attacks on the Handover mechanism. In Section IX, we discuss some attacks which work in other wireless protocols but not in the 802.16 network. We follow this up with a summary of our findings in Section X and suggestions for mitigation of such attacks in Section XI.

II. 802.16 PROTOCOL LAYERS

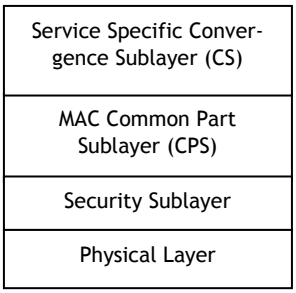

Figure 1: Layers in the 802.16 Protocol

The 802.16 protocol [3], [4] defines the Physical and the Medium Access Control (MAC) layers. The protocol supports a Point to Multipoint and Mesh topology. However, we develop our analysis on the Point to Multipoint topology and refer to the Mesh topology as and when necessary. Refer to Figure 1. The upper three layers in the figure constitute the Medium Access Control Layer. The lowest layer is the Physical Layer. The Service Specific Convergence Sublayer (CS) accepts higher layer protocol data units (PDUs) and transmits them to the MAC Common Part Sublayer (CPS). It also classifies and maps the data units into appropriate Connection Identifiers (CIDs). The CID is a 16 bit Identifier assigned to a logical connection (Uplink as well as Downlink) between the BS and SS. The MAC CPS performs the functions of a conventional MAC Sublayer.

The Security Sublayer provides security mechanisms for authentication and encryption of data across the network. The BS and SS establish shared security information (denoted Security Associations) between them to support secure communication. A client server model is used where the SS requests keying material and the BS responds to it by providing the keying material the SS is authorized to use.

The Physical Layer transmits and receives packets traversing the network. These packets are transmitted in the uplink as well as downlink channels in the form of bursts. A burst is a contiguous sequence of data transmitted using the same physical (PHY) parameters such as modulation scheme, error correcting codes etc. These PHY parameters constitute the burst profile. Successive bursts may be transmitted using different burst profiles. We analyze the MAC CPS, the Security Sublayer and the Physical Layer. However, first we investigate where these vulnerabilities are likely to stem from.

III. WHERE DO THE VULNERABILITIES STEM FROM?

There are two primary factors contributing to the vulnerabilities in this protocol.

A. The Physical Layer is Insecure

The Security Sublayer lies above the Physical Layer and below the MAC CPS. Hence, all the packets from the MAC CPS are encrypted, authenticated and validated. However, the headers and control information added by the physical layer are not encrypted or authenticated. This means that Physical layer information attached to the higher layer packets is vulnerable to analysis.

B. MAC Management Messages are Unencrypted

The MAC management messages (control information) are sent in the clear to facilitate network operations. Furthermore,

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849

information sent between a BS and SS before security associations have been negotiated is insecure and unauthenticated.

The messages which facilitate the network entry procedure are denoted DCD, UCD, DL-MAP, UL-MAP, RNG-REQ, RNG-RSP, PKM-REQ and PKM-RSP. These messages along with the MAC header play a role in the DoS attack. Table 1 discusses each of these MAC management messages and the information they provide to a passive eavesdropper.

To summarize, the vital information obtained from these critical messages includes: BS ID; CID; Individual Burst profiles; Frame Duration; Frame Number; BS Transmit Power; and PHY specification type. This information is enough to map a network and launch a DoS attack.

Table 1: 802.16 information sent unencrypted.

MAC Message	Description
MAC Header	The MAC Header is unencrypted. It contains the CID, length in bytes of the MAC PDU and a flag indicating whether the packet payload is encrypted or not.
DCD (Downlink Channel Descriptor)	It contains the Downlink Channel ID and the Downlink Burst Profile. The Downlink Burst Profile provides information about downlink channel which includes importantly the Modulation Type, FEC (Forward Error Correction) code Type and Parity Bytes.
DL-MAP (Downlink Map)	It contains the Base Station ID and the DL-MAP IE (Information Element). The DL-MAP IE contains information about the start time of each burst and maps the bursts to their corresponding burst profiles through the DIUC (Downlink Interval Usage Code).
UCD (Uplink Channel Descriptor)	It contains the Ranging and Request back off times and the Uplink Burst Profile.
UL-MAP (Uplink Map)	It contains the CID and the UL-MAP IE. It contains the same information as the DL-MAP but about the uplink channel.
RNG-REQ (Ranging Request)	It contains the Downlink Channel ID and at times the requested Downlink Burst Profile.
RNG-RSP (Ranging Response)	It contains the Uplink Channel ID, Timing Adjust Information, Power adjust information, Frame Number and Ranging Status.
PKM-REQ (Privacy Key Management Request)	It contains the authentication key sequence number, a security association identifier and a keyed message digest.
PKM-RSP (Privacy Key Management Response)	It contains the authentication key sequence number, Transport Encryption Key and Security Association ID.
SBC-REQ (Basic Capability Negotiation Request)	It contains the CID, list of physical parameters supported and the bandwidth allocation supported.
SBC-RSP (Basic Capability Negotiation Response)	It contains the CID and the corresponding list of parameters supported by the BS.

