| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | **Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks** |
| Date Submitted | **2004-10-05** |
| Source(s) | Derrick Boom<br>c/o Rex Buddenberg<br>Naval Postgraduate School<br>Monterey, Ca 93943<br><br>Voice: 831/656-3576<br>Fax: [Fax Number]<br>mailto:budden@nps.navy.mil |
| Re: | Masters Thesis |
| Abstract | The Institute of Electrical and Electronics Engineers' new 802.16 standard is set to revolutionize the delivery of Broadband Wireless Access (BWA), much as the 802.11 "Wi-Fi" standard transformed wireless access to Local Area Networks. The standard describes a set of Medium Access Controls (MAC) and Air Interfaces that cover a broad range of broadcast frequencies and applications. As a result, manufacturers are developing 802.16 compliant equipment for high speed point-to-point circuits and point-to-multipoint circuits dubbed Wireless Metropolitan Area Networks (WMANs). These networks can span several miles and contain hundreds of subscribers. Shortly after 802.11 "Wi-Fi" systems became widespread, several serious Denial of Service (DoS) vulnerabilities inherent to the standard were discovered. This thesis examines the MAC layer of the 802.16 standard to determine whether these types of denial of service vulnerabilities are also present in the new standard. Also examined are vulnerabilities that may be new to the 802.16 standard. |
| Purpose | Provided for information. This might cause some revision of the standard to close some of the security vectors uncovered and discussed. |
| Notice | This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16. |
| Patent Policy and Procedures | The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>. |


# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**DENIAL OF SERVICE VULNERABILITIES IN IEEE 802.16 WIRELESS NETWORKS**

by

Derrick D. Boom

September 2004

| | |
|---|---|
| Thesis Advisor: | Rex Buddenberg |
| Second Reader: | Brian Steckler |

**Approved for public release; distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503. | | | |
| **1. AGENCY USE ONLY** ***(Leave blank)*** | **2. REPORT DATE** September 2004 | **3. REPORT TYPE AND DATES COVERED** Master's Thesis | |
| **4. TITLE AND SUBTITLE**: Denial of Service Vulnerabilities IEEE 802.16 Wireless Networks | | | **5. FUNDING NUMBERS** |
| **6. AUTHOR(S)** Derrick D. Boom | | | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | | | **8. PERFORMING ORGANIZATION REPORT NUMBER** |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | | | **10. SPONSORING/MONITORING AGENCY REPORT NUMBER** |
| **11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. | | | |
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release; distribution is unlimited. | | | **12b. DISTRIBUTION CODE** |

**13. ABSTRACT (maximum 200 words)**

The Institute of Electrical and Electronics Engineers' new 802.16 standard is set to revolutionize the delivery of Broadband Wireless Access (BWA), much as the 802.11 "Wi-Fi" standard transformed wireless access to Local Area Networks. The standard describes a set of Medium Access Controls (MAC) and Air Interfaces that cover a broad range of broadcast frequencies and applications. As a result, manufacturers are developing 802.16 compliant equipment for high speed point-to-point circuits and point-to-multipoint circuits dubbed Wireless Metropolitan Area Networks (WMANs). These networks can span several miles and contain hundreds of subscribers. Shortly after 802.11 "Wi-Fi" systems became widespread, several serious Denial of Service (DoS) vulnerabilities inherent to the standard were discovered. This thesis examines the MAC layer of the 802.16 standard to determine whether these types of denial of service vulnerabilities are also present in the new standard. Also examined are vulnerabilities that may be unique to the 802.16 standard.

| **14. SUBJECT TERMS** Wireless Security, IEEE 802.16, IEEE 802.11, Denial of Service | | | **15. NUMBER OF PAGES** 87 |
|---|---|---|---|
| | | | **16. PRICE CODE** |
| **17. SECURITY CLASSIFICATION OF REPORT** Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified | **20. LIMITATION OF ABSTRACT** UL |

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited.**

# DENIAL OF SERVICE VULNERABILITIES IN IEEE 802.16 WIRELESS NETWORKS

Derrick D. Boom
Lieutenant, United States Navy
B.S., Oregon State University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS ENGINEERING**

from the

**NAVAL POSTGRADUATE SCHOOL**
**September 2004**

Author: Derrick D. Boom

Approved by: Rex Buddenberg
Thesis Advisor

Brian Steckler
Second Reader/Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

The Institute of Electrical and Electronics Engineers' new 802.16 standard is set to revolutionize the delivery of Broadband Wireless Access (BWA), much as the IEEE 802.11 "Wi-Fi" standard transformed wireless access to Local Area Networks. The standard describes a set of Medium Access Controls (MAC) and Air Interfaces that cover a broad range of broadcast frequencies and applications. As a result, manufacturers are developing IEEE 802.16 compliant equipment for high speed point-to-point circuits and point-to-multipoint circuits dubbed Wireless Metropolitan Area Networks (WMANs). These networks can span several miles and contain hundreds of subscribers. Shortly after IEEE 802.11 "Wi-Fi" systems became widespread, several serious Denial of Service (DoS) vulnerabilities inherent to the standard were discovered. This thesis examines the MAC layer of the 802.16 standard to determine whether these types of denial of service vulnerabilities are also present in the new standard. Also examined are vulnerabilities that may be unique to the 802.16 standard.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

I would like to thank Professor Rex Buddenberg for his guidance and insight. Without your help I'd never have gotten out of the starting blocks.

I would like to express my appreciation to the US Navy for the wealth of education and training I have received over the course of my sixteen years of service. I joined the Navy as a college drop-out waiting tables to make ends meet. Thanks to the opportunities the Navy has offered, I'm now a Submarine Officer with a Master's Degree in Systems Engineering. I am looking forward to returning to the submarine fleet.

Finally, I'd like to thank my wife and children for their love, patience and understanding. The life of a Navy family is not an easy one, and they have supported me every step of the way.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. BACKGROUND

In homes and offices around the globe, Wireless Local Area Networks (WLANs) have become commonplace. They have proven enormously popular, with millions of wireless cards and routers with integrated access points sold to date. The reasons for this popularity are manifold. These networks are truly routable, working seamlessly with wired LAN equipment. They are also capable of operating at data rates close to those of their wired equivalents. Finally, most WLAN equipment is completely vendor neutral and quite inexpensive.

These advantages are made possible by the fact that virtually all WLAN deployments are built around standards-based equipment, rather than proprietary systems. When the Institute of Electrical and Electronics Engineers (IEEE) released its IEEE 802.11 standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications in 1999 it paved the way for the mass production of vendor interoperable equipment. To guarantee that each new piece of wireless equipment will work with the rest of the network, strict adherence to the IEEE 802.11 standard was enforced by third party interoperability testing. This testing and subsequent "Wi-Fi" branding was conducted by an international industry association known as the Wi-Fi Alliance. Freedom to choose the network equipment creates cost competition among manufacturers, which leads to downward spiraling prices and exponentially rising sales. To date, the Wi-Fi Alliance has certified over 1250 products from over 200 vendors [1].

Given the enormous demand for broadband wireless access, and the commercial success of standards based equipment, extending the reach of wireless networks becomes a logical next step, and the Institute of Electrical and Electronics Engineers released its 802.16 standard in 2001 [2]. Where the better known IEEE 802.11 Standard forms the basis for wireless Local Area Networks with a handful of users inside a few hundred meter radius, the IEEE 802.16 standard enables much larger networks. Dubbed "Metropolitan Area Networks" (MANs), these new networks are meant to provide service to hundreds, or even thousands of users across a city-sized network. The IEEE

802.16 standard defines the air interface for a fixed, broadband wireless network with operating frequencies from 2 to 66 GHz, along with a variety of physical layer specifications. The standard encompasses point-to-point (PTP) and point-to-multipoint (PMP) modes as well as mesh networks.

Formally known as "IEEE Std. 802.16-2004 Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," the standard was ratified on 24 June, 2004 [3]. This standard is a revision of the earliest version of the standard 802.16-2001, and was created by integrating extensions 802.16a-2003 and 802.16c-2002 into the basic standard. The earliest standard had evolved from its basic specification for operating frequencies in the 10 – 66 GHz range to include mesh and non line-of-sight extensions. These extensions included new physical layer specifications which add coverage in the 2 – 11 GHz range. Importantly, the standard incorporates differential Quality of Service (QoS) at its core, making it ideal for jitter-intolerant services such as voice and streaming video. The QoS parameters built into the standard include minimum traffic rate, tolerated jitter and maximum latency. There is also built in support for vendor specified QoS parameters. Networks and equipment have been planned to service a wide variety of scenarios, from commercial wireless backhaul for cell-phone companies to residential broadband internet.

Equipment built under the 802.16 standard is collectively marketed under the WiMAX banner. Analogous to the Wi-Fi Alliance, the WiMAX Forum ensures compliance with the 802.16 standard. WiMAX Forum members include Intel Corporation, Motorola and AT&T Research among many others. With heavy consumer and commercial demand, broad industry support and a well developed standard, sales of 802.16 compliant equipment are expected to soar in the coming years [4].

## B. THE DENIAL OF SERVICE CONCEPT

While the phrase "denial of service" is fairly new, the concept is not. As far back as the American Civil War, denial of service attacks plagued the communications networks of North and South alike. In that era, the targets were telegraph lines, with attacks consisting of raids to physically cut the wires that crossed the countryside. In one

area, Southern guerilla attacks against the telegraph lines were so problematic, that General U. S. Grant resorted to a twenty mile length of underwater cable – no mean feat in 1864. Today, however, we have a vastly different view of denial of service attacks. No longer seen only in warfare, denial of service attacks have been conducted by everyone from teenagers to terrorists in recent years.

Denial of Service attacks may employ one of several attack paradigms. Military jamming denial of services often simply flood the airwaves with unintelligible noise signals. Like military jamming, many of the denial of service attacks carried out across the Internet are also brute force attacks that flood the propagation medium with noise. However, there are several important features of these attacks that make them very unlike military jamming. Rather than injecting energy from outside the network, the Internet denial of service attack works by using the network against itself. Like a lever, the exploited network multiplies the force applied by the attacker by abusing the very mechanisms that make the network possible. With just a relative few requests, attackers are able to cause a flood of millions of information requests to be directed against the target computers. The victim is overwhelmed by the sheer volume of traffic, with either its network bandwidth or its computing power exhausted by the flood of information.

These brute force attacks work by exhausting a limited resource, whether it is radio frequency spectrum, network bandwidth or computational capacity. There are, however, other methods of attack that can be very effective while using just a tiny fraction of the available data channel. These attacks work by exploiting the assumption that every member of a network will always follow the rules of the network. A single misbehaving node can wreak havoc on a network, whether its behavior is malicious or unintentional. In early Ethernet applications, a single interface card could unintentionally flood the network with data packets. The error control method employed by the network only exacerbated the problem. Often, the only real solution was to search for the rogue node and remove it from the network. Attacks based on exploiting network transport and control mechanisms have been seen in a variety of settings, including the wired Internet and wireless networks.

## C. THESIS OBJECTIVES AND ORGANIZATION

Given the success of the IEEE 802.11 standard, and the industry support for WiMAX, there is a significant probability that IEEE 802.16 compliant networks will see widespread use in commercial and military applications. 802.16 compliant equipment has only recently been deployed in commercial settings; however there are already efforts underway to adapt these systems to US military needs [5], [6]. This presents a significant new opportunity in the context of Offensive Information Operations(OIO), as well as potential pitfalls for Defensive Information Operations (DIO). Of the entire spectrum of threats and vulnerabilities, this thesis will focus exclusively on denial of service attacks at the medium access control level, as opposed to physical layer brute force jamming or higher layer packet floods. The tactical networks that may soon be deployed using 802.16 compliant equipment will need very high availability, even in the face of adversaries actively seeking to deny and disrupt network services. By understanding the denial of service vulnerabilities inherent to the MAC from the outset, procurement and deployment plans may be shaped to minimize the threat to friendly systems, while allowing time to develop tools and techniques for Offensive Information Operations. Malicious exploitation of the communication protocol has been shown to provide a highly effective denial of service attack against IEEE 802.11 based networks. These types of attacks can be particularly difficult to counter, as they require only sporadic, low power transmissions to implement. Also, they require little modification to commercially available systems and virtually no specialized equipment to implement.

There are several serious flaws inherent to the IEEE 802.11 standard that create Denial of Service (DoS) vulnerabilities. This thesis examines the 802.16 standard to determine whether these types of denial of service vulnerabilities are also present in the new standard. Also examined are vulnerabilities that may be unique to the 802.16 standard.

Chapter II is an overview of the basic IEEE 802.16 standard and its various extensions, with emphasis on the Medium Access Layer (MAC) and Privacy Sublayer, which are common to all of the point-to-multipoint (PMP) portions of the standard. These layers are crucial to understanding the types of denial of service attacks to which the standard is vulnerable. To help understand deployment scenarios and how IEEE

802.16 links are integrated into the overall network architecture, real-world example networks are presented to form the basis for attack scenarios.

Chapter III is a comparison of IEEE standards 802.11 and 802.16, showing how the newer standard handles the DoS attacks that are effective against 802.11. Exploitation methodologies and scenarios are also presented in this chapter. Also discussed is the role that IEEE 802.16's security measures play in defending against these attacks.

Chapter IV is a discussion of potential denial of service vulnerabilities that are new or unique to the IEEE 802.16 standard. This chapter points out ways in which certain MAC layer messages may be abused to create Denial of Service attacks that target the MAC layer. Difficulties that will be faced by an attacker seeking to generate and transmit spoofed messages are addressed. Also presented are general conclusions concerning the mechanisms that make these abuses possible.

Chapter V contains conclusions and recommendations for further research. This chapter also includes a list of recommended changes to the standard, both general and specific.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. OVERVIEW OF IEEE 802.16 STANDARD

A brief overview of the IEEE 802.16 standard is provided to form the basis for further discussion. The focus will be on the portions of the standard that are most pertinent to this work. This chapter is based on the detailed standard specification, IEEE 802.16-2001 [2] as well as the extensions to the standard, IEEE 802.16a-2003 [7] and IEEE 802.16c-2002 [8]. The latest version of the standard, IEEE 802.16-2004 [3] was not available at the time of this writing. Because IEEE 802.16-2004 [3] is an integration of 802.16-2001, IEEE 802.16a-2003 and IEEE 802.16c-2002, rather than a re-write, this research maintains a high degree of fidelity to the newest standard. Also in this chapter is a description of a real-world IEEE 802.16 network which will serve as the nominal attack target.

## A. INTRODUCTION TO THE IEEE 802.16 ARCHITECTURE

The IEEE 802.16 standard specifies the Physical (PHY) Layer and Medium Access Control (MAC) layer for broadband wireless access (BWA) within a Metropolitan Area Network (MAN). The IEEE 802.16 fills the gap between the IEEE 802.2 Logical Link Layer and the air interface. Along with the bridging capabilities specified in IEEE 802.1, these standards and their higher layer access mechanisms can be used to create fully routable networks. Figure 1 illustrates 802.16's place in the hierarchy of IEEE 802 standards.

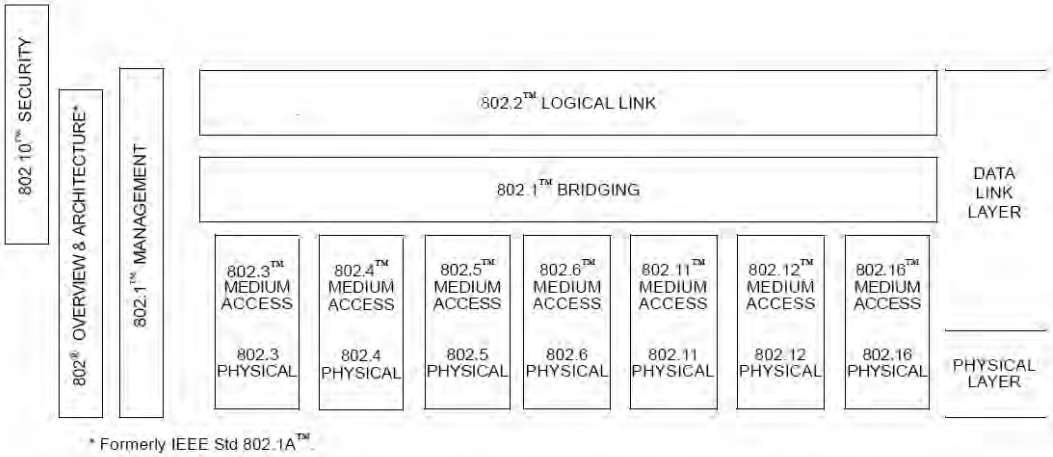


Figure 1. 802.16's Place in the IEEE 802 Standards Hierarchy. (From [2]).

While IEEE 802.16 has only one Medium Access Control Layer specification, it has undergone a series of revisions. These revisions added several different PHY layer specifications as new spectrum allocations, both licensed and unlicensed, became available. In order to prevent confusion, a brief synopsis of the various extensions and frequency ranges of the standard are presented below. The MAC will be discussed in greater detail later in this chapter.

