Chapter 4 – OVERVIEW OF 802.16 – MILITARY RELEVANCE

In the following pages, an overview of the 802.16 standards is provided. Broadband wireless access (BWA) and the related frequency bands used are first defined, and a brief history of BWA standards is presented. A more detailed analysis and overview of the multiple standards, activities and projects initiated within the 802.16 study group is then presented. These include the 802.16-2001 physical (PHY) and Medium Access Control (MAC) standard for the 10 – 66 GHz band, the 802.16a air interface for 2 – 11 GHz with the corresponding MAC enhancements, the recommended practice for coexistence of fixed broadband wireless access systems: 802.16.2-2001 (for 10 – 66 GHz) and the 802.16.2a (for 2 – 11 GHz). Work has also been initiated by the 802.16 group to cover Interoperability Testing (802.16c and 802.16d) and a set of Test Protocols are being developed for this purpose. Finally a mobility project has been initiated (802.16.e) to bring a level of portability or mobility into the standard.

At this time, very few (if any) commercial products follow the 802.16 standard, but many manufacturers have plans to migrate their systems to support the standard. One reason why so few commercial products support the standard is because the standard is very new, is changing, and for some frequency bands, is still under development.

Finally, it is seen that improved security measures at the MAC layer have been introduced for 802.16 (compared to previous standards such as 802.11b). These measures should satisfy the privacy requirements for commercial products but may not be sufficient for military applications.

An analysis is performed on the possibility of using the 802.16 commercial products for military communications. It is concluded that because this commercial standard is designed to meet each country's regulatory restrictions and minimize interference, it produces, by military standards, a non-robust (vulnerable) signal that could be a significant liability in many tactical situations. There is no doubt that the 802.16 standard physical layer is highly vulnerable to signal detection and interruption. Traditional EW techniques of detection, direction finding (DF), and jamming of such a non-robust signal should prove effective and within the capabilities of almost any conceivable adversary.

Because of the large range of the transmissions (a few kilometers), the 802.16 signal is particularly vulnerable since it is made available (for interception and detection) to anyone located within this large perimeter.

Notwithstanding the physical layer robustness issues, given that the 802.16 is a new, unproven standard, it is also recommended at this time to wait until its widespread deployment before considering it further for military applications. As we have seen with the 802.11 standard, the first and second generations of the standard implementations contained a number of weaknesses that are only now being corrected. Hence, given the limited availability of commercial systems that supports 802.16, the real weaknesses of 802.16 are expected to surface only later, when these systems become widely deployed, and when they are subjected to greater exposure and become the target of hackers.

4.1 BROADBAND WIRELESS ACCESS

Broadband wireless access (BWA) is directed at providing broadband data access to businesses and homes using an inexpensive wireless infrastructure. The goal is to provide an economical and competitive solution to wired and satellite broadband. The wireless infrastructure consists of fixed (stationary) customer premise units, served by fixed terrestrial base stations. Services typically include broadband Internet access, digital video and telephony. Supported protocol could include TCP/IP as well as ATM.

4.1.1 Frequency Bands for BWA

Various frequency bands have been allocated across the world to support broadband wireless access. For example, some of the allocations include:

- Millimeter wave bands:
  - 18 – 24 GHz, 26 GHz (ETSI), 27.5 – 29.5 GHz, 38 GHz (ETSI), etc.;
  - LMDS (28 and 31 GHz) in the U.S. and some other countries;
  - Largest spectrum in private hands; and
  - 25 times as large as PCS spectrum cap.
- Microwave (centimeter wave) bands:
  - 3.5 GHz in most countries, 10 GHz in some others; and
  - 2.5 GHz in the U.S. (MMDS) and some other countries.
- License-Exempt bands, e.g. in many countries:
  - 5.725 – 5.825 GHz, 5.15 – 5.35 GHz;
  - 2.4 GHz Wireless LANs; and
  - 57 – 64 GHz.