IV. Denial of Service Attacks at the Physical Layer

We now begin our layer by layer analysis by considering the Denial of Service attacks at the Physical Layer.

A. *Brute Force Jamming*

An attacker can prevent the transmission of packets across a network by introducing constant noise and consequently errors into the transmitted packets. However, such an attack would not be potent as the persistent high-power jamming signal can be detected and stopped.

B. *Precision Jamming*

Here the attacker jams only during the transmissions and only long enough to corrupt the frame. It requires detecting the transmitted frames and jamming for an appropriate amount of time. Jamming gain comes from jamming only a fraction of the frame e.g. jamming just the header will corrupt the entire frame. If you can determine how much of the header needs jammed versus the entire frame size, you can get an estimate of the jamming gain. This kind of an attack reduces attacker exposure.

C. *Targeted Jamming*

Another form of attack at the Physical Layer is known as targeted jamming. This kind of attack includes jamming only selected packets so as to disrupt transmission to specific destinations. Since, this kind of jamming is intermittent it is difficult to detect and avoid. Also, the amount of transmission power that an attacker has to use for such an attack is (on average) less than brute force jamming. However, this kind of an attack needs information about when specific packets are being transmitted. In case of the 802.16 protocol, this is not difficult as the MAC management messages are sent in the clear. The DL-MAP and UL-MAP (MAC management messages) messages indicate when bursts for a specific SS are being transmitted and enable targeted jamming. We will discuss these kinds of attacks in later sections when we discuss the network entry mechanisms.

D. *Message Flooding*

In message flooding, the attacker floods either the BS or SS with messages such that the overall performance of the network falls. Though the BS and SS will ultimately be able to reject these messages due to the failure to validate these messages, it will affect the number of messages either of them are able to process and hence reduce the network performance. Like brute-force jamming, the persistent transmission of messages can expose the attacker to detection. But, the message only needs to be strong enough to be received (as opposed to jamming which must be strong enough to overwhelm legitimate messages) and so may expose the attacker less. Also, flooding of messages is an abnormal activity which might depending on the implementation cause the BS to issue a RES-CMD (reset) message that will de-authenticate a SS. Thus, message flooding has some potential jamming gain.

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849

V. DENIAL OF SERVICE ATTACKS AT THE MAC LAYER

A. Vulnerabilities Prior to Secure Key Exchange

All messages communicated prior to secure key exchange between BS and SS are not authenticated. We describe two attacks arising out of this situation (discussed briefly in [6]). Like the message flooding attack, these attacks require the attacker to generate legitimate 802.16 messages.

1) RNG-RSP Attack

The ranging response (RNG-RSP) message is transmitted by the BS in response to the ranging request (RNG-REQ) message transmitted by the SS (during the Network Entry and Initialization mechanism). The RNG-RSP message contains the CID as well as other information used to fine tune the transmission parameters at the SS. However, the BS is also allowed to send unsolicited RNG-RSP messages to make changes to the transmission profiles if they do not match the requirements. In these cases, since the RNG-RSP message is not authenticated, an attacker can spoof these messages and send rogue messages to the SS with false timing information. This could lead to the SS transmitting in another SS's time slot. As a result the SS could be manipulated to cause errors in other SS messages that are beyond the direct range of the attacker. The RNG-RSP messages can also indicate to the SS to abandon the current channel and search for a new channel thus leading to the restart of the complete network entry and initialization procedure.