### 1. IEEE 802.16-2001

The original IEEE 802.16-2001 [2] specification defined a set of MAC and PHY layer standards intended to provide fixed, broadband wireless access in a point-to-point or point-to-multipoint (PMP) setting. With single carrier modulation in the 10 – 66 GHz range, 802.l6-2001 provided support for both Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD). Assembled into well organized sublayers, IEEE 802.16-2001 defined the basic MAC that is employed over all of the followon variations of the standard. Where IEEE 802.11 relies on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to determine when nodes in the network are allowed to transmit, the IEEE 802.16-2001 MAC uses an entirely different paradigm to control transmissions. Transmission times, durations and modulations are assigned by a Base Station (BS) and shared with all nodes in the network in the form of broadcast Uplink and Downlink Maps. By scheduling transmission times, the vexing "hidden node" problem is avoided. Subscribers need only hear the base station, rather than every other node in the local wireless network. Also, the scheduling algorithm is stable when subjected to overload or oversubscription conditions.

Subscriber Stations (SS) are able to negotiate for bandwidth allocation on a burst-to-burst basis, providing scheduling flexibility. The available modulation schemes include QPSK, QAM-16 and QAM-64. These can vary from frame to frame and from SS to SS, depending on the robustness of the connection. The ability to change modulation and forward error correction schemes to the current propagation conditions allows the network to quickly adapt to weather conditions, such as rain fades. Initial transmission parameters are negotiated through an interactive process called Initial Ranging. This process, in which the BS provides power, modulation and timing feedback to the SS is also conducted on an ongoing basis.

Duplexing of uplink and downlink channels is accomplished using either time division duplexing (TDD) or frequency division duplexing (FDD).

Importantly, IEEE 802.16-2001 incorporates features that provide differential Quality of Service (QoS) down to the PHY layer. QoS support is built around the concept of service flows that are identified, appropriately enough, by a Service Flow ID. Service flows are characterized by their QoS Parameters, which can be used to specify parameters such as maximum latency and tolerated jitter. Service flows are unidirectional, and may originate at either BS or SS. Higher layer mechanisms, such as Diff-Serv, must be employed in conjunction with IEEE 802.16's service flows to ensure end-to-end QoS.

The IEEE 802.16 working group recommendations included several security features which, at this point in the standard's development cycle, were largely optional. At the core of IEEE 802.16 security is the privacy sublayer. The stated goal of the privacy sublayer is to provide confidentiality across the wireless links of the network. This is accomplished by encrypting the data sent between the BS and SS. To prevent theft of service, SS may be authenticated using X.509 digital certificates which are hardwired into every SS. Included in the certificate is the SS's public key and MAC address. Details of the privacy sublayer will be discussed later in this chapter.

### 2. IEEE 802.16a-2003

IEEE 802.16a was a major revision to the basic standard, ratified by the IEEE Standards Board in January 2003 [7]. Most importantly, the IEEE 802.16a extension added support in the 2 – 11 GHz Licensed bands, which opens up many potential markets for the technology. Non Line of Sight (NLOS) operation becomes possible when operating in the 2 – 11 GHz range, extending the geographic reach of the network. Multipath propagation can also become an issue. IEEE 802.16a includes both PHY specification and enhancements to the MAC layer to deal with multipath propagation and interference mitigation. Features were added to allow advanced power management techniques and adaptive antenna arrays. Also, the option of employing Orthogonal Frequency Division Multiplexing (OFDM) was added as an alternative to single carrier modulation. To provide a mechanism for interference mitigation when multiple networks

are present, IEEE 802.16a added Orthogonal Frequency Division Multiple Access (OFDMA) modulation to the range of choices available in the 2 – 11 GHz range.

Security is improved, with many of the privacy layer features now required elements, rather than optional. Privacy features are used to authenticate the sender of certain MAC messages.

IEEE 802.16a also adds optional support for Mesh networks, where traffic can be routed from subscriber station to subscriber station. This is a change from the PMP mode, where traffic is only allowed between BS and SS. Appropriate additions to the MAC layer specification were made to allow for scheduling the transmissions of SS that are part of the Mesh, but not visible to the BS.

The naming convention employed in the standard is shown in Table 1. While some might think the WirelessHUMAN designation refers to a Personal Area Network, it is simply a transmission frequency specification for High-speed Unlicensed Metropolitan Area Networks.

### 3. IEEE 802.16c-2002

In December 2002, the IEEE Standards Board approved amendment IEEE 802.16c [8]. The amendment corrected some errors and inconsistencies in the basic standard and added detailed system profiles for 10 – 66 GHz.

| Designation | Applicability | Duplexing | Notes |
|---|---|---|---|
| WirelessMAN-SC | 10-66 GHz | TDD, FDD | Single Carrier |
| WirelessMAN-SCa | 2-11 GHz Licensed Bands | TDD, FDD | Single Carrier, extended to NLOS frequencies |
| WirelessMAN-ODFM | 2-11 GHz Licensed Bands | TDD, FDD | OFDM for NLOS operation |
| WirelessMAN-ODFMA | 2-11 GHz Licensed Bands | TDD, FDD | ODFM broken into subgroups to provide multiple access in a single frequency band |
| WirelessHUMAN | 2-11 GHz License Exempt Bands | TDD | May be SC, ODFM or ODFMA. Must include Dynamic Frequency Selection |

Table 1. Air Interface Nomenclature and Description. (After [7]).

### 4. IEEE 802.16-2004

IEEE 802.16-2001, 802.16a and 802.16c were integrated into IEEE 802.16-2004 which was ratified on 24 June 2004 and was published in September 2004. The revision was originally developed as a set of system specifications titled IEEE 802.16-REVd, but was comprehensive enough to classify as a complete reissue of the basic IEEE 802.16 standard. The document is over 900 pages in length and brings the family of standards into a single document. This is the version of the standard which will be used for WiMAX certification.

### 5. IEEE 802.16e and Beyond

The IEEE 802.16 Working Group is quite energetic, with committees actively working on extensions to add mobility, conformance standards and test methodologies. The IEEE 802.16e extension, which adds support for mobile subscriber stations, is expected to be ratified during 2005. IEEE 802.16e has undergone several draft revisions. Also in the works are the IEEE 802.16f and g amendments dealing with the Network Management Plane.

## B. PROTOCOL LAYERS WITHIN IEEE 802.16

The IEEE 802.16 standard is constructed in the form of a protocol stack with well defined interfaces. As shown in Figure 2, the MAC consists of three sublayers: the Service Specific Convergence Sublayer, the MAC Common Part Sublayer and the Privacy Sublayer. When the IEEE standard refers to the MAC, it is generally discussing the MAC Common Part Sublayer, rather than the integrated stack of sublayers.

The Service Specific Convergence Sublayer (CS) maps higher level data services to MAC layer service flows and connections. The CS is provided in two variations to allow integration with both ATM and packet based networks. The packet CS supports Ethernet, point-to-point protocol (PPP) and both IPv4 and IPv6 internet protocols.

The MAC Common Part Sublayer (MAC CPS) is the nucleus of the standard. In the MAC CPS are found the rules and mechanisms for system access, bandwidth allocation and connection management. Unlike IEEE 802.11, IEEE 802.16 uses a stateful MAC layer. As discussed in later chapters, this has important security ramifications. Denial of

Service attacks at this layer can now be seen as attempts to interrupt the operation of a state machine. The MAC CPS communicates with the Convergence Sublayer via the MAC Service Access Point (MAC SAP). Communication takes place using only four basic types of primitive, which allow for the creation, modification, and deletion of

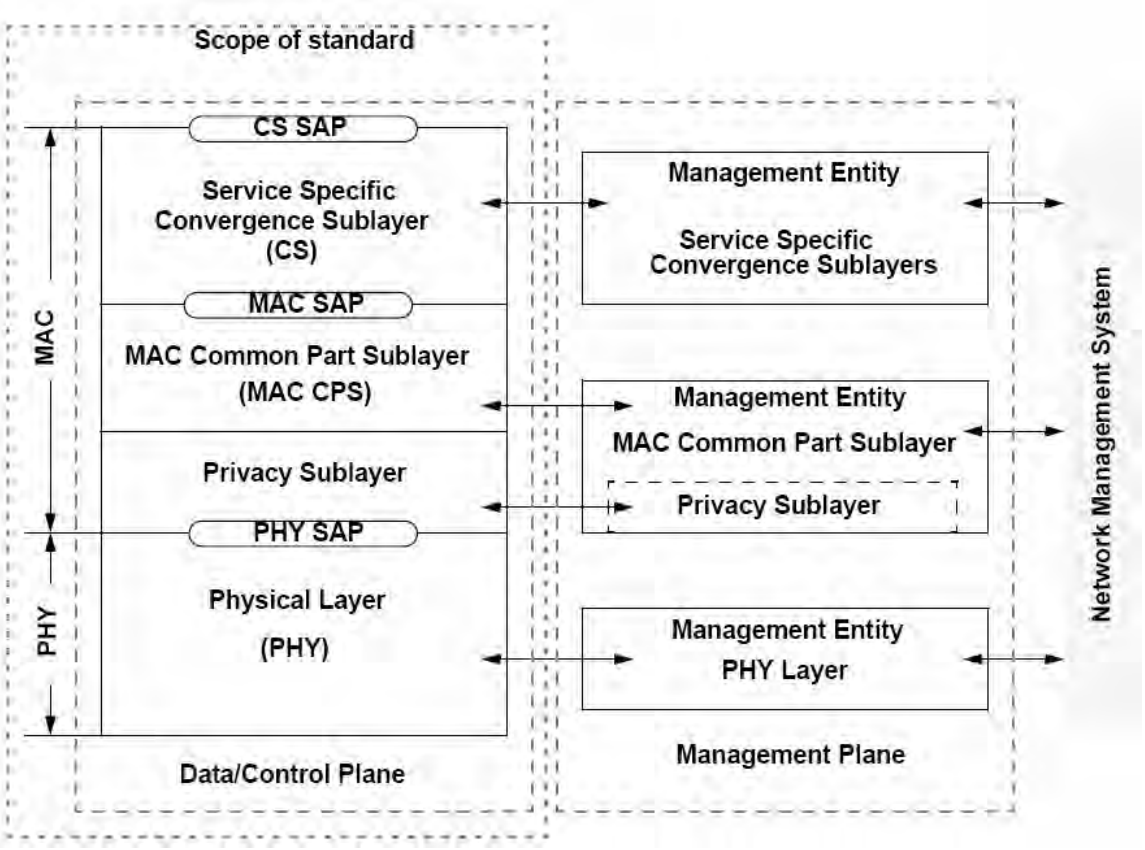


Figure 2. Protocol Layering in IEEE 802.16. (From [2]).

connections and the transport of data over the connection. QoS decisions for transmission scheduling are also performed within the MAC CPS.

The Privacy Sublayer lies between the MAC CPS and the PHY layer. This sublayer provides for encryption and decryption of data traveling to and from the PHY layer, and is also used for authentication and secure key exchange. The Privacy Sublayer currently employs 56-bit Data Encryption Standard (DES) encryption for traffic and 3-DES encryption for key exchanges. However, explicit in the privacy layer specification is the ability to support other cryptographic suites in the future.

Operating in similar fashion to the MAC SAP is the PHY SAP, which passes data to and from the PHY. Again there are a limited number of primitives, with only three basic types used.

In keeping with the broad range of frequencies supported, the PHY layer contains several forms of modulation and multiplexing, as previously discussed. The tremendous flexibility of the PHY provides engineers the ability to tailor their systems to the real world requirements of cost, capacity and spectrum availability. The PHY also allows designers to choose among various forward error correction (FEC) schemes, including Reed-Solomon and Block Turbo Codes.

Of note, the modular nature of the standard as a whole allows entirely new PHY specifications to be added in the future. New modulation schemes or frequency ranges could be added with only minimal change to the rest of the standard. For example, frequency hopping or direct sequence spread spectrum modulation can be added, just as the IEEE added ODFM support with the 802.16a extension.

## C. THE MEDIUM ACCESS CONTROL COMMON PART SUBLAYER

In keeping with usage within the IEEE 802.16 standard [2], from this point forward the MAC CPS will be referred to as simply "the MAC."

### 1. MAC Layer Overview

The Medium Access Control Common Part Sublayer (from here forward referred to as the MAC Layer) is the core of the IEEE 802.16 standard. Built to support a point-to-multipoint topology, its purpose is to provide for efficient sharing of the physical medium. The Base Station is the central node of the wireless network and acts as the bridge to the wired network. It is analogous to the Access Points (APs) seen in IEEE 802.11 networks. However, the two standards use entirely different methods to share the airwaves. Where IEEE 802.11 uses carrier sense multiple access to avoid transmission collisions, IEEE 802.16 uses scheduled transmissions to ensure collision-free access. The Base Station performs all scheduling functions and uses Time Division Multiplexing on

the downlink to SS. In turn, subscribers share the uplink using Time Division Multiple Access (TDMA). Uplink and downlink schedules are transmitted every frame using UL-MAP and DL-MAP messages.

Since the standard is designed to build outdoor networks with nodes miles apart, it must be able to adapt its transmissions to compensate for difficult atmospheric conditions. In fact, the MAC Layer allows for dynamically variable modulation and forward error correction (FEC) codes. Thus, on a frame to frame basis the BS and SS are able to optimize their transmission burst profile, trading off bandwidth with robustness. The BS always begins its transmissions with the most robust modulation and FEC scheme available to ensure that all SS are able to receive the uplink and downlink maps. On a schedule published in the DL-MAP, the BS then transitions to progressively higher capacity bursts. Similarly, each SS will transmit its uplink using the exact time and burst profile scheduled by the BS.

To accommodate traffic bursts, SS are able to ask for longer uplink windows which allow them to pass more traffic. Exchanging Dynamic Service Change Requests and Grants, the BS and SS are able to negotiate bandwidth allocations according to their respective needs and capabilities. There are several mechanisms that can be used to tailor the service level received by an SS, including unsolicited bandwidth grants and polled opportunities.

Like TCP, the IEEE 802.16 MAC Layer is designed around establishing and maintaining a series of logical connections. Just as a single computer can have different TCP connections open for Web Browsing, Telnet and mail services, a single SS may have different connections open for radio link control, network management and user data transport. Unlike TCP connections however, each of these MAC Layer connections can have radically different parameters for security, bandwidth and priority.

Known by unique Connection Identifiers (CIDs), connections are assigned and managed by the BS. During the initial network entry, an SS is assigned three CIDs representing Basic, Primary Management and Secondary Management connections. The Basic connection is used to send brief, delay-intolerant messages for control of the radio link. The Primary Management connection is used to transport longer, less urgent

messages such as registration requests and privacy key management messages. There are also Broadcast CIDs that address every SS in the local radio network. These are used to transmit the uplink and downlink transmission schedules, for example. Once the SS is fully registered with the network, it is assigned unidirectional service flows which carry user traffic. Note that a singe CID can carry traffic for many different higher-layer sessions.

The IEEE 802.16 MAC Layer is stateful. In fact, the MAC layer can be viewed as a series of state machines, each determining the operation of individual processes within the MAC structure. There are state machines for initial network entry, authentication and key management, among others. This becomes an important concept when examining the inner workings of the various operational mechanisms of the MAC Layer.

### 2. Frame Format

IEEE 802.16 supports two types of transmission duplexing: Time Division Duplexing and Frequency Division Duplexing. An illustrative example of a TDD Frame is shown in Figure 3. In the TDD case, the BS transmits the entire downlink, starting with the DL-MAP and UL-MAP messages which describe the timing and contents of the downlink and uplink respectively. In the downlink direction, the schedule informs SS when the BS is planning on shifting transmission burst schemes during the downlink. In the uplink direction, the schedule informs each individual SS when it will be allowed exclusive use of the transmission spectrum.

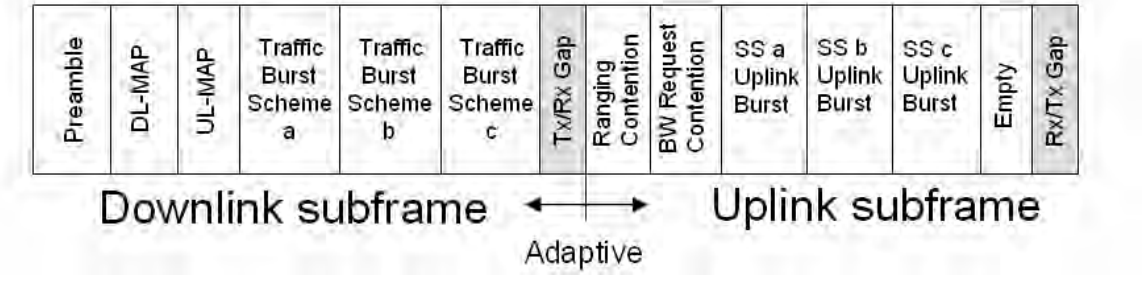


Figure 3. Example of a TDD frame. (Synthesized from [2] and [7]).

In the FDD case, transmissions are also scheduled using DL-MAP and UL-MAP messages. However, uplink and downlink transmissions occur simultaneously on different frequencies.