4.1.2 Broadband Wireless Access Standards History

A few projects were initiated to try to standardize the Physical (PHY) and MAC layers used for broadband wireless access. In particular, two of the major initiatives are:

- The Broadband Radio Access Networks (BRAN) initiative of the European Telecommunications Standards Institute (ETSI). It includes the HIPERACCESS and HIPERMAN standards (see below).
- The 802.16 initiative, started in the USA by Roger Marks, from the National Institute of Standards and Technology, U.S. Department of Commerce. This initiative started with a project development in the summer of 1988 and was followed by the creation of an IEEE study group that led to the formation of an IEEE 802.16 standard group[1]. Current and former membership of the 802.16 standard groups includes over 144 companies from 12 countries[2].

A very short description of HIPERACCESS and HIPERMAN is given below. Since the goal of this report is to study 802.16, the rest of this report will be dedicated to the IEEE standard.

4.1.3 Broadband Wireless Access in ETSI BRAN

- BWA effort share many features of HiperLAN2 (the 5 GHz WLAN solution).
- HIPERACCESS:
  - For frequencies above 11 GHz;
  - Line-of-sight connections, up to 5 miles (8 km) range;

[1] The main 802.16 web site is at web addresses: http://WirelessMAN.org or http://ieee802.org/16/.

[2] Countries of 802.16 Members (current and former, as of July 2002): Canada (48), Finland (4), France (2), Germany (2), Greece (2), Israel (22), Italy (1), Japan (2), Korea (4), Spain (1), UK (11), USA (161).

- 25 to 60 Mbps data rates, using Single Carrier;
- HIPERACCESS began before 802.16; and
- HIPERACCESS is completing its work.

The current versions of HIPERACCESS Physical Layer specification (TS 101 999), the HIPERACCESS System Overview (TR 102 003) and the HIPERACCESS Data Link Layer specification (TS 102 000) can be found on the ETSI/BRAN web site[3].

- HIPERMAN:
  - For frequencies below 11 GHz;
  - Does not need line of sight, up to 15 miles (24 km) range;
  - 10 to 25 Mbps data rates; and
  - Selected 802.16 MAC/802.16a OFDM PHY as baseline.
- Harmonization efforts under way to have some degree of compatibility with 802.16.

The current versions of the "Functional Requirements for Fixed Wireless Access systems below 11 GHz: HIPERMAN" (TR 101 856), and the draft HIPERMAN Physical layer, Data Link Control (DLC) layer and System Reference documents can be found on the ETSI/BRAN web site[4].

4.2 THE 802.16 STANDARDS, PROJECTS AND ACTIVITIES

4.2.1 Scope of the IEEE 802.16

The IEEE 802.16 Working Group on Broadband Wireless Access Standards develops standards and recommended practices to support the development and deployment of broadband Wireless Metropolitan Area Networks (WMAN).

The 802.16 standard specifies the physical layer (PHY) and medium access control layer (MAC) of the air interface of interoperable point-to-multipoint broadband wireless access systems. The specification enables access to data, video, and voice services with a specified quality of service. The medium access control layer is structured to support multiple PHY specifications, each suited to a particular operational environment, both in licensed bands designated for public network access and in license-exempt bands. It applies to systems operating between 2 and 66 GHz, where such services are permitted.

The 802.16-2001 standard includes a particular physical layer specification applicable to systems operating between 10 and 66 GHz. This 10 – 66 GHz air interface, based on single-carrier modulation, is known as the WirelessMAN-SC air interface. An amendment to this standard, to support 2 – 11 GHz using an enhanced version of the same basic medium access control layer along with new physical layer specifications, is in development in Project 802.16a.

4.2.2 Overview of the 802.16 Standards, Projects and Activities

The IEEE Standard 802.16-2001 supports a point-to-multipoint topology in which each base station, normally connected to a public network, communicates with potentially hundreds of stationary subscriber stations, each of which is typically mounted on a rooftop. Through the WirelessMAN MAC, each base

[3] http://www.etsi.org/t_news/0202_bran.htm

[4] http://portal.etsi.org/bran/Summary.asp

station allocates uplink and downlink bandwidth to satisfy, almost instantaneously, the prioritized bandwidth requirements of the subscribers. The air interface is designed to carry any data or multimedia traffic with full Quality of Service (QoS) support. The MAC supports burst frequency-division duplex (FDD) and time-division duplex (TDD) in a consistent framework. It also supports real-time adaptive modulation and coding so that, in each burst, communication in the link to each subscriber station is optimized at that instant.