2) AUTH_INVALID Attack

The invalid authentication (AUTH_INVALID) message can be transmitted by the BS in response to a so-called PKM-REQ message. The PKM-REQ message is unencrypted and a part of the secure key exchange mechanism. Hence, if an attacker spoofs these messages and sends an AUTH_INVALID message to the SS, the key exchange will not only fail but it will also cause the SS to start the entry process again.

B. Carrier Sense Attack

This is a version of targeted jamming. In the uplink, the SS compete for slots to transmit data. This is accomplished by the use of contention windows. The SS select slots in the contention windows when they are supposed to transmit. If the SS does not receive an acknowledgement to the transmitted message in a fixed interval time, it assumes that a collision has taken place and it then picks a slot within a larger contention window. The UL-MAP message contains the details of the slot in which each SS is going to transmit. The UL-MAP message is transmitted in the clear and can be eavesdropped by an attacker. Hence, the attacker knows exactly at what time a particular subscriber station is likely to transmit. The attacker can then generate a message similar to the one transmitted by the SS and align itself to transmit at the same time that the SS will transmit. This will lead to a collision and consequently a degradation of the transmission of the messages in the uplink. This type of attack is difficult to detect and prevent as the attacker transmits for a very small amount of time. The result of this is a high jamming gain for the attacker.

VI. NETWORK ENTRY AND INITIALIZATION

Every SS when it first enters a network needs to perform Network Entry and Initialization. A sequence of critical MAC management messages are exchanged between the BS and SS during this procedure (Figure 2). If some of these critical management messages are jammed, the SS would be prevented from entering the network resulting in a denial of service. We discuss the impact of jamming these messages at each step of the procedure.

1) Physical Layer Synchronization: The SS scans potential downlink channels for a valid downlink signal.
2) Downlink Synchronization: The SS searches the downlink for a DL-MAP message. The SS also searches for the DCD message. The SS will stay in synchronization as long as it keeps receiving DL-MAP and DCD messages at specified intervals. The SS will wait for a time T21 (For Timer values refer to Table 3) after achieving PHY synchronization for the first DL-MAP. If it does not receive DL-MAP within that time, the SS will lose synchronization and start scanning the next downlink channel. After receiving the first DL-MAP message, the SS has to keep receiving the DL-MAP and DCD messages within time intervals LOST_DL-MAP and T1 respectively to remain in synchronization. If not, the SS will start scanning the next downlink channel.
3) Uplink Synchronization: The SS expects to see within T12 of receiving the first DL-MAP message a UCD message which describes characteristics of the uplink physical channel. If not the SS loses synchronization and restarts the network entry procedure. After the receipt of the UCD message, the SS expects to receive the UCD and UL-MAP at periodic intervals. If not received for a time specified by times T12 and LOST_UL-MAP respectively; synchronization is considered lost and the network entry procedure restarts. During this process of uplink synchronization, the UL-MAP defines time slots for unassociated SS to attempt to communicate on a contention basis.
4) Ranging: The first SS message is a RNG-REQ. However, these messages can be lost because of contention collisions or incorrect choice of initial parameters. The SS waits for time T3 for receiving the RNG-RSP message containing fine tuning information from the BS. If it is not received, the SS will retry over a longer contention window and possibly new initial parameters. This procedure is repeated until a retry counter is exhausted at which time the SS will restart the initialization procedure.
5) Basic Capability Exchange: After the initial ranging, the SS carries out capability negotiation by sending an SS basic capability request (SBC-REQ) message. If the SBC-RSP message is not received in a time equal to T18, the SS will reinitialize the whole entry procedure. It is also important that the SBC-REQ reaches the BS within time T9 after initial ranging; else the BS will release and age out the CIDs associated with this connection.
6) Authorization and key exchange: The authorization and