### 3. Format of MAC Messages

Since the format and contents of MAC Management messages is central to this thesis, these will be discussed in some detail. Messages exchanged between the BS MAC and the SS MAC are referred to as Protocol Data Units (PDUs), and are sent in the form shown in Figure 4. There are two types of MAC header that are used. The first is the Generic MAC header, which is used for the transfer of nearly all of the standard MAC Management messages. The other format header is the Bandwidth Request Header, which is used in standalone fashion without a payload. The cyclic redundancy check is entirely optional for MAC management messages and is only used if specifically required by the QoS parameters of the SS.

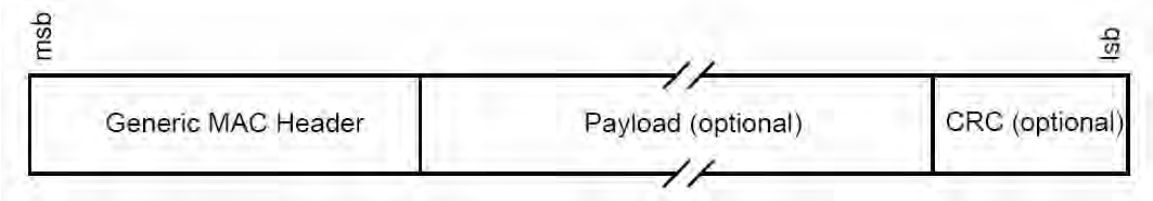


Figure 4. The Format of MAC Management Protocol Data Units. (From [2])

The format of the generic MAC header is shown in Figure 5. The Header Type (HT bit) is always set to zero for generic headers, and is set to one for the bandwidth request header. The other fields are as shown in Table 2. Of particular note are the Type and EKS fields. The Type field shows which management message is stored in the payload. The EKS field is used to ensure that the BS and SS are synchronized in their use of Traffic Encryption Keys and Initialization Vectors. For a complete listing of the MAC management messages and their Type codes, see the Appendix.

According to section 7.1.1 of the IEEE 802.16-2001 standard, MAC Management messages are not to be encrypted. This decision was made to "facilitate registration, ranging and normal operation of the MAC sublayer" [2]. This is a key statement, as it makes the generation of false management messages possible. If all the MAC management messages were encrypted, once the BS and SS had exchanged traffic

encryption keys, these messages would be exceedingly difficult to spoof. Also of note is that regardless of encryption settings, the MAC header is never encrypted.

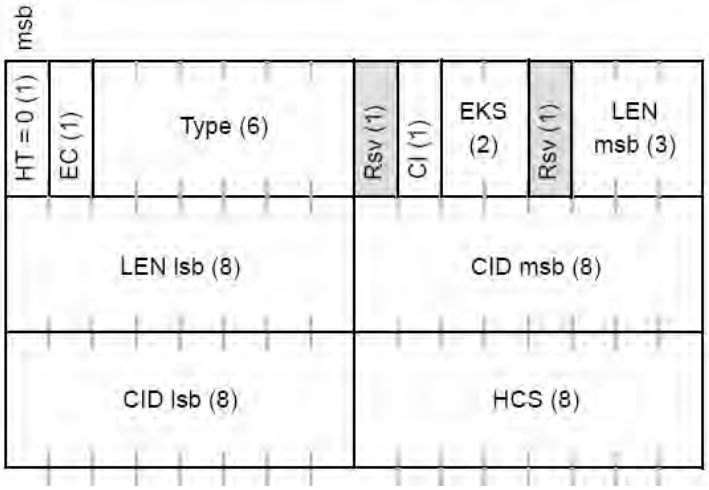


Figure 5. Generic MAC Header Format. (From [3]).

| Name | Length (bits) | Description |
|---|---|---|
| CI | 1 | CRC Indicator<br>1 = CRC is appended to the PDU<br>0 = No CRC is appended |
| CID | 16 | Connection Identifier |
| EC | 1 | Encryption Control<br>0 = Payload is not encrypted<br>1 = Payload is encrypted |
| EKS | 2 | Encryption Key Sequence<br>The index of the Traffic Encryption Key and Initialization Vector used to encrypt the payload. This field is only meaningful if the Encryption Control field is set to 1. |
| HCS | 8 | Header Check Sequence<br>An 8-bit field used to detect errors in the header. The generator polynomial is $g(D)=D^8+D^2-D-1$ |
| HT | 1 | Header Type. Shall be set to zero. |
| LEN | 11 | Length<br>The length in bytes of the MAC PDU including the MAC header. |
| Type | 6 | This field indicates the payload type, including presence of subheaders. |

Table 2. Generic MAC Header Fields. (From [3]).

## 4. Ranging, Authentication and Establishing IP Connectivity

As seen in Figure 6 from [2], subscriber stations go through a multi-step process to join a network. Once an SS has detected an active channel, it announces its presence

to the BS via a Range Request (RNG-REQ) message. Determining the range between the BS and SS is important because SS uplinks are timed so that their transmissions arrive in a precisely scheduled window to minimize dead air time spent waiting on an individual SS's propagation delay. In a network with hundreds of SS, as might be seen in a residential wireless DSL-type deployment, the cumulative effect of these propagation delays would have a negative impact on network efficiency.

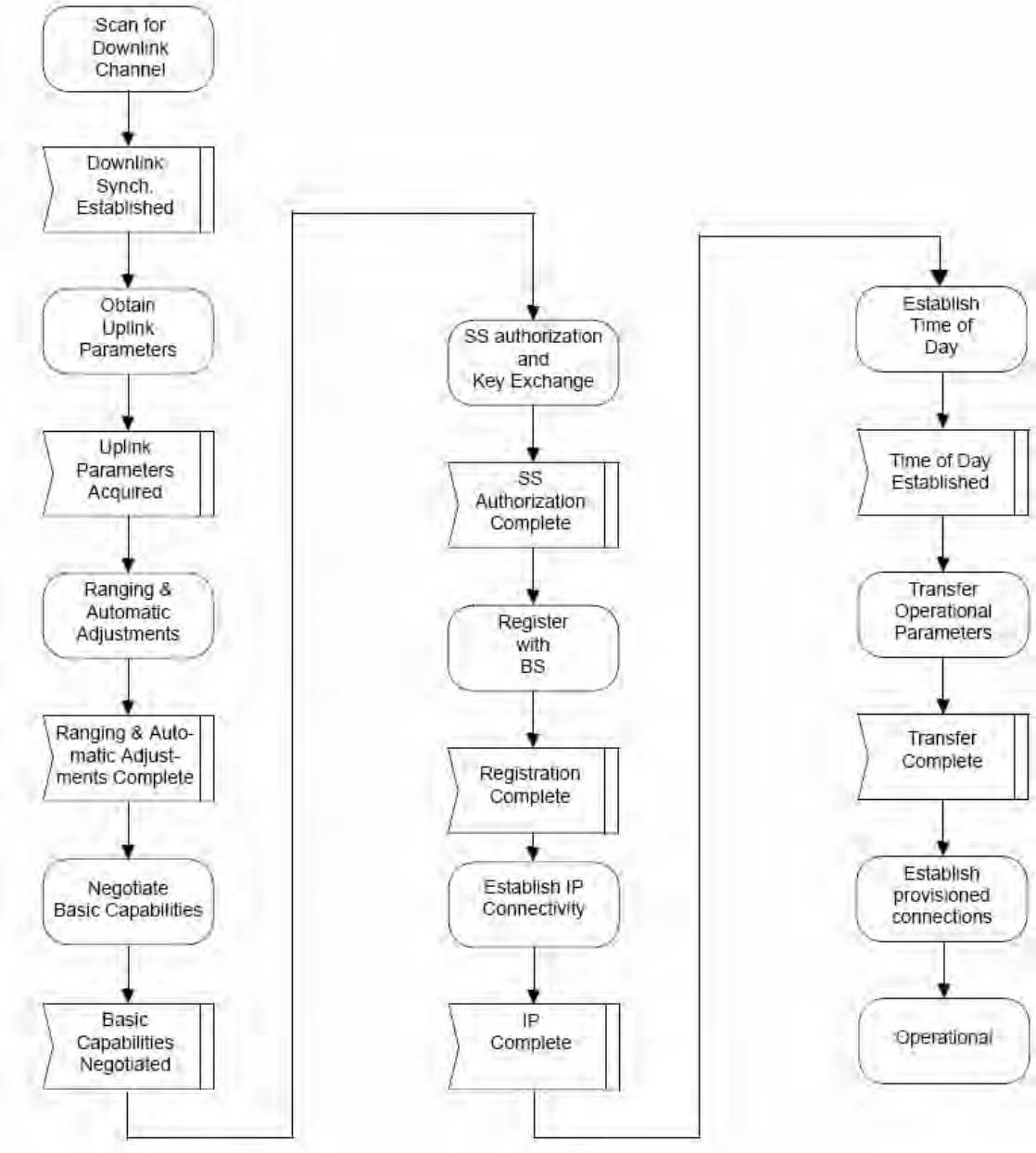


Figure 6. SS Initialization Overview. (From [2]).

Transmitted during an Initial Maintenance time slot, the RNG-REQ also allows the SS to inform the BS of its preferred downlink burst profile. The BS, in turn, uses the Range Response (RNG-RSP) to adjust the SS transmission frequency, time and power. The BS also uses this message to inform the SS of its Basic and Primary Management CIDs. The SS and BS continue to exchange RNG-REQ and RNG-RSP messages using the newly assigned Basic CID, until the link has been fine tuned, and performance is acceptable to both parties. Once an acceptable radio link has been established, the SS informs the BS of the physical parameters and bandwidth allocation schemes it can support.

The next step in the SS initialization process is requesting authorization to enter the network. Since theft of service is a large concern for commercial deployments, the IEEE 802.16 standard requires strong authentication of the SS. The procedures for authentication and key exchange are discussed in the Privacy Sublayer section that follows in this chapter.

Upon completion of the authentication process, the SS is provisioned with a full set of authentication and traffic encryption keys. The SS is then assigned its Secondary Management CID, so that it may receive standards-based management messages for things such as such as Dynamic Host Configuration Protocol (DHCP).

The remainder of the SS initialization process consists of establishing IP connectivity and network time of day, followed by transferring operational parameters and establishing transport connections. These are accomplished using well known standards such as DHCP, Trivial File Transfer Protocol (TFTP) and User Datagram Protocol (UDP).

## D. PRIVACY SUBLAYER

The stated purpose of the Privacy Sublayer is to prevent eavesdropping on user data as it traverses the wireless link. With the exception of MAC management messages, all data traffic between the BS and SS is encrypted. However, the main focus of the Privacy Sublayer is on protecting service providers against theft of service, rather than protecting network users. Encrypting user data is simply a very desirable means to the

end of preventing theft of service. It is also important to note that the privacy layer only protects data at the Open System Interconnection (OSI) layer two level. It does not provide end-to-end encryption of user data as seen in Virtual Private Networks and layer seven solutions such as S/MIME and SSH. Nor does it provide protection of the physical signal as a low probability of intercept scheme would. Both physical and higher layer security technologies would need to be integrated to provide a highly secure, routable communications network.

To manage the exchange and synchronization of encryption keys, IEEE 802.16's Privacy Sublayer employs the Privacy Key Management (PKM) protocol from the DOCSIS BPI + specification that is commonly used for cable modems.

The protocol employs several different keys when setting up privacy encryption. These are summarized in Table 3. During the initial startup and ranging procedure, the SS submits its X.509 Digital Certificate to the BS. The BS verifies the authenticity of the certificate. If the SS is authorized to join the network, the BS uses the SS's Public Key to encrypt an Authorization Key (AK). The AK is used in several different ways. It is used to derive a Key Encryption Key (KEK). It is also used to derive Hashed Message Authentication Code (HMAC) keys that are used in the generation and verification of MAC management messages. Finally, the KEK is used to protect a Traffic Encryption Key (TEK) that is generated by the BS, and sent to the SS. The TEK is the key actually used to encrypt data traffic exchanged between the BS and SS.

The standard ensures that an SS is always in possession of valid encryption keys. For both authentication and traffic encryption keys, SS are given two sets of keys with staggered lifetimes. The key changeover schemes used for AKs and TEKs are very similar and ensure an orderly transition between key material generations.

| Key | Generated by | Used for | Lifetime | Algorithm |
|---|---|---|---|---|
| Public/Private Key Pair | Manufacturer | - SS authentication<br>- exchanging AK | Permanent | RSA |
| Authentication Key (AK) | BS | - generating KEKs<br>- Calculating HMAC digests<br>- Verifying received HMAC digests | 1 day to 70 days | 3-DES, SHA-1 |
| Key Encryption Key (KEK) | BS, SS | - encrypting TEK for transmission (BS)<br>-decrypting TEK for use (SS) | Same as AK | 3-DES |
| Traffic Encryption Key (TEK) | BS | - encrypting data traffic | 30 minutes to 7 days | DES |

Table 3. Summary of Cryptographic Keys Associated with the Privacy Sublayer.

## E. PHYSICAL LAYER

While an in-depth discussion of the OSI model physical layer of the IEEE 802.16 standard is beyond the scope of this thesis, there are a few points that should be covered with regards to the physical layer.

First of all, to a great extent the methods employed in a DoS attack will depend on the frequency and modulation scheme employed by the target network. For example, an attacker's ability to sniff traffic sent across a 50 GHz line-of-sight link will be much more dependent on the geographic arrangement of attacker and victim than would be the case in a 2.4 GHz area broadcast.

Secondly, while the IEEE 802.16 standard was originally written to support a handful of physical medium interfaces, it would not be unreasonable to expect that the standard will continue to evolve and may be extended to support other PHY specifications. The modular nature of the standard is very helpful in this regard. For example, the very first version of the standard only supported single carrier modulation. Since that time, Orthogonal Frequency Division Multiplexing (OFDM) has been added. The standard has also been extended for use in new frequency bands. Beyond the world of international standards, it would likewise be possible for developers to adapt the IEEE

802.16 MAC layer to work with proprietary PHY mechanisms. For example, the standard would make an excellent basis for military spread spectrum communications systems.

## F. EXAMPLE NETWORKS

For the purposes of illustration, this section will briefly describe real-world deployments of pre-802.16 networks. These are provided to give the reader a sense of the types of IEEE 802.16 deployments that may be seen in the future. Given the very flexible nature of the standard, there are bound to be many different types of deployments, from suburban DSL replacement networks to cellular backhaul point-to-point links.

### 1. Houston County Study

Houston (pronounced "house-ton") County Georgia recently commissioned a wireless broadband study, conducted by Siemens [9]. The purpose of the study was to assess the feasibility of county-wide universal broadband access. The study examined the economic and technical issues that would need to be addressed to accomplish this goal, and also included some real-world testing using equipment from Alvarion, Inc. While the equipment was "pre-802.16," it still adhered fairly closely to the published standard. The test network used Alvarion BreezeACCESS VL equipment, operating in an unlicensed frequency band at 5.8 GHz. The BS used a single 120 degree sector antenna, and SS used flat array antennas approximately 12" square.

Despite the rural nature of Houston County, the study demonstrated the operation of a text-book Metropolitan Area Network. As shown in Figure 7, the test network had a single Base Station serving five Subscriber Stations which were located from 3 to 12 miles away. The SS were nominally serving wireless broadband to County office buildings, including the Courthouse and Police Training Center. The IEEE 802.16 links were simulating service to wired local area networks in a manner analogous to T1 class landlines. Despite challenging propagation conditions due to trees and elevation changes, the most distant SS was able to achieve end-to-end traffic rates of 4.6 MBits/sec in the

downlink and 2.9 MBits/sec in the uplink. These speeds were measured by a commercial website that measures file transfer times. This test network was created to demonstrate the viability of a county-wide network with approximately 100 commercial subscriber stations.

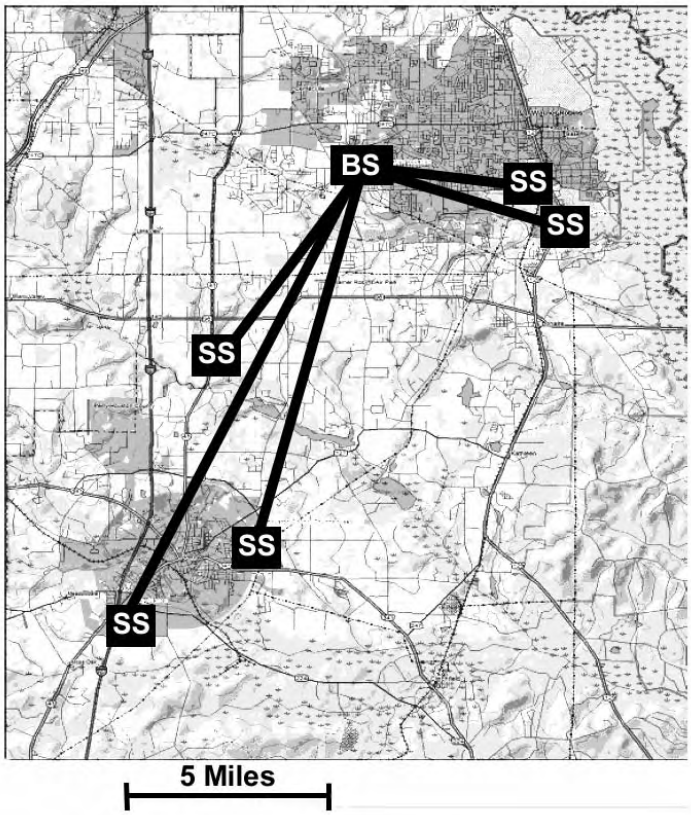


Figure 7. Houston County Test Network. (After [9]).