The IEEE Standard 802.16-2001 defines the WirelessMAN-SC air interface, a single-carrier (SC) modulation scheme for 10 – 66 GHz operation. At these frequencies, propagation is strictly line-of-sight, but tremendous spectral allocations such as 1.3 GHz of spectrum in the U.S. Local Multipoint Distribution Service (LMDS) allocation, are available. The standard takes full advantage of the allocations, specifying bit rates of up to 120 Mbps on each reusable 25 MHz channel. The primary markets will include commercial, industrial, and multi-tenant residential buildings. In further support of this industry, the 802.16 Working Group has completed IEEE Standard 802.16.2-2001, a Recommended Practice on Coexistence, and is currently developing, in Project 802.16c, system profiles for use in compliance and interoperability testing.

While the WirelessMAN MAC in IEEE Standard 802.16-2001 provides the foundation for a wireless MAN industry, the physical layer (PHY) is not suitable for lower-frequency applications, where the available spectrum allocations are narrower and near non-line-of-sight operation is possible. For this reason, most of the recent efforts in the 802.16 Working Group have gone toward the development of IEEE Project 802.16a, an amendment to address 2 – 11 GHz operation. Successive versions of the 802.16a draft have been in ballot since November 2001, and the details are nearing completion. The amendment includes both licensed and 5 – 6 GHz license-exempt bands. In the licensed bands, the current draft provides for compliance using any of three physical layer modes: single-carrier (SC) modulation, orthogonal frequency division multiplex (OFDM), or orthogonal frequency division multiple access (OFDMA), with advanced antenna options supported. For the license-exempt spectrum, the current 802.16a draft specifies the OFDM mode.

In license-exempt operation, wireless MANs are susceptible to interference with other wireless MANs as well as with other devices such as wireless LANs. As one solution to this problem, the 802.16a draft specifies a dynamic frequency selection (DFS) method for license-exempt bands similar to the one being standardized in IEEE Project 802.11h. The draft also supports the use of a mesh architecture in which some subscriber stations communicate with other data-forwarding subscriber stations rather than directly with the base station. This allows extending the cells and reaching customers not directly reachable from the base station. The defined scheduling algorithms provide for collision-free transmissions in mesh deployment. The protocols also eliminate the hidden-terminal problem typical of wireless LANs.

The work of the 802.16a group should be completed within the next few months. The next great hurdle for the 802.16 group is to bring a level of portability or mobility into the standard. To support this initiative the Working Group recently initiated the Study Group on Mobile Broadband Wireless Access (Project 802.16e), whose scope includes: “mobile broadband wireless access networks supporting mobility at vehicular speeds.”

One important new player is the Worldwide Interoperability for Microwave Access (WiMAX) Forum, whose mission includes promoting IEEE Standard 802.16 to achieve global acceptance as well as developing and implementing test procedures to ensure interoperability.

Related to interoperability, the 802.16 working group has initiated a series of projects to form the basis of compliance and interoperability testing. This work will include the production of a Protocol Implementation Conformance Statement (PICS) as well as a Test Suite Structure and Test Purposes document.

The activities of 802.16 and its various standards and projects are summarized in Table 4-1.