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849

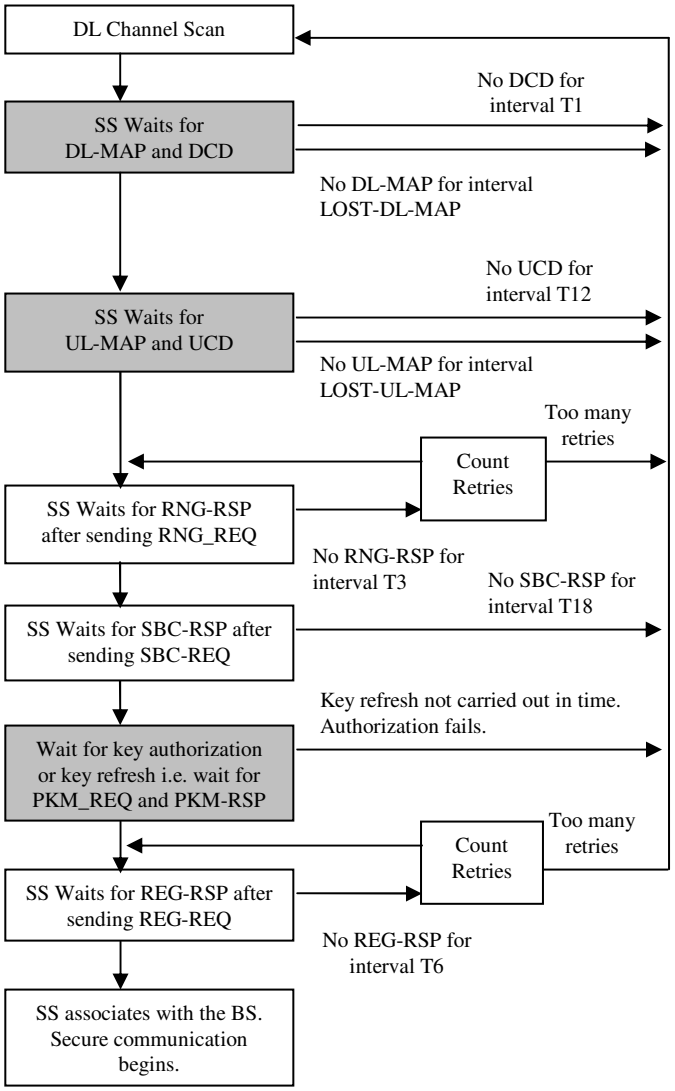

Figure 2: Flowchart indicating the various steps in the network entry and initialization procedure and the MAC management messages critical for its successful completion. The shaded boxes indicate the messages that must be received periodically. The messages in the other boxes have to be received one-time only.

key exchange is performed by the SS sending so-called PKM-REQ messages and the BS replying to them with PKM-RSP messages containing the Authentication Key. It is also imperative that the SS periodically send the PKM-REQ messages so as to keep refreshing the Authentication Key. If the keying material is not refreshed, the authorization fails and the SS has to restart the network entry procedure.

7) Registration Process: The SS sends the registration request (REG-REQ) message and waits for the response for time T6. If a response is not received within this time, the SS resends the REG-REQ. It keeps on retrying a fixed number of times after which it reinitializes the MAC and hence the network entry and initialization procedure would have to begin again.

As can be seen from the above discussion, an attacker has multiple opportunities to cause problems in the Network Entry and Initialization procedure. First, if the attacker jams enough DL-MAP and DCD messages and prevents the receipt of these messages over the said time intervals, it will make the SS move to the next channel to scan for a PHY frame (as in step 1 above) and restart the complete network entry procedure. Second, an attacker can jam specific MAC messages and let the last message get through before synchronization is lost, significantly delaying the network entry procedure without causing a telltale timeout. Third, even if synchronization is lost, time is wasted in searching for a new downlink channel. Fourth, during the Initial Ranging opportunity after the UL-MAP is received, if the attacker keeps jamming the particular slot where the SS transmits, the SS will back off and then randomly pick a slot in a longer transmission window, which if repeated sufficient number of times will cause the contention window to become very large and introduce a very large delay in the network entry procedure. Finally, if critical messages such as SBC-RSP and REG-RSP are jammed, the initialization mechanism needs to restart.

There are similar timers set in the Mesh Mode. Though the entry procedure is slightly different, the possibilities of attack and its impact in Mesh mode are similar and hence is not discussed separately here.

VII. DoS Traffic Attacks

Similar to during initialization, attacks can be affected in the Data Exchange mechanism and the mechanism for setting up Service flows. However, this traffic can be encrypted and would require more effort to identify the critical packets. An attacker may be interested in targeting specific types of information to specific users. Since the UL-MAP and DL-MAP are unencrypted, specific flows can potentially be identified and targeted by the attacker without affecting other flows. Finally, SS that have completed the initialization stage are still vulnerable to DoS attacks. The attacker can jam DL-MAP, UL-MAP, DCD, or UCD packets to the SS and cause a timeout that would in turn cause the station to restart the initialization procedure.