### 2. Verizon Avenue's Suburban DSL Replacement Networks

Another type of IEEE 802.16-based network that may become common are those that provide DSL and cable modem class service to underserved suburban or rural areas. In several test markets, Verizon Avenue (a subsidiary of the cellular phone giant) has installed networks that serve hundreds of households. These generally have one or two antenna towers with several 120 degree sector antennas, and serve residences within just a few miles of the tower. Each home is provided with a small directional antenna and an Ethernet interface box. In these test markets, customers receive 768 kbps (downlink)

service for approximately $30 per month [10]. This will probably be the first IEEE 802.16 network that the public becomes familiar with.

# III. EXAMINATION THE IEEE 802.16 STANDARD FOR KNOWN IEEE 802.11 DENIAL OF SERVICE VULNERABILITIES

There has been a great deal of interest in exploiting IEEE 802.11 wireless LANs. Unfortunately, there has also been a great deal of success. Hackers, security consultants, government agencies and even college students have all identified and tested vulnerabilities inherent in the IEEE 802.11 standard. These vulnerabilities have included cryptographic weaknesses, network exploitations and denial of service attack vulnerabilities. In this chapter, DoS vulnerabilities in the IEEE 802.11 MAC layer are presented, with accompanying analysis of the IEEE 802.16 MAC for similar vulnerabilities. Information on the IEEE 802.11 standard is drawn from the standard itself [11] as well as from published reports on vulnerabilities.

## A. INTRODUCTION TO IEEE 802.11 VULNERABILITES

In their 2003 presentation to the 11th USENIX Security Symposium, John Bellardo and Stefan Savage asserted that the IEEE 802.11 MAC layer is vulnerable to two broad classes of DoS attacks [12]. Bellardo and Savage proposed that the vulnerabilities in IEEE 802.11 were either "identity vulnerabilities" or "media-access control vulnerabilities." These two categories quite neatly encapsulate the attacks presented in [12], as well as the attacks presented in other published research [13], [14], [15]. This thesis will also use these categories to describe vulnerabilities found within IEEE 802.16. Not considered in [12] are attacks at the PHY layer, such as military broadband jamming of the RF spectrum. While resistance to RF jamming is vitally important to military networks, attacks at the PHY layer are considered outside the scope of this thesis.

### 1. Identity Vulnerabilities

Identity vulnerabilities occur when control and information messages are not properly authenticated. According to Bellardo and Savage, IEEE 802.11 is particularly vulnerable to these types of attack because the standard implicitly trusts message source addresses [12]. The standard lacks a robust sender authentication mechanism at the MAC

level. For a receiving station without the ability to authenticate the true source of a message, any correctly formatted message from an appropriate source address will be perceived as genuine. As a result, attackers are able to abuse a variety of powerful MAC messages [14].

### 2. Media-Access Control Vulnerabilities

While Bellardo and Savage do not explicitly define media-access vulnerabilities, they do provide two clear examples from which the definition might be inferred. The two exploits presented show how and attacker may take advantage of the mechanisms that are designed to fairly share the transmission medium. The first attack exploits IEEE 802.11's physical carrier sense mechanism by transmitting many short packets in rapid succession, causing all nodes within range to believe the medium is already in use. The victim nodes then listen patiently for their fair turn to communicate. As long as the attacker is transmitting, this turn never comes. In contrast, the virtual carrier sense attack sends relatively few packets. However, these packets use forged length fields within the packet to reserve a very long transmission period. During this period, fooled nodes don't even use their physical carrier sense mechanism to check to see if the medium really is busy. Instead, they just count the microseconds until the reserved transmission period expires.

## B. DEAUTHENTICATION ATTACK

### 1. IEEE 802.11 Background

The deauthentication attack is a near-perfect exploitation of IEEE 802.11's inherent identity vulnerability [12]. When a new node wishes to join an IEEE 802.11 network, it must first go through an authentication and association process before it is allowed access to the rest of the network. Authentication may be either "open" (any node may join the network), or shared key (node must be in possession of the network password). Once authenticated, a node goes through an association process and then is finally allowed to exchange data across the full network. There are only a limited number of control, management and data frames allowed during the authentication and association process. One of these messages allows nodes to demand deauthentication

from each other, which is useful for switching between wireless networks that overlap geographically. A node in receipt of a deauthentication message will immediately remove itself from the network and return to its base state.

In the deauthentication attack, a rogue node first determines the address of the Access Point (AP) that is controlling the wireless network [12]. Analogous to the BS in an IEEE 802.16 network, the Access Point is the bridge between the wired and wireless LANs. The address of the AP is easily determined, as it is not protected by cryptological means. The AP source address is used only to allow subscribers to determine which network to deauthenticate from; it is not a form of authentication. While some AP's are configured so that they do not directly broadcast their presence, their address may still be found by listening to the transmissions of other nodes.

Once the attacker has the AP address in hand, he uses the default broadcast address to transmit the deauthentication message to every station within reach. Believing the message to be the genuine article (and with no means to find otherwise), any station that receives the deauthentication message immediately stops communicating with the network. These newly deauthenticated nodes must now restart the authentication and association process from the very beginning. Repeated transmissions of deauthentication messages can bring network traffic to a complete standstill [12], [14]. No advanced cryptological techniques are required to mount the attack because none are employed.

There are other messages within IEEE 802.11 that may be abused to cause this complete denial of service. The disassociation message may be constructed and employed in near identical fashion to the deauthentication message [12]. Known as the disassociation attack, this tactic is slightly less efficient from an attacker's standpoint because more of the spoofed messages are required. Even though there are other messages which may be abused, for the sake of simplicity the term "deauthentication attack" will be used from this point forward when generically discussing attacks that exploit IEEE 802.11's identity vulnerability at the MAC level.

There are a few key properties of the deauthentication message that make the deauthentication attack possible. Most importantly, the deauthentication message itself is totally unauthenticated aside from a logical check of the message source address.

Second, the information needed to construct a valid message is not cryptographically protected and is in fact, quite easily determined. Also, the victim will respond to a correctly formatted deauthentication message regardless of when it is received. Hence, an attacker simply needs to generate a barrage of deauthentication messages and send them to the victim. To make matters worse, the attacker doesn't even need to be authenticated or associated with the network in order to inject these messages [13].

### 2. Application to IEEE 802.16

IEEE 802.16 contains several MAC messages that are analogous to the deauthentication message found in IEEE 802.11. The Reset Command (RES-CMD) message, is transmitted by a base station to direct a particular subscriber station to completely reset itself [2]. It is management message type 25, as shown in the Appendix. A subscriber in receipt of a valid RES-CMD will reinitialize its MAC and attempt to repeat initial system access. The message is intended to allow a BS reset unresponsive or malfunctioning SS. Similarly, a BS may transmit the De/Re-register Command (DREG-CMD) to an SS, thereby forcing the SS to change its access state. DREG-CMD is management message type 29, as shown in the Appendix. This command may be used for several purposes, including forcing an SS to completely leave the transmission channel.

Fortunately, IEEE 802.16 incorporates substantial protection against the misuse of the RES-CMD and DREG-CMD commands. The primary mechanism is message authentication in the form of Hashed Message Authentication Code (HMAC) Digests, using the SHA-1 hash algorithm. As described in Internet Engineering Task Force Request for Comments 2104, an HMAC digest is a general purpose authentication code calculated using both the original message and a shared secret key [16]. In the case of IEEE 802.16, the specified algorithm generates a 160 bit value which is appended to the original message. Together, these three elements—message, shared secret key and HMAC digest—allow the receiver to verify that the author is legitimate and that the message was received in its original form. The receiver simply uses its own copy of the secret key to calculate an HMAC digest for the message and compares this result with the digest calculated by the sender. The two sets of calculated HMAC digest values will match only if the two parties are using the same key and same message. Since only the

legitimate sender and intended recipient share the secret key, a match guarantees that the message arrived from the legitimate sender unaltered. See Figure 8 for an overview of the attack.

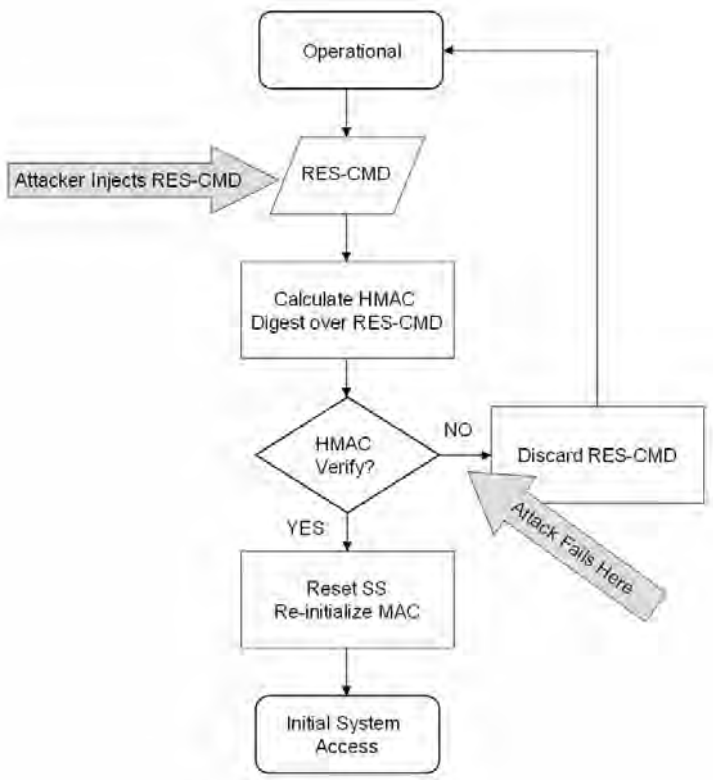


Figure 8. Failure of the Deauthentication Attack using RES-CMD.

The authentication system described above rests on a few underlying assumptions. Most importantly, the keyed hash algorithm is assumed to be cryptographically strong. In simple terms, the algorithm used must not allow an attacker to guess or otherwise calculate correct hash values without exhaustively trying every possible key. Another underlying assumption is that the key used when calculating the HMAC digest is truly secret. This is an assumption that fails when referring to IEEE 802.11. The Wired Equivalent Privacy (WEP) was famously discovered to employ a flawed encryption mechanism. Once the flaw was revealed, the privacy and authentication mechanisms in use were entirely compromised. Fortunately, IEEE 802.16 employs different encryption standards. The standard currently allows the choice of 3-DES EDE with a 128-bit key or RSA with a 1024-bit key. Even if these well proven

algorithms were compromised, the message authentication vulnerability could be repaired by changing crypto suites—this is an explicit feature of the standard.

IEEE 802.16 is protected from the deauthentication attack because it employs strong authentication of those key MAC messages, such as RES-CMD and DREG-CMD. It is important to note that not *every* MAC message is authenticated. The implications of this will be discussed in detail in a later chapter.

## C. REPLAY ATTACK

### 1. IEEE 802.11 Background

Generically speaking, a replay attack is one in which an attacker fraudulently reuses a piece of valid information that he has intercepted or overheard. The attacker does not need to modify the message, but merely repeats it at an opportune time. As applied to IEEE 802.16, an attacker might capture a message (along with its associated HMAC) and replay the message unaltered. This section will discuss the ways that IEEE 802.16 will respond to this replayed message.

As previously discussed, IEEE 802.16 employs Hashed Message Authentication Code (HMAC) digests to ensure the authenticity of received messages. While HMACs provide a receiver assurance that the message was received as sent, they are not absolute assurance that a message is being used as intended. The sender and the contents of the message are authenticated, but nothing else. A message that has been captured by an attacker then replayed later will still authenticate properly as long as the encryption keys haven't changed in the interim. Since the message contents cannot be altered in any way, the replayed message is of only limited utility. However, there remain scenarios in which unaltered, rebroadcast messages can cause significant problems for the victim. Any consumer who has been billed twice for a single purchase will have a feel for this.

When used against IEEE 802.11 networks, the replay attack can be useful as a DoS weapon. At the most basic of levels, any valid message will cause a DoS condition if it is repeated often enough. This is the brute force case. Since the message is valid, it consumes both bandwidth and computing time as the message is decoded and acted upon. IEEE 802.11 is vulnerable to this type of attack because messages aren't serialized in any

fashion. There is no built-in method to detect and discard replayed messages. Moving beyond the brute force level, a replay attack can be effective at exploiting higher level functions in an IEEE 802.11 network.

Of note for IEEE 802.16 is that the attacker might need both BS and SS capabilities to observe and replay his message, depending on the exact scenario presented. Depending on the network implementation, the attacker might even need to coordinate the operations of two separate units. For example, in a FDD system, BS and SS transmissions occur at different frequencies. A replay attack against this FDD system would require the attacker to receive information on one frequency then transmit it on that same frequency. If this is not possible with a single unit, the attacker would need to have both BS and SS operating in unison. This is a very different scenario than that seen in the Ethernet and Wi-Fi worlds where every node in the network has the same transmit and receive capability.

### 2. Application to IEEE 802.16

Since the presence of the HMAC digest requires that a message must be retransmitted unchanged, whether a particular message may be reused is dependent on the internal details of the message. Any transient information within the message, for example a timestamp or a transaction serial number, generally makes the message unsuitable for a replay attack. The transient information allows the receiver to detect the retransmission and ignore the duplicate copies of the message.

Looking once again at the Reset Command, it initially appears that the RES-CMD message could be effectively replayed by an attacker. The command itself contains no serial number, no timestamp and no transient information. See Table 4. Messages of this type seem very appropriate for replay.

| Management Message Type | Message Parameters |
|---|---|
| 25 = RES-CMD | HMAC Digest |

Table 4. Reset Command Format. (After [2]).

However, this is not the case. The IEEE 802.16 standard requires the HMAC to be calculated using the entire message, including the MAC header. See Figure 4. Since

the header is covered by the HMAC digest, it too must be retransmitted unaltered, and this is where the replay attack falls apart. The header contains the Connection ID (CID) of the SS which must be reset. For this reason, the RES-CMD command is a one time use message. Once reset, the SS will resume operation under the new CID assigned by the BS. The CID is a 16-bit value, and the BS cycles sequentially through all 65,536 choices of CID. This makes it very unlikely that the CID will be reused. Even if the SS were to resume operation using the same CID, it would negotiate a new set of keys with which to authenticate the message. A replay attack based on the RES-CMD fails on two different levels. Therefore, the RES-CMD command is useless to an attacker attempting to employ the replay attack. For similar reasons, a replayed DREG-CMD also fails to elicit action by the SS.

In the case of the RES-CMD and DREG-CMDs, the replay attack fails to cause the actions desired by the attacker. However, IEEE 802.16 remains somewhat vulnerable to interference from brute force replay denial of service attacks, because there is no mechanism in place to specifically detect and discard repeated packets. An attacker could repeat many messages (whether valid or not) in an attempt to interfere with the proper operation of the network. There are several ways in which the victim network might respond, depending on the exact content and timing of the replayed message.

In the least damaging case, the attacker's signal would act like a narrowband noise signal competing with legitimate broadcasts. While this would have a negative impact on network efficiency, dynamic FEC and modulation changes would be able to mitigate the impact of this attack.

In a more damaging attack, the attacker would repeat copies of a single SS's traffic to the BS in such a way as to cause the BS to send a RES-CMD to the SS whose traffic is being replayed. This is a worthy goal for an attacker, as the reset would cause the victim to stop all broadcasts and return to the initial registration cycle. However, whether or not this second effect will happen is open to conjecture. The standard only states that the RES-CMD may be used "if an SS is unresponsive to the BS or the BS detects continued abnormalities in the uplink transmission from the SS" [2]. The standard does not specify exactly what constitutes "continued abnormalities in the

uplink." The exact set of conditions that result in a RES-CMD will be decided by the equipment manufacturers. The effect of this type of attack will be implementation specific.

## D. AP SPOOF

### 1. IEEE 802.11 Background

In an AP spoof, an attacker "steals" users from a legitimate network by setting up a rogue access point that is configured to mimic a nearby network. This is a classic man-in-the-middle attack, where an attacker places himself between two parties and manipulates the communications between them. This is an exceptionally powerful exploit, as the attacker can gain access to information that would normally be beyond his reach. When using his position as man-in-the-middle for denial of service, the attacker simply discards the victim's traffic as it passes through his node. The position of man-in-the-middle can be very difficult to achieve in wired networks, requiring intimate access with the victim network. However, in a wireless network this position is much easier to achieve. One simply needs to set up an access point that is a more attractive choice for association than the legitimate AP. This so-called "rogue AP" can be configured to mimic the legitimate AP by copying the SSID, MAC address and even home page of the host network.