Table 4-1: Summary of 802.16 Standards, Projects (P) and Activities

IEEE 802.16 Standards, Projects(P) and Activities		
AIR INTERFACE STANDARD **(PHYs with common MAC)**	**802.16-2001** (10 – 66 GHz)	• MAC • PHY for 10 – 66 GHz • Approved by IEEE in Dec. 2001
	P802.16a amendments (2 – 11 GHz)	• MAC Enhancements • PHY for 2 – 11 GHz • Licensed and license-exempt bands • Draft 6 released in Oct. 2002 • Approval expected early 2003
COEXISTENCE **(Recommended Practice)**	**802.16.2-2001** (10 – 66 GHz)	• 10 – 66 GHz • Approved by IEEE in July 2001
	P802.16.2a amendments (2 – 11 GHz)	• Includes 2 – 11 GHz licensed • Draft 1 done in September 2002 • Completion expected mid-2003
Follow-up Projects		
Interoperability Testing	**P802.16c** (10 – 66 GHz)	• Used as basis of compliance and interoperability testing • Draft 4 released in Oct. 02 • Approval expected early 2003
	P802.16d (2 – 11 GHz)	• New project, to form the basis of 2 – 11 GHz interoperability testing.
Test Protocols **(10 – 66 GHz)**	**P1802.16.1**	• Protocol Implementation Conformance Statement (PICS) • Started; final expected early 2003
	P1802.16.2	• Test Suite Structure and Test Purposes (started Oct. 02)
Mobility **(initially for < 6 GHz)**	**MBWA** – Mobile Broadband Wireless Access **(P802.16e)**	• Study Group formed in Mar. 02 • To investigate mobility enhancements for 802.16a
Other Activities related to 802.16		
Forum for the coordination of interoperability testing	**WiMAX** Worldwide Interoperability for Microwave Access	• To certify the interoperability of BWA products and technologies under a global standard • Support 802.16 • Developing and submitting baseline test specs

4.3 SOME OF THE TECHNICAL CONSIDERATIONS OF 802.16-2001 (10 – 66 GHZ)

The IEEE 802.16-2001 standard[5] was approved by IEEE in December 2001. It specifies the air interface, including the MAC and PHY layers, of fixed point-to-multipoint broadband wireless access systems providing multiple services. The standard includes a particular physical layer specification broadly applicable to systems operating between 10 and 66 GHz.

4.3.1 Properties of IEEE Standard 802.16-2001

- Broad bandwidth:
  - Up to 134 Mbps in 28 MHz channel (in 10 – 66 GHz air interface).
- Supports multiple services simultaneously with full QoS:
  - Efficiently transport IPv4, IPv6, ATM, Ethernet, etc.
- Bandwidth on demand (frame by frame).
- MAC designed for efficient used of spectrum.
- Comprehensive, modern, and extensible security.
- TDD and FDD.
- Link adaptation: Adaptive modulation and coding:
  - Subscriber by subscriber, burst by burst, uplink and downlink.
- Point-to-multipoint topology.

4.3.2 More Technical Details

More technical details on the PHY and MAC layers of the 802.16-2001 standard are provided in Annex A and in Table 4-2 in the following section.

4.4 AMENDMENT PROJECT IEEE 802.16A – AIR INTERFACE FOR 2 – 11 GHZ

This standard will extend the IEEE 802.16 WirelessMAN standard for applicability to 2 – 11 GHz bands, both licensed and license-exempt, and provide a foundation for the expansion of wireless metropolitan area networks in residential neighborhoods. It will include Medium Access Control Modifications and additional Physical Layer Specifications for 2 – 11 GHz. This standard is still under development, with Draft 6 released in October 2002. Approval by IEEE is expected by the end of 2002 or early 2003.

- **Licensed Bands**

The 2 – 11 GHz bands provide a physical environment where, due to the longer wavelength, true LOS may not be totally necessary and multipath may be significant. The channel bandwidths used in this physical environment typically vary from 1.5 to 28 MHz. Channel bandwidths allowed shall be limited to the regulatory provisioned bandwidth divided by any power of 2 no less than 1.25 MHz.

[5] http://standards.ieee.org/getieee802/download/802.16-2001.pdf

- **License-Exempt Bands (primarily 5 – 6 GHz)**

The physical environment for the 2 – 11 GHz license-exempt bands is similar to that of 2 – 11 GHz licensed bands. However, the license-exempt nature introduces additional interference and co-existence issues, whereas regulatory constraints limit the allowed radiated power. In addition to the features of licensed band, the PHY and MAC introduce mechanisms such as:

- DFS (dynamic frequency selection) to detect and avoid interference; and
- Support for Mesh topologies.