VIII. Vulnerabilities In The Handover Mechanism

A handover (HO) occurs when the MS moves and needs to change the BS which it is being served by to obtain better signal quality or a higher QoS. The handover is defined in the 802.16e specification. The aim of a handover is to seamlessly transfer a MS from the serving BS to a new target BS. The handover process consists of a number of stages during which different MAC management messages are exchanged to facilitate the transfer. At each of these stages, a DoS attack can be constructed by jamming certain critical management messages. We examine these attacks below.

A. Stage 1 - Cell Reselection:

1) Jamming of MOB_NBR-ADV message

During this stage, MS acquires neighboring BS information

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849

from the MOB_NBR-ADV message broadcast by the serving BS. This message eliminates the need for an MS to scan neighboring BSs for DCD/UCD broadcasts. Jamming this message which is sent every fixed interval of time, (MOB_NBR_ADV interval) would necessitate greater work by the MS in determining a suitable handover target BS. Though this attack does not cause a break down in the hand over mechanism, it can increase HO delay.

2) Jamming MOB_SCN-RSP message

During this stage, an MS also requests from the serving BS scanning intervals for scanning neighboring BSs for determining their suitability as a target for handover. This is done using the MOB_SCN-REQ and MOB_SCN-RSP messages. A MOB_SCN-REQ message is sent by an MS to the serving BS to request for scanning intervals. The MOB_SCN-RSP is BSs reply to the MOB_SCN-REQ message either granting or refusing the scanning intervals. If after observing the MOB_SCN-REQ message, the corresponding MOB-SCN_RSP message is jammed, the allocation of scanning intervals can be delayed. The MOB_SCN-REQ message is retransmitted if a MOB_SCN-RSP message is not received within time T44. Hence, we need to jam one MOB_SCN-RSP message every T44 interval to cause a denial of service.

3) Jamming messages indicating scan interval termination

The MOB_SCN-REQ and MOB_SCN-RSP messages are also used for termination of scanning intervals. If either of these messages is sent, with scan duration set to zero, the scanning intervals are terminated. Again, jamming these messages at such a time would prevent the termination of scanning intervals.

4) Jamming UL_MAP to terminate association

Attacking the Association mechanism would constitute another DoS attack. Association is an optional initial ranging procedure occurring during scanning intervals with respect to one of the BSs. The function of this procedure is to allow an MS to acquire and record ranging parameters and service availability information for selection of appropriate BS for handover. There are three types of Associations viz: Association without coordination, Association with coordination and Network assisted Association. Among these, Association with coordination and Network assisted Association are performed based on the information conveyed by the serving BS to the MS and neighboring BSs. These procedures however require that the MS receive a UL_MAP at the first frame following the rendezvous time. The Rendezvous time is the ranging interval provided by the neighboring BS for association in terms of the relative frame number. If however, the UL_MAP is jammed, the association procedure is terminated and further association occurs as per Association without coordination which does not use information from serving BS and consequently is more tedious. Thus, jamming the right UL_MAP message could prolong the association procedure.

B. Stage 2 - HO Decision and Initiation

The HO Initiation is indicated by the transmission of either the MOB_MSHO-REQ message by the MS or MOB_BSHO-REQ message by the BS. In reply to the MOB_MSHO-REQ message, the BS sends a MOB_BSHO-RSP message. Jamming of either of these messages for a sufficient number of times, could stop the handover process. After the transmission of MOB_MSHO-REQ message, the MS expects a response in a time interval given by MS_handover_retransmission_timer. If this time is exceeded, the MOB_MSHO-REQ message is retransmitted and this process continues until the retries are exhausted. Thus, jamming the MOB_MSHO-RSP message a sufficient number of times could cause the handover to fail.

Again, when the handover recommendation of the BS is rejected by the MS, it sends a MOB_HO-IND (HO-IND type = 10) message to the BS. If the BS fails to send a MOB_BSHO-REQ or a MOB_BSHO-RSP message within time T42 of this message, the handover is cancelled.

Thus, jamming of either of these messages could be a potent attack. A similar effect could be obtained by jamming the MOB_HO-IND message itself due to which the BS will not reply with the above mentioned messages in the stipulated amount of time, thus causing the handover to get cancelled.

C. Stage 3 - Synchronization to target BS downlink

Once, the handover to target BS has taken place, the MS has to carry out a procedure identical to initial ranging. The extent to which this procedure will have to be carried out would depend on the amount of information exchanged by the serving and target BSs over the backbone about the MS. This leads to an obvious DoS attack identical to the one in case of the Network Entry and Initialization mechanism.