The attacker can choose to wait for new users attempting to reach the legitimate AP, or use a denial of service attack to disrupt existing connections. Since IEEE 802.11 devices select APs based on received signal strength, the attacker need only ensure that his AP has greater signal strength as seen by the victim. This may be accomplished most simply by positioning the rogue AP between the victim and the legitimate AP. Other methods include using directional antennas and RF amplifiers.

The victim is fooled into thinking he is interacting with the legitimate network while his traffic is flowing into the rogue AP. There are utilities that automate this process, complete with web servers that capture unencrypted passwords as victims attempt to log on to bogus pages. Unless there are higher level firewalls or intrusion

detection systems in place, this attack gives the attacker all the credentials he needs to access the legitimate network.

The vulnerability at the root of this attack is that IEEE 802.11 does not require strong two-way authentication between access points and users. Unless add-on security devices are used, the credentials presented by an AP are easily forged. In fact, AP credentials which typically only consist of a unique station name, are much more easily forged than the credentials that must be presented by user terminals. The AP credentials are broadcast across the network, even when the option to "advertise" the presence of the AP is disabled. This allows an attacker to "sniff" the AP's credentials by observing a relatively trivial amount of network traffic. Contrast this to the subscriber's WEP password that is used for authentication. While the Wired Equivalent Privacy key can be broken, an attacker must observe a very large volume of traffic and employ sophisticated (including some freely available) cryptographic tools. From an overall network security standpoint, employing only weakly authenticated access points is a very dangerous practice. When compared to the full range of exploits possible, using this vulnerability for a DoS attack is relatively benign.

### 2. Application to IEEE 802.16

This vulnerability also exists in IEEE 802.16. With the intent that commercial WiMAX networks would be used to provide high speed data services across a large geographic area, the IEEE 802.16 Working Group devoted a great deal of energy to preventing theft of service. As discussed in Chapter 2, every SS is required by the standard to incorporate an X.509 digital certificate to allow strong authentication of SS. *However, there is no such requirement for BSs*. In fact, the IEEE 802.16 makes no mention of BS authentication. Analogous to the IEEE 802.11 AP Spoof, this type of hijack could be called a BS Spoof.

It is worth noting that this is a hijack only at the PHY and MAC layers. Higher layer data streams (TCP connections, for example) would not be preserved and would need to be exploited by other means. There are applications designed for hijacking Internet browser sessions (most notably HostAP) that could be adapted for the purpose of spoofing real websites present on an IEEE 8021.6 network. In this case, user data could

be protected by application level encryption. Even though this is not a complete hijack, it can still be used as a potent DoS weapon. During a BS Spoof DoS attack, the radio links would show a good connection while the higher layer data went nowhere.

For example, a review of the user documentation for two "pre-802.16" compliant systems reveals that manufacturers are providing BS authentication in much the same way as IEEE 802.11. It must be noted that both of these systems were developed prior to the IEEE 802.16-2004 standard being ratified and therefore do not benefit from the full range of privacy and authentication services afforded by the standard. The Alvarion BreezeACCESS VL 5.8 GHz uses an Extended Service Set ID (ESSID) and MAC address as the mechanism for BS authentication [17]. Base Stations are provided with both default and global ESSIDs, which are designed to assist in registering with new BS within the overall wireless network. MAC address filtering is an additional feature that is optionally enabled. These mechanisms are virtually identical to those employed by IEEE 802.11. The RedLine AN-50 Point-to-Point System uses a different authentication method, employing only password-based encryption of the wireless link [18].

## E. MAC ADDRESS SPOOFING

The IEEE 802.16 standard requires that every SS have a 48-bit universal MAC address burned into its firmware [2]. This value is used as part of the initial ranging process and during the authentication process, allowing the BS and SS to verify each other's identity. There are several issues with using a device's hardware MAC address as a form of authentication. The drafters of the standard seem to be operating under the assumption that the MAC address of a SS or BS is immutable. This is not entirely the case. While the value that is encoded in the hardware cannot be changed, the value that is reported by the firmware is subject to change. There are numerous programs capable of changing the MAC address reported by network adapters within personal computers. These programs use features of the computer's operating system (whether Windows or Linux) to modify the MAC address that is reported by the network adapter. Changing the MAC of a PC's network adaptor is a trivial process that can be accomplished in just minutes.

In the IEEE 802.11 realm, for a period, it was thought that MAC address filtering at the access point could prevent unauthorized users from joining the wireless network. Even though MAC spoofing was well known, the reasoning went that the 48-bit MAC contains too many possible values to allow brute force guessing. Unfortunately, nearly as soon as the practice of MAC address filtering became widespread, there were hacker utilities released to circumvent this protection. The problem is that hackers didn't need to guess authorized MAC addresses. The addresses were broadcast across the wireless network as required by the IEEE 802.11 standard. Therefore, the MAC addresses in use could easily be "sniffed" out of the airwaves. In IEEE 802.16, the very first message an SS sends to a BS (RNG-REQ) contains the SS's MAC address. The response from the BS (RNG-RSP) also contains this value. Therefore, an attacker capable of listening to the IEEE 802.16 link in either uplink or downlink direction will be able to determine the MAC address of authorized SS.

However, whether one can change the MAC address of an SS will depend on the architecture of the SS under scrutiny. The case of modifying the MAC address of a stand-alone unit is very different than the scenario presented by a network card resident in a PC. Currently, all available IEEE 802.16-based networking equipment is in the form of stand-alone units. This is about to change. One of the major contributors to the WiMAX Forum, Intel Corporation, has publicly announced that it plans on selling IEEE 802.16 compliant chipsets inside laptops [19]. This is analogous to the scenario with the Centrino chipset today. In this case, spoofing a MAC address will be just as trivial for IEEE 802.16 as it is today for IEEE 802.11.

For a stand-alone unit, modifying the MAC of an SS MAC will require changes at the firmware level, which is difficult unless the capability is provided by the manufacturer. As an example, there are several brands of router that have the capability to change the MAC address written directly into the user accessible configuration utility. For example, some Linksys routers have a "MAC Addr. Clone" tab in their configuration utility [20]. In the future, there will most likely be manufacturers that allow a similar capability in their IEEE 802.16 equipment. There need be only one particular SS firmware version to compromise the entire premise of MAC address authentication. As

soon as would-be attackers discover the capability, they will purchase that SS, and download the correct firmware.

In summary, MAC address filtering is helpful from a network management point of view, but is a flawed authentication method. It is for precisely this reason that, in addition to a MAC address, each SS is required to have an X.509 compliant digital certificate.

## F. ATTACKS ON PHYSICAL CARRIER SENSE

Any wireless network will be vulnerable to radio frequency jamming. However, the degree of vulnerability will vary widely, depending on the physical layer interface. Parameters such as transmitter power, receiver sensitivity, RF frequency and bandwidth and antenna directivity all play important roles when examining the effectiveness of broadband noise jamming attacks. Though this type of jamming is a PHY layer attack, there are attacks that create a denial of service condition by generating "noise" at higher layers. A SYN flood is an example of this. There are also several analogous attacks that have been demonstrated to be very effective against IEEE 802.11.

### 1. IEEE 802.11 Background

The mechanism under attack is the Carrier Sense Multiple Access (CSMA) component of the IEEE 802.11 MAC layer. CSMA is the method used to share the wireless medium and ensure that data collisions do not occur over the airwaves. Each unit that desires to transmit must first listen to ensure that no other station is transmitting. If no carrier is present (indicating no transmissions underway) the station is free to transmit. IEEE 802.11 actually uses two carrier sense methods: physical carrier sense and virtual carrier sense. Both of these have been exploited to create denial of service attacks. Since virtual carrier sense has no analogue in IEEE 802.16, only physical carrier sense will be examined here.

There are several ways to exploit the physical carrier sense protocol [12]. One just needs to make legitimate nodes in the network believe that there is another station transmitting. While this could be accomplished with specialized RF signal generators, the most rudimentary method is to have a rogue node simply transmit continuously. In

[13] this is accomplished by exploiting a management primitive that can be used to place a network card into a test mode where it continuously transmits a test pattern. Any node within range of the rogue node will correctly determine there is a transmission underway and defer its transmission. This attack requires no specialized equipment and accomplishes its jamming using only 23 mW from a commodity wireless network interface card. Contrast this with traditional jamming transmit power levels, which may need to be orders of magnitude higher to achieve a full denial of service. Also, note that the physical carrier attack will only affect the network that the attacker has synchronized with. Other networks in the area will be able to continue to operate. Again, contrast this with pure RF jamming, where every system that communicated in the same 2.4 GHz spectrum of the target would be jammed, including cordless phones.

This attack is very effective because it bypasses all of the mechanisms designed to protect the signal from outside interference. The Direct Sequence Spread Spectrum modulation, the Forward Error Correction algorithms and the Cyclic Redundancy Checks are all rendered useless by an attacker *exploiting the standard* rather than merely using brute force noise.

### 2. Application to IEEE 802.16

Since IEEE 802.16 uses a nearly contention free MAC, it does not use physical carrier sensing to control the permission to transmit. In fact, in the few contention transmission windows that exist in a frame, collision *detection* is practiced rather than collision avoidance. Any request an SS makes in a contention window that goes unacknowledged is assumed to have collided with another SS's transmission. The request is then retransmitted in another randomly chosen timeslot.

However, there are lessons that can be learned from the physical carrier sense attack. The attack works by exploiting the sharing mechanism that ensures fair and efficient use of the transmission spectrum.

All subscriber stations (even those not yet authenticated on the network) receive the UL-MAP that schedules the transmission time and modulation scheme for every SS seeking to uplink traffic. Therefore, an attacker who desires to deny service to a particular SS has all the information he needs to send malicious transmissions that will

collide with the legitimate uplink. Thus an attacker can target a single SS's transmissions for denial of service, and he can attack with minimal power because he can closely mimic the legitimate sender's RF signals.

In this scenario, an attacker would synchronize with the target network and undergo the initial ranging process in order to fine tune his transmission timing and frequency. This is necessary in order to be able to transmit signals that can truly compete "in band" with the victim SS's transmissions. If the attacker is not synchronized with the legitimate transmissions, he is competing as noise rather than as an intelligible signal and IEEE 802.16 has several mechanisms that are meant to correct for noise on the transmission channel. Once the attacker is synchronized with the target network and has received a UL-MAP, he may select a target. Since the transmissions are allocated by CID, the attacker must target a set of connections rather than an SS by name. The attacker will not know precisely which SS is being interfered with, and may in fact only be targeting a subset of the SS's several connections. The final step is to simply transmit at the scheduled time, using the scheduled modulation scheme. The messages sent could be completely forged, replayed or both. The attackers signal should then collide with the legitimate transmission. Rather than being rejected by noise filters, the rogue transmission will be competing as an intelligent signal. Depending on the relative transmission power of the two competing SS, the signal decoded by the BS will either be in a degraded state, or will be completely unintelligible. The effect over a series of transmission windows will be to starve out the affected SS. It is also possible that the BS will order the SS to reset itself due to the 'garbled' transmissions received by the BS.

The high degree of selectivity that is possible with this type of attack has some side benefits, as well. Because the attacker's transmissions are brief and indistinguishable from legitimate transmissions, it may be very difficult to pinpoint the attacker. This is a decided change from the broadband jamming scenario with its indiscriminate transmissions at relatively high power. Also, the ability to pare one SS from the network might be very useful when attempting to perform BS spoofing.

For the attacker, another benefit of this type of selective denial of service attack is that the BS will provide helpful feedback on the progress of the attack. As the victim

SS's transmissions are degraded, the BS will order the SS to shift to progressively more robust modulation and FEC schemes. An attacker that tracked the ordered modulation scheme would be able to observe the precise power level required to achieve the desired effect. This would be helpful if the attacker were trying to minimize his radiated power in order to remain undetected.

# IV. IEEE 802.16 UNIQUE DENIAL OF SERVICE VULNERABILITIES

## A. MESSAGE INJECTION ISSUES

Assuming an attacker is able to overcome PHY layer synchronization issues and break any physical layer bulk encryption that might be present in a military system, there remain two issues that must be addressed before one can mount the attacks described in this chapter. One must first be able to create and transmit the messages that will be used as the basis for the attack. Next, there is the issue of message timing, both in an intra-frame basis and in an operational state basis.

### 1. Message Generation Issues

In order to be able to inject messages into the wireless stream, one must first have the capability to generate these messages in the first place. This is not as trivial an undertaking as it might first appear. While there are several methods that have been discovered suitable for generating IEEE 802.11 messages, to date there have been no published reports on how to create arbitrary messages in IEEE 802.16. There are several reasons for this. However they all seem to return to one issue-- the standard is new. Although truly IEEE 802.16 compliant equipment is only months or years from the market place, as of this writing only pre-802.16 equipment is available. Therefore, hackers and security experts have yet to experiment with the equipment. It took years before the test and undocumented modes needed to generate arbitrary frames were discovered in IEEE 802.11 systems. Also, there has yet to emerge a significant market for diagnostic and test software. The attacks described in [14] were implemented using commercially available test equipment that was created for network testing. While it is assumed that similar equipment will emerge for diagnosing and testing IEEE 802.16 networks, as of this writing, the author is unaware of any commercial product that is suitable for generating and injecting IEEE 802.16 messages.

In [12], the author describes how IEEE 802.11 management frames can be generated using commodity hardware. Essentially, one exploits a debug port to overwrite the storage buffer of the network interface card. This allows arbitrary frames to be

inserted just prior to transmission, which ensures that the message is sent without being "corrected" by the error controls of the firmware. Figure 9 shows the "AUX Port" that was used to inject the bogus messages.

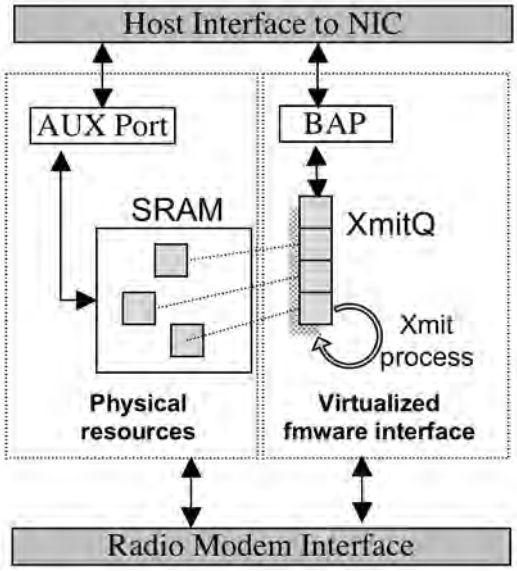


Figure 9. Block Diagram Showing How the AUX Port is used to Circumvent Firmware. (From [12]).

The IEEE 802.16 standard specifies exactly what messages may be passed though the Service Access Points (SAP) that link the layers of the protocol stack. Therefore, it should not be possible to tamper with the internals of the firmware and device memory. However, examination of the IEEE 802.11 protocol stack reveals that it was specified in much the same manner as IEEE 802.16. Comparing Figures 2 and 10 shows that, at this level of abstraction, the two standards are very similar. The two standards share this layered protocol model with other IEEE 802-based LANs, including Ethernet.

Whether it will be possible to access the internals of interface devices will be largely dependent on the types of hardware that becomes available in the future. It seems likely that developers will use similar implementation and testing methods when building new IEEE 802.16 systems. Based on past experience, it seems highly probable that eventually, a product will be released with debug-type access to the firmware. It is up to the device manufacturers to strive to avoid this type of mistake. Unfortunately, the process of translating abstract specification into practical implementation is a challenging one.

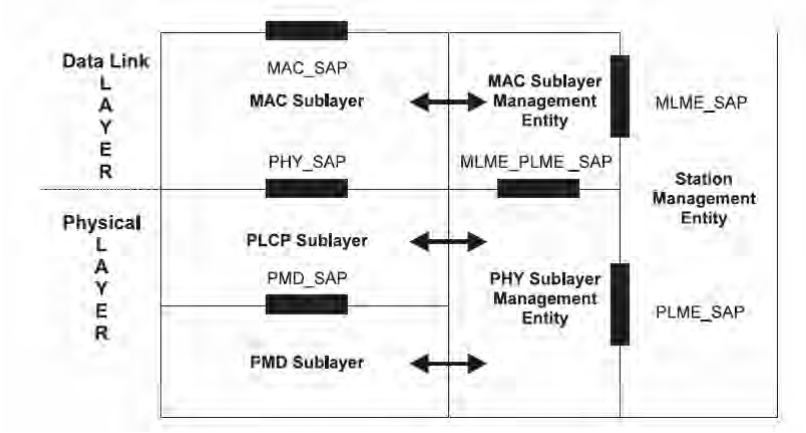


Figure 10. Protocol Layering in IEEE 802.11. (From [11]).

Currently available 802.16-like equipment are wireless routers that stand physically alone. They are accessed via an Ethernet port, which makes firmware tampering difficult. However as previously noted, this is likely to change as Intel Corporation has publicly announced its plans to have WiMAX in laptops by 2006 [19]. IEEE 802.16 network interface cards will be subjected to the same types of abuse that their Wi-Fi predecessors have endured.