4.4.1 P802.16a PHY Alternatives

The PHY layer varies according to different applications, band plans, and regulatory environments. The three 2–11 GHz air interface specifications suggested in the draft 802.16a standard are:

- WirelessMAN-SC: This uses a single-carrier (SC) modulation format.
  - TDMA (TDD/FDD)
  - BPSK, QPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM
  - Most vendors will use Frequency-Domain Equalization
- WirelessMAN-OFDM: This uses orthogonal frequency-division multiplexing with a 256-point transform. Access is by TDMA. This air interface is mandatory for license-exempt bands.
  - 256-point FFT with TDMA (TDD/FDD)
- WirelessMAN-OFDMA: This uses orthogonal frequency-division multiple access with a 2048-point transform. In this system, multiple access is provided by addressing a sub-set of the multiple carriers to individual receivers.
  - 2048-point FFT with OFDMA (TDD/FDD)

4.4.2 Key P802.16a MAC Features

- OFDM/OFDMA Support.
- ARQ.
- Dynamic Frequency Selection (DFS) for license-exempt.
- Optional Advanced Antenna System (AAS) support.
- Mesh Mode:
  - Optional topology for license-exempt operation only;
  - Subscriber-to-Subscriber (relay) communications; and
  - TDD only.

4.5 COMPARISON OF KEY FEATURES OF 802.16-2001 AND P802.16A

The features of the 802.16-2001 and Project 802.16a standards are summarized and compared in Table 4-2.

Table 4-2: Comparison of Key Features of 802.16-2001 and 802.16a

	802.16-2001	P802.16a – Licensed and Licensed Except (LE) Bands		
		SC	*OFDM*	*OFDMA*
Frequency Band	10 – 66 GHz	2 – 11 GHz	2 – 11 GHz	2 – 11 GHz
Data Rate	2 – 155 Mbps			
LOS consideration	LOS	Near-LOS	Near-LOS	Near-LOS
Typical channel bandwidth	20 – 28 MHz	1.5 – 28 MHz	1.5 – 28 MHz	1.5 – 28 MHz
Center frequency	Multiple of 250 kHz	No restriction as long as Quadrature modulation used	$5000+5n_{ch}$ (MHz) n_{ch}=0,1,…199 for LE bands	$5000+5n_{ch}$ (MHz) n_{ch}=0,1,…199 for LE bands
Uplink scheme	DAMA-TDMA	TDMA	TDMA	CDMA
Downlink scheme	TDM	TDM	TDM	TDM
Duplexing techniques	TDD, FDD, H-FDD	TDD FDD H-FDD	FDD, H-FDD, TDD (in LE bands, only TDD)	FDD, H-FDD, TDD (in LE bands, only TDD)
Uplink modulation type	QPSK, 16 QAM, 64 QAM	Block adaptive modulation	OFDM Data: QPSK, 16 QAM, 64 QAM	OFDM Data: QPSK, 16 QAM, 64 QAM
Uplink FEC code type	RS, RS+ convolutional, coding, RS+ Parity Check, Turbo code	RS, Pragmatic TCM, BTC, CTC (convolutional turbo code)	Concatenated RS+ convolutional coding, BTC, CTC	Concatenated RS+ convolutional coding, BTC, CTC
Downlink modulation type	QPSK, 16 QAM, 64 QAM	Block adaptive modulation	OFDM QPSK, 16 QAM, 64 QAM	OFDM Data: QPSK, 16 QAM, 64 QAM
Downlink FEC code type	RS, RS+ convolutional, RS+ Parity Check, Turbo coding	RS, Pragmatic TCM, BTC, CTC	Concatenated RS+ convolutional coding, BTC, CTC	Concatenated RS+ convolutional coding, BTC, CTC
MAC support of PHY	Unframed FDD, Framed FDD, TDD	TDD, FDD	TDD, FDD (in mesh mode = only TDD)	TDD, FDD (in mesh mode = only TDD)
MAC	Basic	Basic, (ARQ), (STC), (AAS)	*Licensed*: Basic, (ARQ), (STC), (AAS)	*Licensed:* Basic, (ARQ), (STC), (AAS)
			License-exempt: Basic, DFS, (ARQ), (STC), (MSH), (AAS)	*License-exempt:* Basic, DFS, (ARQ), (STC), (MSH), (AAS)

4.6 RECOMMENDED PRACTICE FOR COEXISTENCE OF FIXED BROADBAND WIRELESS ACCESS SYSTEMS – IEEE 802.16.2 AND P802.16.2A

The 802.16.2-2001 recommended practice[6] for the bands 10 – 66 GHz was approved by IEEE in July 2001. Amendments are under way in Project 802.16.2a to provide a recommended practice for coexistence in the bands 2 to 11 GHz.