IX. DENIAL OF SERVICE ATTACKS THAT DO NOT WORK

We now look at attacks which work in other wireless protocols but do not work in the 802.16 protocol due to some of the added security features (discussed briefly in [6]).

A. De-authentication Attack

The reset command (RES-CMD) and deregistration command (DREG-CMD) are issued by the BS to reset the subscriber station or to make the subscriber station repeat the network entry procedure. An attacker might try to issue these messages and reset the SS. In 802.11 a similar attack is possible and allows an attacker to kick users off the network [8]. However, in 802.16 the Security sublayer, ensures that most of the MAC management messages, including all those that are transmitted after the privacy key exchange is complete, are authenticated by appending a 160 bit authentication code (generated using a shared secret key). Thus the receiver can use the shared secret key to verify if the message is sent by an authenticated BS. Hence, the de-authentication attack will fail in case of this protocol. Note that though MAC management messages are authenticated, they are not encrypted.

B. Replay Attack

In a replay attack, the attacker captures a transmitted message and resends it after a certain amount of time. For exam-

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849

ple, if a BS issues a legitimate RES-CMD message, an attacker could capture it and replay it later causing a de-authentication attack.

When the HMAC is calculated for this message, the MAC header is included while calculating the message. The MAC header contains a CID field of the SS which is incremented after each new session of transmission. This leads to the break down of the replay attack. Thus, in general, all authenticated MAC management messages are not vulnerable to replay attack. Also, if you assume the case where the BS repeats a transmission with the same CID, it will negotiate a new set of secret keys requiring the recalculation of the HMAC digest. Thus, the replay attack here fails on two counts.

Due, to the inclusion of the HMAC, all authenticated messages in the 802.16 protocol are not vulnerable to Replay attacks.

C. Access Point Spoofing

In access point spoofing the attacker pretends to be a legitimate BS. SS that associate may reveal private information or receive little or no useful service. The danger of access point spoofing existed in the 802.16-2004 specification. This specification only mentions the requirement for the SS to be authenticated using Digital Certificates without requiring the BS to be authenticated. Thus, an attacker can pose as a BS and launch a DoS attack. However, 802.16e includes the requirement of mutual authentication using either EAP or X.509 certificate before management messages are exchanged between them. Thus, a strong mutual authentication mechanism has all but eliminated the possibility of an Access Point Spoof.

D. Message Injection

For an attacker to inject MAC management messages into the network, there are a number of hurdles. First, it is important to decide what message is to be transmitted. Also, the attacker needs to transmit at the precise time indicated in the DL-MAP and UL-MAP messages. Though, the attacker has timing information, it could be difficult to implement this due to the finite delay between detection of the timing information and generation of messages to be injected. The message injection by an attacker is also thwarted by the use of HMAC which is not available to him. Hence, like the replay attack, message injection is not possible.

We summarize all the attacks, capabilities required by the attacker, the effort required and the consequences in Table 2.

X. SUMMARY

We have found that, by jamming certain critical control packets, it is possible to realize significant jamming gain. The protocol specifications that make this possible are:

1) Even with the strongest specified encryption and authentication, elements of the protocol are sent in the clear and can open significant lines of analysis for exploitation.
2) Management messages are sent unencrypted so that they can be easily identified. Management messages are critical to maintaining the association between a SS and BS. Jamming specific frames (described above) can prevent a SS from associating or cause it to lose association and have to reinitialize with the network.
3) The mapping of BS frames to specific connections is sent in the clear. It identifies which parts of the frame belong to specific connections. The identification is through an abstract connection identifier; however, minimal analysis would be able to associate connection identifiers to specific user streams. Conversely, the SS frames are also mapped in the clear so that an attacker can anticipate transmissions from a specific user. These open mappings would enable an attacker to target specific users or even specific traffic (e.g. a voice connection) from a specific user.
4) The so-called initialization process whereby a new SS acquires and associates to a BS is brittle and easily broken. In any of a half a dozen steps in the initialization sequence the attacker can jam critical management messages to the SS or BS so that association is delayed by 10's of seconds or is outright prevented indefinitely.
5) Before the authentication process is completed, an attacker can send false messages to the SS causing it either to restart initialization or to potentially interfere with other users. Once associated, a SS must hear certain management frames periodically or it considers the association lost. An attacker can jam these messages to a SS until it stops communication.
6) An attacker can jam critical management messages at each of the three stages of the handover process and cause a delay or disruption in the hand over mechanism.