### 2. Timing of Injected Messages

The question that must be answered is this: when can an attacker inject a message so that the victim will receive and obey it? It appears that successfully injecting MAC messages into the stream of traffic flowing across an IEEE 802.16 wireless network will be a difficult task. There are several obstacles that must be overcome. Aside from the fact that the standard's effective use of message authentication severely limits the types of messages that might be spoofed, the primary problem is one of timing. The attacker must find an open spot in the schedule, and then time his transmission accordingly. When transmitting from a rogue SS to the BS, the propagation delay is learned as part of the initial ranging process. However, when attempting to inject messages from a BS, the attacker doesn't know how much propagation delay will be encountered. There are also synchronization issues that must be considered. The second major hurdle is that the IEEE 802.16 MAC is stateful. The MAC only accepts certain messages at certain times, and won't act upon those presented incorrectly. In combination, these two obstacles will make attacks based on message injection difficult to realize.

IEEE 802.16 details several different transmission schedules, which correspond to different PHY layer specifications. While the PHY details vary widely, the MAC structure is fairly static across the different PHY specifications. Recall that there are two basic cases of transmission schedules: FDD and TDD.

### *a. Frequency Division Duplexing (FDD)*

In FDD systems, the uplink and downlink channels are in separate frequencies, with the downlink transmitted in discrete bursts. Since the uplink and downlink must be scheduled to support half-duplex SS, there may be times when the uplink or downlink channels are unused, allowing the attacker to inject his messages. In the uplink direction, all transmissions are scheduled. However it is important to note that the downlink maps only specify when the BS will transition between different modulation and FEC and do not detail when traffic for any particular SS will be sent.

This is both an opportunity and an obstacle for an attacker attempting to inject spoofed BS MAC messages. SSs listen to the entire downlink, scanning for messages addressed to them. Therefore, an attacker should be able to blanket broadcast his malicious message at the appropriate time and modulation. Because the attacker won't know in advance when there will be gaps in the BS transmission, his will cause collisions with other downlink traffic which may or may not be desirable. In a lightly loaded network, the attacker might be able to wait for an empty portion of the downlink frame and then transmit. Conversely, in a heavily loaded network, the downlink may be continuous from frame to frame. See Figure 11.

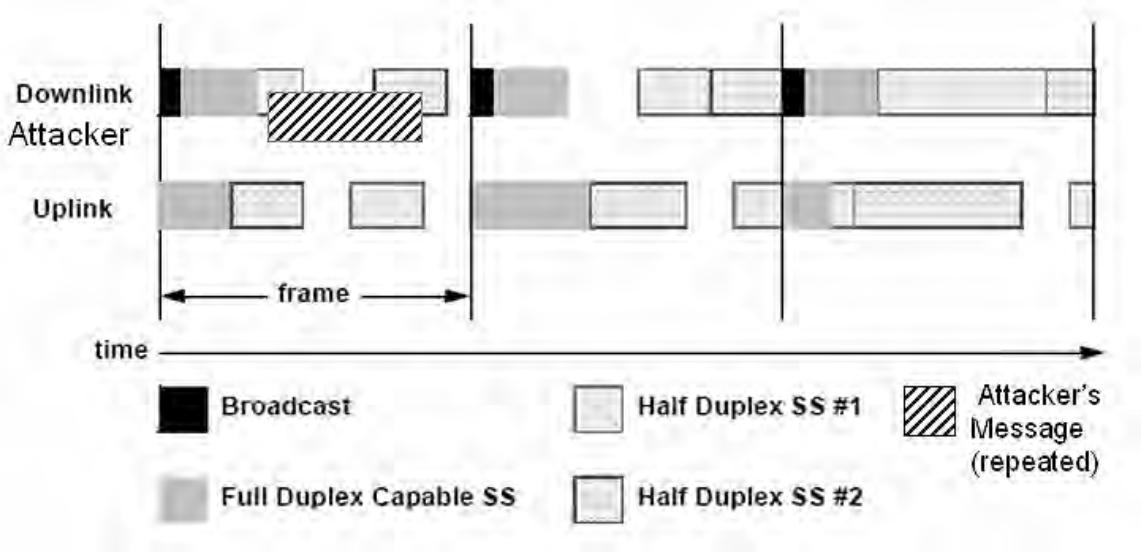


Figure 11. Message Injection Into a Gap in the FDD Bandwidth Allocation. (After [2]).

### *b. Time Division Duplexing (TDD)*

In the time division duplex case, there are no gaps in the downlink. See Figure 12. The downlink subframe is completely filled by the BS's transmissions. MAC frames may be filled with nulls to pad them out the required length, rather than allowing silent intervals within the downlink. Following the downlink there is a brief pause that ensures BS has time to switch from transmit mode to receive mode. This is the Tx/Rx Time Delay, which is followed immediately by the uplink. Following the uplink, there may be empty transmission slots if the network is lightly loaded. During these empty time slots the BS may transmit null messages at reduced power and SS are forbidden to transmit. There is another pause (the Rx/Tx Time Delay) before starting the next frame. The relative duration of the downlink and uplink subframes are adaptively determined from frame to frame. In the uplink direction, there are maintenance opportunities set aside to allow new SSs to join the network and also to allow current SSs to make bandwidth requests. With regards to timing issues alone, this is an excellent opportunity for an attacker to inject messages in the uplink direction. However, as will be discussed later, there are still issues of MAC statefulness to overcome.

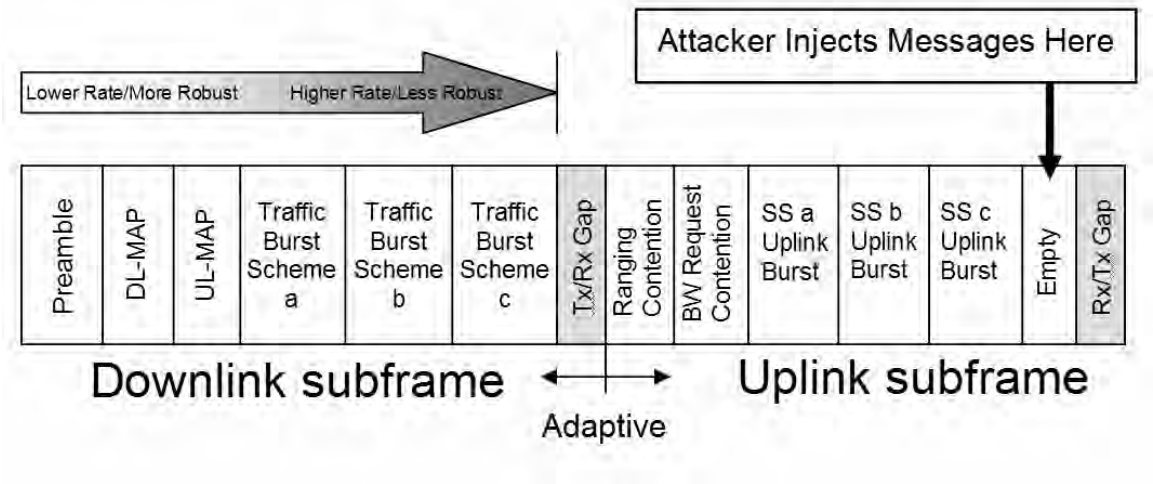


Figure 12. Injecting a Message into a TDD frame. (Synthesized From [2] and [7]).

## B. THE MAC AS STATE MACHINE

In addition to timing issues that deal with the exact microsecond of message arrival, there are timing issues concerning the exact state of the receiver's MAC when the injected message arrives. The IEEE 802.16 MAC is specified as a state machine, with defined transitions from state to state. As a simple example, see Figure 13, which shows the state transitions during dynamic service addition (DSA), deletion (DSD) and change (DSC).

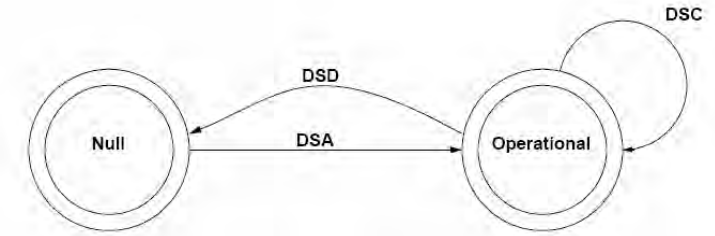


Figure 13. An Overview of the Dynamic Service Flow State Machine. (From [2]).

For an attacker wishing to inject MAC messages into an SS's downlink, this can be a significant obstacle. Aside from the timing issues previously discussed, the attacker must also be aware of the victim's state, so that an appropriate message may be sent. For example, for a machine in the Null state above, receiving a spoofed dynamic service change (DSC) message would have no effect. The message would be discarded.

Here is a less trivial example of the manner in which an injected message would be discarded. During the initial startup process, an SS sends an Authorization Request (Auth Request). The BS determines whether or not the SS is authorized to join the network, and sends the appropriate response. If the SS's credentials are valid, the BS sends an Authorization Reply (Auth Reply) message that includes an authorization key and other information that allows the authentication process to move forward. If the BS chooses to reject the SS, it sends an Authorization Reject message. An SS that receives an Auth Reject message at this point will enter a wait state and try again to authenticate later. At first blush, the Auth Reject message would appear to be well suited to form the basis of a DoS attack. One could imagine the "Auth Reject attack," where an attacker sends thousands of rejection messages into a victim network. After all, the message is not itself authenticated with an HMAC digest, and contains no unique serial number or other difficult to replicate field. It is simply an error code that represents the reason for rejecting the SS's attempt to authenticate.

Unfortunately for a would-be attacker, the message is only applicable for a very brief time during the authorization process. As shown in Figure 14, the Auth Reject message (shown highlighted) is only acted upon if the SS is in the Auth Wait state. An SS will only spend a short period in the Auth Wait state while awaiting BS authorization. At other times this message is discarded as non-applicable. For these reasons, the Auth Reject Attack is a failure.

## C. PROPOSED DENIAL OF SERVICE ATTACKS

Close examination of the IEEE 802.16 MAC reveals that there are at least two potential vulnerabilities that bear further examination and experimentation. The first potential vulnerability lies in the RNG-RSP message that is sent by the BS to set and maintain the proper timing of the SS transmissions. The second potential vulnerability comes from the specification for the Auth Invalid message.

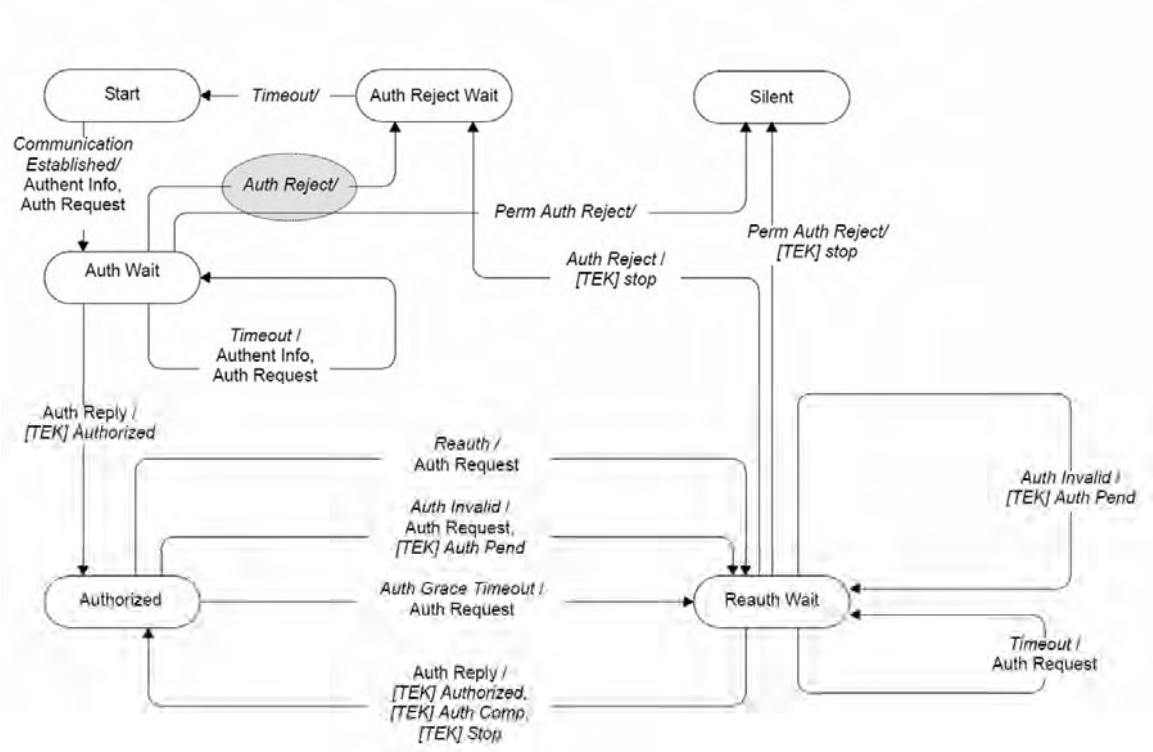


Figure 14. The Authorization State Machine. (From [3]).

### 1. The RNG-RSP Attack

The Ranging Request (RNG-REQ) message is the very first message sent by an SS seeking to join a network. The message announces the SS's presence and is a request for transmission timing, power, frequency and burst profile information. The message is also sent periodically to allow for adjustments on the part of the SS. The BS responds to the SS request using a Ranging Response (RNG-RSP) message. The format of the message is shown in Table 5.

| **Management Message Type** | **Uplink Channel ID (8-bits)** | **Message Contents** |
|---|---|---|
| 5 = RNG-RSP | ID of uplink channel on which BS received RNG-REQ | Shown in table XY. |

Table 5. Format of the RNG-RSP Message.

Early versions of the standard required an SS to make a RNG-REQ on a periodic basis. These requests would have been made during contention-based windows used for station maintenance. If an SS were unable to complete the periodic ranging process, it

would be excluded from the network and ordered to re-initialize its MAC. This created a dangerous DoS vulnerability. An attacker that could transmit enough interfering messages to fill all of the scheduled time for station maintenance would be able to prevent all SS from conducting periodic ranging, effectively shutting down the network.

Fortunately, the IEEE 802.16a revision of the standard changed this situation. The standard was revised to allow the BS to use any received packet to form the basis of a ranging adjustment. This frees the SS from the requirement to periodically re-range in a contention-based time slot. It also allows for more timely correction of timing and frequency drift.

Despite this change, the RNG-RSP message remains vulnerable to a potentially more serious type of exploitation. The problem is that the RNG-RSP message can do more than merely fine-tune SS transmission times. The BS can also use the RNG-RSP message to order the SS to change uplink and downlink channels, transmission power levels and even abort all transmissions and re-initialize its MAC. There are several reasons why the RNG-RSP message is vulnerable to exploitation: the message is not encrypted, it is not authenticated, and it is stateless. An SS will take the action directed by any validly formatted RNG-RSP that is addressed to it. For details of the encoded contents of the RNG-RSP message, refer to Table 6. According to the standard, the only required fields are the Timing Adjust, Power Level Adjust and Ranging Status. All other fields are optional.

There are a variety of ways that the message may be misused. The most basic way to abuse the message is to spoof unsolicited RNG-RSP messages with the Ranging Status field set to a value of 2, which corresponds to "abort." This attack is shown on the SS RNG-RSP flowchart, Figure 15. To address the message to a specific SS, the attacker would need to sniff the channel IDs in use by the victim. A less effective, brute force method would be to simply cycle through all 65,536 possible CIDs. This is a very inefficient, but fairly effective way to interfere with all nodes within range of the attacker's rogue transmitter. Also, since the standard specifies only that the CID be "arbitrarily chosen" it is possible that there will be implementations of the standard that

| Name | Type (1 byte) | Length (bytes) | Value |
|---|---|---|---|
| Timing Adjust | 1 | 4 | Tx timing offset adjustment (signed 32-bit). The time required to advance SS transmission so frames arrive at the expected time instance at the BS. Units are PHY specific. During periodic ranging, the range of the value of this parameter shall be limited to +/- 2 modulation symbols. |
| Power Level Adjust | 2 | 1 | Tx Power offset adjustment (signed 8-bit, 0.25 dB units) Specifies the relative change in transmission power level that the SS is to make in order that transmissions arrive at the BS at the desired power. |
| Offset Frequency Adjust | 3 | 4 | Tx frequency offset adjustment (signed 32-bit, Hz units) Specifies the relative change in transmission frequency that the SS is to make in order to better match the BS. (This is fine-frequency adjustment within a channel, not reassignment to a different channel.) |
| Ranging Status | 4 | 1 | Used to indicate whether uplink Messages are received within acceptable limits by BS.<br>1 = continue, 2 = abort, 3 = success, 4 = rerange |
| Downlink frequency override | 5 | 4 | Center frequency, in kHz, of new downlink channel on which the SS is to redo initial ranging.<br>If this TLV is used, the Ranging Status value shall be set to 2.<br>*Shall be used for licensed bands only*. |
| Uplink channel ID override | 6 | 1 | *Licensed bands:* The identifier of the uplink channel with where the SS should redo initial ranging (not used with PHYs without channelized uplinks).<br>*License-exempt bands:* The Channel Number where the SS should redo initial ranging. |
| Downlink Operational Burst Profile | 7 | 1 | This parameter is sent in response to the RNG-REQ Requested Downlink Burst Profile parameter. It contains the least robust DIUC that may be used by the BS for transmissions to the SS. |
| SS MAC Address | 8 | 6 | SS MAC Address in MAC-48 format |
| Basic CID | 9 | 2 | Basic CID assigned by BS at initial access. |
| Primary Management CID | 11 | 2 | Primary Management CID assigned by BS at initial access. |
| PHY Specific Values | 12-16 | | These were added by IEEE 802.16a to provide ODFMA and AAS support. |

Table 6. RNG-RSP Message Encodings. (After [3], [4] and [5]).

simply use sequential CIDs rather than truly arbitrary numbers. If the CIDs were not truly arbitrary, the attacker would only need a single active CID to use as the start point for a much more efficient brute force attack. The advantage of these types of brute force method is that an attacker wouldn't need to know much more than the operating channel of the network to be attacked.

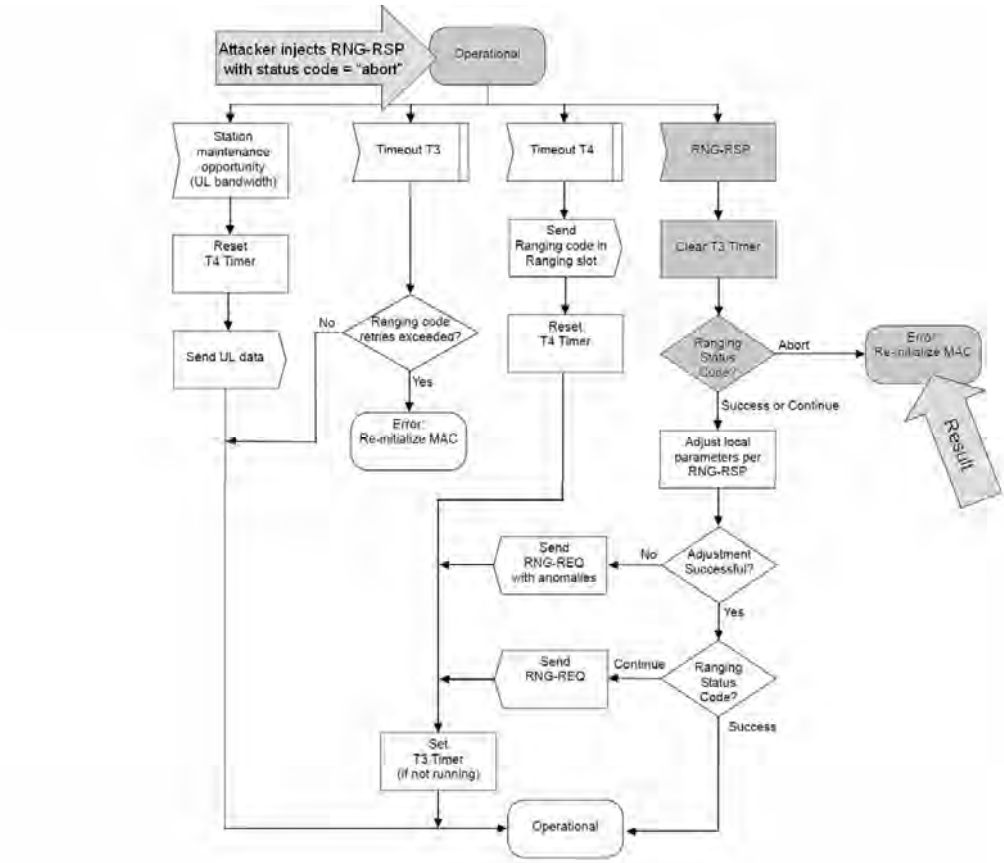


Figure 15. Flow of the RNG-RSP Attack. (After [7]).

Another way that the RNG-RSP message might be used is to shift a victim node to a channel of the attacker's choosing. The attacker would once again spoof the CID and message contents, however this time the message would be used to override the uplink and/or downlink channel(s) used by the SS. There are a couple of scenarios which might ensue. If the attacker has no BS operating at the specified channel, the SS will eventually find its way back to the proper channel, as it scans and discards unused frequencies. Depending on the number of channels available for use, this could take some time, as the SS must listen for a minimum of 2ms before moving onto the next channel (Note that frames are of .5ms, 1ms or 2ms duration). Alternately, an attacker could shift only the uplink, or only the downlink. This would certainly disrupt the proper operation of the SS, and might prove to be an effective DoS attack.

Shifting the victim SS to a channel of the attacker's choosing would also work very well when used in conjunction with a BS Spoof as described in the previous chapter. This would seem an ideal way to push an SS off of a legitimate BS and onto an illegitimate one.

### 2. The Auth Invalid Attack

As previously discussed, the "Auth Reject Attack" is a failure. However, the authorization state machine is a very attractive target and bears further investigation. The authorization state machine is one part of the privacy key management (PKM) system used in IEEE 802.16. It uses two basic types of MAC management messages—requests and responses. Requests, in the form of the PKM-REQ message, are made by SS. PKM-RSP is the response message sent by the BS. Table 7 shows the structure of these messages.

| **Management Message Type** | **Message Code** | **PKM Identifier** | **PKM Attributes** |
|---|---|---|---|
| 9 = PKM-RSP<br>10 = PKM-REQ | Identifies type of PKM message | Serial number of message | Varies from by type of message |

Table 7. PKM Message Format. (After [2]).

The Message Code is an 8-bit field that identifies the exact type of PKM message. Messages using invalid Codes are silently discarded. The complete list of PKM Codes and their meanings are listed in Table 8. The PKM Identifier is an 8-bit field that acts as a message serial number. The SS increments the identifier field each time it generates a new PKM-REQ. When the BS sends its PKM-RSP message, it includes the Identifier of the message it is responding to. The SS will discard response messages with Identifier fields that do not match a pending request. The PKM Attributes field varies by PKM message type. This field is used to provide amplifying information such as error codes, key lifetimes and display strings. For example, the Security Association Add message includes an Authorization Key sequence number and a series of SA Descriptors that specify the desired properties of the new security association.

| Code | PKM Message Type |
|---|---|
| 0-2 | *Reserved* |
| 3 | Security Association Add |
| 4 | Auth Request |
| 5 | Auth Reply |
| 6 | Auth Reject |
| 7 | Key Request |
| 8 | Key Reply |
| 9 | Key Reject |
| 10 | Auth Invalid |
| 11 | TEK Invalid |
| 12 | Authentication Info |
| 13-255 | *Reserved* |

Table 8. PKM Message Codes. (After [2]).

There are four PKM messages of interest: Auth Reject, Key Reject, Auth Invalid and TEK Invalid. These are interesting because these messages have a negative impact on the authorization state of the SS. Therefore, these messages make good candidates for use in attacks similar to the IEEE 802.11 Deauthentication Attack, discussed in an earlier chapter.

Three of these four messages can be quickly ruled out as possible candidates for use in a DoS attack. As discussed previously, the Auth Reject message requires the use of an HMAC digest to authenticate the message. If the HMAC digest sent by the attacker doesn't equal that calculated by the SS, the message is discarded. Therefore an attacker would need to be able to calculate correct HMAC digest values based on the current AK of the SS. Barring an unanticipated compromise in the cryptographic suite in use, this is extremely unlikely. It is also only used in the Auth Wait state of the authorization state

machine—a state that the SS passes through quite quickly. For these reasons the Auth Reject message is unsuitable for use in a DoS attack.

The Key Reject and TEK Invalid messages both require authentication by HMAC digest. The attributes of the Key Reject message are shown in Table 9 for illustration. As discussed above, this is a nearly insurmountable obstacle for an attacker to overcome. There is a second reason that the Key Reject message is unsuitable for use in a DoS attack. As required by the standard, the TEK Invalid message Identifier code is set to zero. However, the Key Reject message needs to have a PKM Identifier code that corresponds to the number of an open request by the SS. While this is only an 8-bit number (255 choices) this is another hurdle that must be overcome, either by brute force or intelligent guessing. Each guess would need a new HMAC calculation as well.

| Attribute | Contents |
|---|---|
| Key-Sequence-Number | Authorization key sequence number |
| SAID | Security Association ID |
| Error-Code | Error code identifying reason for rejection of Key Request |
| Display-String (optional) | Display string containing reason for Key Reject |
| HMAC-Digest | Keyed SHA message digest |

Table 9. Key Reject Message Attributes. (From [2]).

A much better choice of messages is the Auth Invalid message. As shown in Table 10, the Auth Reject message is not authenticated by HMAC digest. Therefore it would be easy to generate. Also, in stark contrast to the Auth Reject message, the Auth Invalid message will be accepted at almost any time during the SS's operation. While the SS is only in the Auth Wait state for a brief period, the vast majority of an SS's operational time is spent in the Authorized state where the Auth Invalid message is meaningful.

| Attribute | Contents |
|---|---|
| Error-Code | Error code identifying reason for Authorization Invalid |
| Display-String (optional) | Display String describing failure condition |

Table 10. Auth Invalid Message Attributes. (From [2]).

Even better for the attacker, the Auth Invalid error code includes a value that translates to a stateless rejection. This error code is sent *unsolicited* by the BS when an SS's HMAC digests fail to verify properly. For the full range of choices for Auth Reject/Auth Invalid error codes, see Table 11. Notable is error code 0, which sends no additional failure information whatsoever. Ironically, according to paragraph 11.2.10 of [2], this code was included for "security reasons." The final reason that the Auth Invalid message will most likely be accepted (and acted upon) is that this message does not employ the PKM Identifier serial number. The PKM Identifier for an Auth Invalid message is zero. Therefore, the SS will not reject the message on the basis of an invalid serial number because no serial number is expected. This is a consequence of the stateless nature of the message.

| Error Code | Messages | Description |
|---|---|---|
| 0 | All | No information |
| 1 | Auth Reject, Auth Invalid | Unauthorized SS |
| 2 | Auth Reject, Key Reject | Unauthorized SAID |
| 3 | Auth Invalid | Unsolicited |
| 4 | Auth Invalid, TEK Invalid | Invalid Key Sequence Number |
| 5 | Auth Invalid | Message (Key Request) authentication failure |
| 6 | Auth Reject | Permanent Authorization Failure |

Table 11. Auth Invalid Message Error-code Values. (From [3]).

As shown in Figure 16, the Auth Invalid message causes a transition from the Authorized state to the Reauth Wait state. The SS remains in this wait state until otherwise directed by the SS. When the Reauth Wait timer expires, a Reauth Request is sent by the SS, requesting another chance to rejoin the network. The duration of the Reauth Wait timer is measured in seconds.

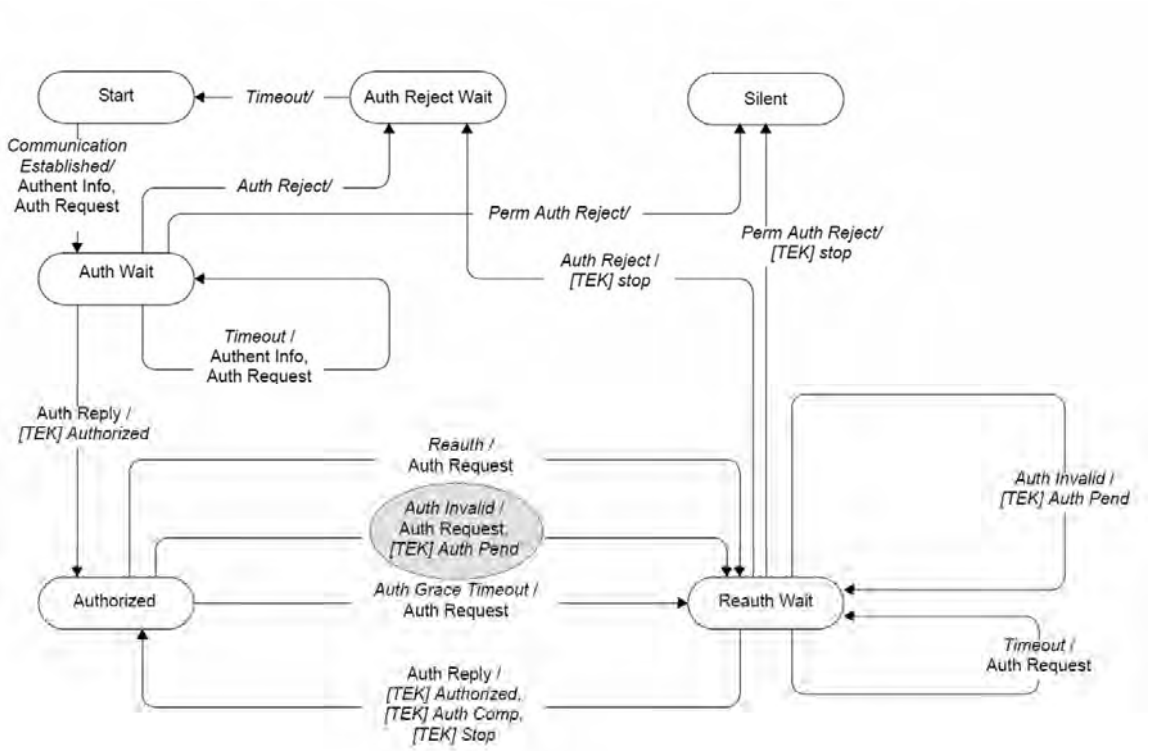


Figure 16. Authorization State Machine Highlighting the Auth Invalid message. (After [3]).

Another event that might occur while an SS Authorization State Machine is in the Reauth Wait state is the reception of an Auth Reject Message indicating a permanent error. This message forces the SS to transition to the Silent state and cease all subscriber traffic. While in the Silent state, the SS will still respond to management messages sent by the BS. Recall that the Auth Reject message is not authenticated by an HMAC, serial number or other means making it vulnerable to spoofing. Also note that the Auth Reject message was previously discovered to have little value as a DoS weapon because the SS spent little of its lifetime in the state required for the message to be processed. However, in this instance, the attacker is able to *force* the SS into a state where the Auth Reject message will be processed. By manipulating the Authorization State Machine, an attacker is thus able to multiply the effectiveness of the Auth Invalid DoS. He need simply follow up the Auth Invalid message with a Permanent Auth Reject message. The victim SS is pushed into the Silent state, awaiting a reset of its MAC.

## D. SUMMARY

At this point, these proposed denial of service attacks are pure conjecture, based only upon academic analysis of the written standard. Actual experimental testing, whether real-world or simulation is required to test the validity of these reported vulnerabilities. The true test of these attacks will be dependent upon the silicon embodiment of the standard, rather than the paper document.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. CONCLUSION AND RECOMMENDATIONS

## A. CONCLUSION

The vulnerabilities examined in this thesis are currently only theoretical, based on a paper evaluation of a printed standard. It remains to been seen if the actual equipment that is built around the standard is truly vulnerable to the attacks described here. In turn, whether these vulnerabilities may be actually exploited by practical means will also depend on the hardware units that become available. Even if these vulnerabilities truly are present in the equipment sold, by most measures, exploiting them will be difficult.

However, we cannot depend on this difficulty as an assumed form of protection. For example, cracking WEP is difficult. It took well educated and dedicated hackers to write the first program to exploit the wired equivalent privacy key stream re-use vulnerability. Now however, a hacker doesn't even need to know what WEP stands for to be able to circumvent it. The programs that are used to exploit the vulnerability are freely available on the Internet. If there are vulnerabilities inherent in IEEE 802.16, they will be exploited.

There is a *window of opportunity* to improve the security measures of the IEEE 802.16 standard before WiMAX certified equipment has been built and sold by the millions. Changes need to be made before there are many "legacy" WiMAX branded systems in customer hands and while there is still time to ensure interoperability with the earliest equipment.

The vulnerabilities inherent in IEEE 802.11 were only discovered after there were hundreds of thousands (if not millions) of units already in operation. Efforts to patch the newly discovered vulnerabilities were made piecemeal and well after the fact. As a result, the vast majority of Wi-Fi deployments remain at risk to denial of service attacks (and worse). The reputation of the standard has been damaged, and sales of Wi-Fi equipment have probably suffered somewhat. For IEEE 802.16, this situation can be avoided.

## B. RECOMMENDATIONS

There are several possible solutions to every vulnerability presented in this thesis, and each of these could be the subject of another piece of research. However, there are a few potential solutions the author would like to present as a starting point for further development.

### 1. Increase the Scope of the Privacy Sublayer

Currently, MAC Management messages are not permitted to be encrypted. This should change. Encrypt or authenticate all MAC Management messages unless there is a compelling reason not to. This alone would thwart most of the attacks presented in this thesis.