XI. RECOMMENDATIONS AND SUGGESTIONS

Vulnerability mitigation can be done in two ways. One way is to modify the protocol so that the existing security issues are eliminated. However, there are certain attacks which can be avoided simply by changing the operating conditions and without modifying the protocol. We discuss both the approaches below.

Modifications to the protocol

1) *Transmitting the initial ranging messages securely by using public key cryptography:* Encrypting the messages will make it difficult for the attacker to identify what messages are being transmitted at a particular instant thus making his decision of whether to jam or not difficult
2) *Encrypting MAC management messages:* This will ensure that an attacker is unable to gain information about the exact locations of the bursts intended for a particular recipient SS. Thus, it will become difficult for an attacker to target messages bound for a specific customer.
3) *Authenticating all management messages using Hash functions:* This precaution helps us in avoiding RNG-RSP attacks whereby an attacker sends a RNG-RSP message with incorrect parameters to the SS. Once authenticated,

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849

the SS will easily be able to discard all messages not sent by the Base Station.

4) *Using Spread Spectrum techniques to avoid physical layer jamming:* This approach provides resistance to jamming.

Modifications to the Operating Conditions

Now we look at some attacks that we can prevent simply by changing the operating conditions:

1) *Using highly directional transmit and receive antennas:* This can reduce exposure to jamming and interception.
2) *Increasing the power of the transmitted signal:* This has better protection against jamming at the expense of greater battery drain in battery operated devices and potential negative impact on cell planning.

We can conclude that to quell the most efficient and the majority of the attacks we have discussed; changes to the protocol are required. Changing Operating conditions will only have a limited impact on mitigating the risk of Denial of Service Attacks.

XII. ACKNOWLEDGMENT

This work was funded by AFRL award FA8750-07-1-0079.

XIII. REFERENCES

[1] Todor, C., *Wireless Communication Standards – A Study of IEEE 802.11, 802.15 and 802.16,* Standards Information Network/IEEE Press, p.360, (2004).

[2] Loutfi, N., *WiMAX: Technology for Broadband Wireless Access,* John Wiley and Sons, p.283, (2007).

[3] IEEE, *IEEE Standards 802.16 – IEEE standard for Local and Metropolitan Area Networks – Air Interface for Fixed Broadband Wireless Access Systems,* IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, (October 2004).

[4] IEEE, *IEEE 802.16e – Part 16: IEEE Standard for Local and Metropolitan Area Networks – Air Interface for Fixed and Mobile Broadband Wireless Access Systems*, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society (February 2006).

[5] Barbeau, M., *WiMAX/802.16 Threat Analysis*, Proc. of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks, p.8-15, (October 10-13, 2005).

[6] Boom, D., *Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks,* Naval Postgraduate School, Thesis, (September 2004).

Table 2: Summary of the Various DoS Attacks, Capabilities required by attacker, the Effort required and the Consequences.
J: Jam target TX: Transmit to target RX: Receive from target D: Detect target transmissions

ATTACK	CAPABILITIES								EFFORT	CONSEQUENCE
	SS				BS					
	J	TX	RX	D	J	TX	RX	D		
Brute Force Jamming	x								Persistent noise signal. Jamming gain = 1	Disruption of communication. Can be targeted through directional antennas.
					x					
Precision Jamming	x								Jam only during a fraction of the frame duration. Effort will be determined by comparing the duration for which the frame is jammed with the total duration of the frame.	Corruption of the frame with limited exposure of the attacker
					x					
Targeted Jamming	x						x		Intermittent Jamming of critical packets. Jamming gain > 1 and depends on the frequency of jamming.	Can disrupt specific SS or connections. Intermittent jamming more difficult to detect.
			x		x					
Message Flooding		x							Requires Persistent injection of spurious packets similar to brute force jamming.	Can starve receivers of processing resources. It could also lead the BS to reset a SS.
						x				
Carrier Sense Attack				x	x				Targeted jamming of packets during contention access at SS network initialization.	Prevent or delay network entry. Can appear as legitimate contention user.
RNG-RSP attack			x			x			The attacker must generate a valid RNG-RSP message. These are not authenticated prior to establishing a security association and can be injected during initialization.	Can command the SS to reset. Incorrect timing offset or power level information causes SS to misbehave and the BS abandons initialization. Intermittent transmission harder to detect.
AUTH_ INVALID attack			x			x			The attacker must generate a valid AUTH_INVALID message. These are not authenticated prior to establishing a security association. Must be injected at the appropriate time.	Causes the SS to abandon key exchange and restart network initialization. Intermittent transmission harder to detect.
Network Entry and Initialization Reset Attack	x						x		Targeted jamming of specific packets for specific timeout intervals. The amount of effort required will vary depending on the PHY specification (how often specific packets are sent and timeout values).	Causes the SS to restart network initialization. Attack is robust. If one stage fails can attempt in later stage. Intermittent jamming more difficult to detect. Alternatively can delay network entry.
DOS Traffic Attacks			x		x				Traffic is encrypted, but, can use unencrypted management information to target specific connections. Certain management packets can be targeted to reset the connection.	Specific connections can be jammed while others are unaffected. Can reset the connection.
Hand Over Mechanism Attack	x							x	Targeted jamming of specific packets for specific timeout intervals. The amount of effort will depend on the number of retries allowed for each of these messages.	Hand Over mechanism can be delayed, made more tedious or cancelled depending on which message is jammed.
				x	x					

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849

[7] Brown, Timothy, X., James, Jesse, E., Sethi, Amita, *Jamming and Sensing of Encrypted Wireless Adhoc Networks*, Proc. of the Seventh ACM International Symposium on Mobile Adhoc Networking and Computing (MobiHoc), p.120-130 (May 22-25, 2006).

[8] Bellardo, J., Savage, S., *802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions*, Proc. of the USENIX Security Symposium, *Washington D.C.,* (August 2003).

[9] Maccari, L., Paoli, M., Fantacci, R., *Security Analysis of IEEE 802.16*, Proc of Communications, 2007. ICC'07. IEEE International Conference on, Glasgow (Scotland), (24 – 28 June 2007).

[10] Nasreldin, M., Asian, H., El-Hennawy, M., El-Hennawy, A., *WiMax Security*, Proc of Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on, (25 – 28 March 2008).

[11] Arkoudi, A., *Security of IEEE 802.16*, Royal Institute of Technology, Thesis, (2006).

[12] Krishnun, S., *An assessment of threats of the Physical and MAC Address Layers in WiMAX/802.16*, Edith Cowan University, Report.

Table 3: Timer values and recommended settings

System	Name	Time Reference	Minimum Value	Default Value	Maximum Value
BS	Invited Ranging Retries	Number of retries on inviting ranging request	16	-	-
SS	T1	Wait for DCD Timeout	-	-	50 sec
SS, MS	T3	Ranging Response reception timeout following the transmission of a Ranging Request	-	50 ms	200 ms
SS	T6	Wait for registration response	-	-	3 s
BS	T9	Registration timeout, the time allowed between the BS sending a RNG-RSP to an SS, and receiving a SBC-REQ from that same SS	300 ms	300 ms	-
SS	T12	Wait for UCD descriptor	-	-	50 sec
SS	T18	Wait for SBC-RSP timeout	-	50 ms	<<T9
SS	T20	Time the SS searches for preambles on a given channel	2 MAC frames	-	-
SS	Lost DL-MAP interval	Time since last received DL-MAP message before downlink synchronization is considered lost	-	-	600 ms
SS	Lost UL-MAP interval	Time since last received UL-MAP message before uplink synchronization is considered lost	-	-	600 ms
BS	DCD Interval	Time between transmission of DCD messages	-	-	10 s
BS	UCD Interval	Time between transmission of UCD messages	-	-	10 s
SS	T21	Time the SS searches for a decodable DL-MAP on a given channel	-	-	11 s
SS	T23	Network Entry: Detect Network	1 s	-	-
BS	MOB-NBR-ADV-interval	Nominal time between transmission of MOB-NBR-ADV messages.	-	-	30 s
MS	T42	MOB_HO-IND timeout when sent with HO_IND_type = 0b10.	-	-	-
MS	T44	Time the MS waits for MOB_SCN-RSP.	-	-	-

Digital Object Identifier: 10.4108/ICST.WICON2008.4849
http://dx.doi.org/10.4108/ICST.WICON2008.4849