For most of the messages, the encryption required does not need to be able to withstand lengthy, offline attacks. The data contained within the MAC Management messages is only useful for a short period of time. Therefore, the encryption scheme employed does not need to use a particularly long encryption key. It just needs to be robust enough to delay an attacker by minutes, not years. Short keys can provide excellent protection if changed often enough. For example, any particular UL-MAP is only valuable to an attacker for a period of milliseconds before the assigned transmission windows will have passed. Just as there are Key Encryption Keys and Traffic Encryption Keys for use with algorithms of different strength (and by extension, different computational overhead), there could be a MAC Message Key that is even lighter in computational weight.

There are two basic benefits of encrypting MAC Management messages. First, it prevents an attacker from being able to easily craft malicious messages. Remember, the RNG-RSP message with code "Abort" only needs an easily sniffed CID for a target. If the message is encrypted, an attacker needs a CID *and a key*. The privacy layer has already allowed for the secure exchange of keys, so the attacker is out of luck. Second, encrypting MAC Management messages denies an attacker the information he needs to be able to the craft malicious messages in the first place. For example, if an attacker is not able to determine the CID of an SS, he must brute-force guess it.

One could think of this method as enforcing the principle of least privilege at the MAC Layer. For example, a node just entering the network doesn't need the privilege of knowing the entire UL-MAP. It just needs to know when *it* is allowed to transmit. So we could encrypt the portions of the UL-MAP that new nodes don't need to know.

### 2. Use the Statefulness of the MAC to Its Full Advantage

There will remain messages that cannot be encrypted. For example, one may point out that the RNG-RSP message discussed above may be sent before keys have been exchanged. Therefore it cannot be encrypted or authenticated with an HMAC. However, this is not entirely true. The message cannot be encrypted or authenticated only when keys have not yet been exchanged. At all other times it can be authenticated. So we should authenticate it whenever possible. For an example of this, see Figure 17, which is an adaptation of the actual RNG-RSP flowchart as seen in Figure 15. Portions of the flowchart not germane to this discussion were omitted and changes are highlighted.

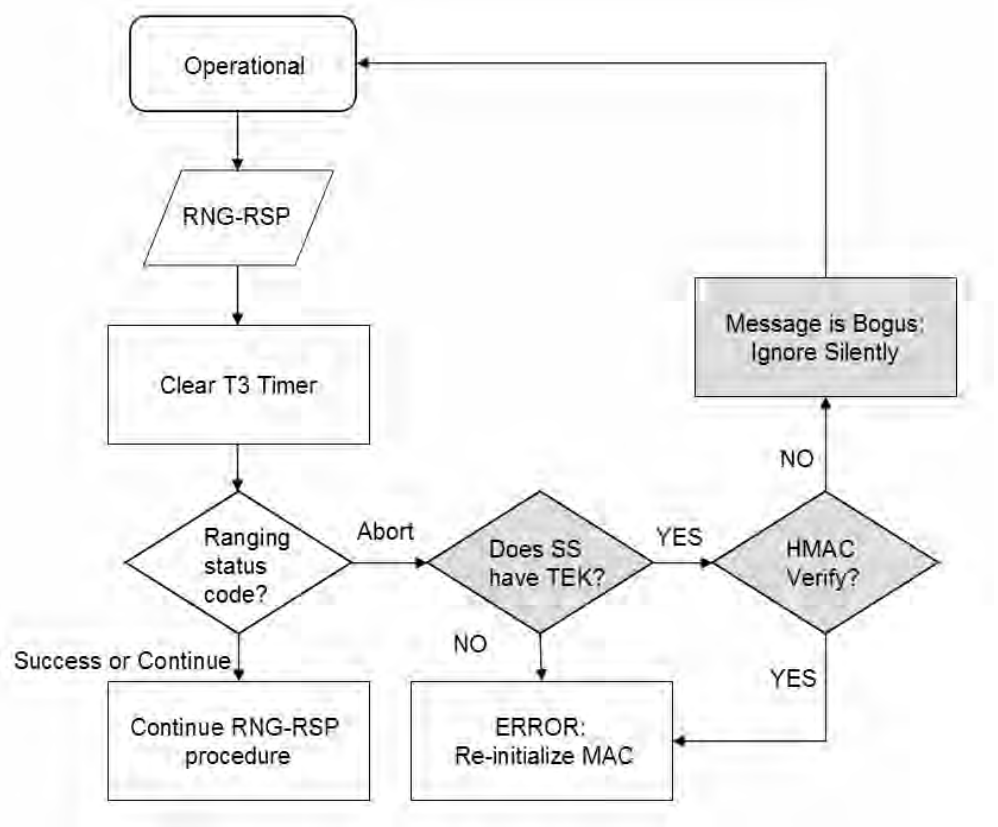


Figure 17. Modified Section of RNG-RSP State Machine. (After [7]).

With this modified state machine, the RNG-RSP attack will not work against an SS that has been authenticated on the network because it is in possession of securely exchanged encryption keys. The only time an attacker would be able to effect the RNG-RSP attack on an SS would be in the brief time between initial network entry and authentication.

A well written piece of computer code has error traps that deal with unexpected conditions. For example, well written code will include checks on the user input and reject numbers when characters are expected. This code would then warn the user of the error. Similarly, the MAC Layer should trap errors in its input. For example, a RNG-RSP with "Abort" as its code is by definition an unexpected state. It should be properly checked and an error code should be generated. This would inform the BS that the SS has received an Abort which may be of help diagnosing an attack.

### 3. Require Strong Two Way Authentication

One-way authentication is a poor method to prevent theft of service. If attackers are able to own the base station equipment, they are able to "own" an SS from a legitimate network. Hardware MAC addresses are insufficient protection. This has been a lesson painfully learned with IEEE 802.11. There are a variety of schemes suggested to provide strong two-way authentication, including IEEE 802.1X. Further research will show which method is best. Even though higher layer encryption (if used) will protect user data, BS spoofing still translates to an effective DoS attack.

### 4. "Band-aid" Fixes

Finally, there are a few specific fixes. These are rather disparagingly known as "band-aids" as they only address the superficial wound, not the underlying cause. In this case however, when the above measures have been taken, it is appropriate to repair minor flaws with minor fixes.

The Auth Invalid message that tells the Authorization state machine (Figure 16) to move to the Auth Wait state should be authenticated using an HMAC derived with a valid key. Since the TEK is suspect, one could use the KEK to perform the keyed hash that generates the HMAC. One could even use the SS's public key to encrypt this message.

### 5. Recommendations for Military Use

In the author's opinion, the standard is an excellent starting point for the basis of a military tactical network. Given that the above recommendations have been applied, there would remain changes required to create a military wireless network. Because of the unique military environment and requirement for very high availability, DoD should adopt an appropriately robust spread spectrum physical layer to improve conventional jamming resistance. Second, DoD should continue to use higher layer encryption to protect end-to-end transmissions.

### 6. Use the WiMAX Forum to Enforce More Than Interoperability

The WiMAX Forum is the body that verifies compliance with the IEEE 802.16 standard, and awards the WiMAX "seal of approval" to equipment that passes testing. However, all of the equipment that has caused problems in the IEEE 802.11 realm passed their Wi-Fi certification too. The problem is that bare compliance with the words of the standard is not enough. It is not enough to be interoperable. The equipment manufacturers have a responsibility to the rest of the consortium to ensure that their equipment meets the standard *and* meets security best practices. A set of equipment can meet the standard perfectly, but if it also includes a "bonus" test message that can be used as a very effective DoS weapon, the equipment should not pass certification. If an attacker cannot generate bogus messages, he certainly cannot transmit them. I recommend that the WiMAX forum require a thorough security examination of equipment that will bear its logo.

## C. SUGGESTIONS FOR FURTHER RESEARCH

This thesis is just an early look at a brand new standard. The opportunities for research are many. Aside from studying solutions to the specific issues addressed in this paper, there are entire fields of research that may be applied to investigate the IEEE 802.16 standard. Radio frequency propagation studies could investigate the extended range capabilities of the standard. Network managers will have a variety or questions that must be answered. There are issues of network co-existence that can be addressed.

Specifically, there are a few topics the author would like to suggest:

Test the proposed attacks either using pre-release equipment or network simulation software. Ideally, this research would be conducted using direct input from equipment developers.

Test the IEEE 802.16 MAC Layer with physical layers that will be useful for military application, including HF and DSSS signals.

Measure commercial equipment's resistance to conventional jamming techniques in order to improve the knowledge base for future offensive military actions. The equipment will be especially popular in countries that lack wired broadband infrastructure.

Conduct field testing in tactical environments to develop practical military applications for equipment based on the IEEE 802.16 standard. In their Naval Postgraduate School thesis [6], Munoz and Guice conducted preliminary tactical testing, but there is much more that can be done in this area. As important as developing equipment is the task of developing *doctrine* for the employment of tactically deployed broadband networks.

# APPENDIX. IEEE 802.16 MAC MANAGEMENT MESSAGES

This appendix was derived from Table 13 in [2], [7] and [8]. It is a list of all the IEEE 802.16 MAC Management Messages, plus Sender, Connection and Authentication information.

| Type | Message Name | Message Description | Sent By | Connection | Authentication |
|---|---|---|---|---|---|
| 0 | UCD | Uplink Channel Descriptor | BS | Broadcast | None |
| 1 | DCD | Downlink Channel Descriptor | BS | Broadcast | None |
| 2 | DL-MAP | Downlink Access Definition | BS | Broadcast | None |
| 3 | UL-MAP | Uplink Access Definition | BS | Broadcast | None |
| 4 | RNG-REQ | Ranging Request | SS | Initial Ranging or Basic | None |
| 5 | RNG-RSP | Ranging Response | BS | Initial Ranging or Basic | None |
| 6 | REG-REQ | Registration Request | SS | Primary Management | SS X.509 Cert |
| 7 | REG-RSP | Registration Response | BS | Primary Management | SS Pub Key |
| 8 | *reserved* | | | | |
| 9 | PKM-REQ | Privacy Key Management Request | SS | Primary Management | Varies |
| 10 | PKM-RSP | Privacy Key Management Response | BS | Primary Management | Varies |
| 11 | DSA-REQ | Dynamic Service Addition Request | BS or SS | Primary Management | HMAC |
| 12 | DSA-RSP | Dynamic Service Addition Response | BS or SS | Primary Management | HMAC |
| 13 | DSA-ACK | Dynamic Service Addition Acknowledge | BS or SS | Primary Management | HMAC |
| 14 | DSC-REQ | Dynamic Service Change Request | BS or SS | Primary Management | HMAC |
| 15 | DSC-RSP | Dynamic Service Change Response | BS or SS | Primary Management | HMAC |
| 16 | DSC-ACK | Dynamic Service Change Acknowledge | BS or SS | Primary Management | HMAC |
| 17 | DSD-REQ | Dynamic Service Deletion Request | BS or SS | Primary Management | HMAC |
| 18 | DSD-RSP | Dynamic Service Deletion Response | BS or SS | Primary Management | HMAC |
| 19, 20 | *reserved for future use* | | | | |
| 21 | MCA-REQ | Multicast Assignment Request | BS | Primary Management | None (Message does includes a unique Transaction ID) |
| 22 | MCA-RSP | Multicast Assignment Response | SS | Primary Management | None (Message does includes a unique Transaction ID) |
| 23 | DBPC-REQ | Downlink Burst Profile Change Request | SS | Basic | None |
| 24 | DBPC-RSP | Downlink Burst Profile Change Response | BS | Basic | None |

| Type | Message Name | Message Description | Sent By | Connection | Authentication |
|---|---|---|---|---|---|
| 25 | RES-CMD | Reset Command | BS | Basic | HMAC |
| 26 | SBC-REQ | SS Basic Capability Request | SS | Basic | None |
| 27 | SBC-RSP | SS Basic Capability Response | BS | Basic | None |
| 28 | CLK-CMP | SS network clock comparison | BS | Broadcast | None (Message has sequence number) |
| 29 | DREG-CMD | De/Re-register Command | BS | Basic | HMAC |
| 30 | DSX-RVD | DSx Received Message | BS | Primary Management | Indirectly from authenticaton of DSx-REQ message |
| 31 | TFTP-CPLT | Config File TFTP Complete Message | SS | Primary Management | HMAC |
| 32 | TFTP-RSP | Config File TFTP Complete Response | BS | Primary Management | None |
| 33 | ARQ-Feedback | Standalone ARQ Feedback | BS or SS | Basic | None |
| 34 | ARQ-Discard | ARQ Discard message | BS or SS | Basic | None |
| 35 | ARQ-Reset | ARQ Reset message | BS or SS | Basic | None |
| 36 | REP-REQ | Channel measurement Report Request | BS | Basic | None |
| 37 | REP-RSP | Channel measurement Report Response | SS | Basic | None |
| 38 | Reserved | | | | |
| 39 | MSH-NCFG | Mesh Network Configuration | BS or SS | Broadcast | Varies (Reject message is not authenticated) |
| 40 | MSH-NENT | Mesh Network Entry | SS | Basic | HMAC |
| 41 | MSH-DSCH | Mesh Distributed Schedule | SS | Broadcast | None |
| 42 | MSH-CSCH | Mesh Centralized Schedule | BS | Broadcast | None |
| 43 | MSH-CSCF | Mesh Centralized Schedule Configuration | BS | Broadcast | None |
| 44 | AAS-FBCK-REQ | AAS Feedback Request | SS | Basic | None (uses Request serial numbers) |
| 45 | AAS-FBCK-RSP | AAS Feedback Response | BS | Basic | None (uses Request serial numbers) |
| 46-255 | Reserved | | | | |

Table 12. MAC Management Messages. (After [3], [4], [5]).

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


[1] Wi-Fi Alliance Press Release. "Wi-Fi Alliance Announces Additional Wi-Fi® Certification Laboratories." [http://www.wi-fi.com], July 2004. Accessed 14 August 2004.

[2] The Institute of Electrical and Electronics Engineers. *IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE Std 802.16-2001. IEEE, 2001.

[3] The Institute of Electrical and Electronics Engineers. *IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE Std 802.16-2004. IEEE, 2004.

[4] Alvarion Ltd. "Introducing WiMAX, the Next Broadband Wireless Revolution." 2004.

[5] K. Wongthavarawat, A. Ganz. "IEEE 802.16 Based Last Mile Broadband Wireless Military Networks With Quality of Service Support." *Proceedings of MILCOM 2003*. IEEE, 2003.

[6] R. Guice, R. Munoz. *IEEE 802.16 Commercial Off the Shelf (COTS) Technologies as a Compliment to Ship to Objective Maneuver (STOM) Communications.* Naval Postgraduate School Master's Thesis, September 2004.

[7] The Institute of Electrical and Electronics Engineers. *IEEE Standard for 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 Std 802.16a-2003. IEEE 2003.

[8] The Institute of Electrical and Electronics Engineers. *IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems—Amendment 1: Detailed System Profiles for 10-66GHz*, IEEE Std 802.16c-2002. IEEE 2002.

[9] Siemens Business Services, Inc. "Wireless Broadband Report Presented to the Wireless Houston County Committee." 2004.

[10] Alvarion Ltd. "Verizon, Two Tech Firms Team to Bring Wireless Broadband to Grundy, Va." Press Release 23 August 2004.

[11] The Institute of Electrical and Electronics Engineers. *IEEE Standard for Local and Metropolitan Area Networks Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11 1999 Edition. IEEE, 1999.

[12] J. Bellardo and S. Savage. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions." Presented at 11th USENIX Security Symposium, 2003.

[13] C. Wullems, K. Tham, J. Smith, M. Looi. "A Trivial Denial of Service Attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANs." *Proceedings of the 2004 Wireless Communications Symposium*. IEEE, 2004.

[14] R. Boshonek. *Advanced Denial of Service Techniques in IEEE 802.11b Wireless Local Area Networks.* Naval Postgraduate School Master's Thesis, June 2002.

[15] W. Meyers. *Exploitation of an IEEE 802.11 Standard Wireless Local Area Network Through the Medium Access Control (MAC) Layer.* Naval Postgraduate School Master's Thesis, June 2001.

[16] H. Krawczyk, M. Bellare and R. Canetti. "Internet Engineering Task Force Request for Comments: 2104." [http://www.ietf.org/rfc/rfc2104.txt], 1997. Accessed 7 August 2004.

[17] Alvarion Ltd. "Alvarion BreezeACCESS VL 5.8GHz Version 1.2 System Manual." 2004.

[18] RedLine Communications. "AN-50 PTP System User Manual" 2004.

[19] The Register. "Intel: WiMAX in notebooks by 2006." [http://www.theregister.co.uk/2004/07/02/intel_wimax/] September 2004. Accessed 12 September 2004.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Organization of Addressee
   Camp Pendleton, California

4. Roger Marks
   National Institute of Standards and Technology, U.S. Department of Commerce
   Boulder, Colorado

5. LCDR Joseph Staier, Assistant Dean of Electrical & Computer Engineering
   US Coast Guard Academy
   New London, Connecticut

6. Prof. Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

7. Prof. Brian Steckler
   Naval Postgraduate School
   Monterey, California

8. MAJ Carl Oros
   Naval Postgraduate School
   Monterey, California