4.6.1 802.16.2-2001

This Recommended Practice provides guidelines for minimizing interference in fixed broadband wireless access systems. Pertinent coexistence issues are addressed, and recommended engineering practices provide guidance for system design, deployment, coordination and frequency system usage. This document covers frequencies of 10 – 66 GHz in general, with particular focus on 23.5 – 43.5 GHz bands. If followed by manufacturers and operators, it should allow for a wide range of equipment to coexist in a shared environment with acceptable mutual interference.

4.6.2 P802.16.2a

The goal of this project is to amend the "Recommended Practice for Coexistence of Fixed Broadband Wireless Access Systems" above to include the frequency bands 2 – 11 GHz. It takes into consideration the coexistence issues with point-to-point systems utilized in these bands. Draft 6 of this recommended practice was completed in October 2002 and approval by IEEE is expected by the end of 2002 or early 2003.

4.7 INTEROPERABILITY TESTING AND TEST PROTOCOLS FOR 802.16

4.7.1 P802.16c (System Profiles for 10 – 66 GHz)

This project, which was officially initiated in May 2002, aims at fostering the development of interoperability tests for systems built to the 10 – 66 GHz WirelessMAN-SC air interfaces. Draft 4 was released in October 2002 and approval by IEEE is expected in early 2003.

- Used as basis of compliance and interoperability testing:
    - MAC Profiles: ATM and IP Packet; and
    - PHY Profiles: 25 and 28 MHz; TDD and FDD.

4.7.2 P802.16d System Profiles for 2 – 11 GHz

In September 2002, the 802.16 Working Group approved submission of proposed Project Authorization Request (PAR) P802.16d on 2 – 11 GHz System Profiles. This work is expected to form the basis of 2 – 11 GHz interoperability test specifications.

4.7.3 P1802.16.1 Test Protocols for 10 – 66 GHz

Project P1802.16.1 is to define a Protocol Implementation Conformance Statement (PICS). Proforma document for the WirelessMAN-SC air interface. A full proposed PICS draft was received as a contribution in the fall 2002, and a Call for Comments on it was issued. The document is called "Draft Standard for Conformance to IEEE Standard 802.16 – Part 1: Protocol Implementation Conformance

[6] http://standards.ieee.org/getieee802/download/802.16.2-2001.pdf

Statement (PICS) Proforma for 10 – 66 GHz WirelessMANTM-SC Air Interface". Completion is expected in 2003.

4.7.4 P1802.16.2 Test Suite Structure and Test Purposes

The Working Group approved submission of a PAR to initiate the P1802.16.2 "Test Suite Structure and Test Purposes" for the 10 – 66 GHz. This would be the second of three anticipated conformance and interoperability test documents for this band.

4.8 MOBILE BROADBAND WIRELESS ACCESS FOR 802.16A

In March 2002, the 802.16 working group formed the Mobile Broadband Wireless Access Study Group to investigate mobility enhancements to 802.16. This group will address enhancements to the IEEE 802.16a PHY/MAC to support nomadic and mobile operation, roaming, and cell-to-cell and sector-to-sector handoff capability as well as other protocol and MIB support.

In September 2002, the 802.16 Working Group endorsed a project prepared by the Mobile Wireless MAN Study Group. The proposed project P802.16e will amend IEEE Standard 802.16 by specifying "Physical Layer and Medium Access Control Modifications for Mobile Operation in Licensed Bands below 6 GHz".

4.9 WIMAX FORUM

As a non-profit organization, the objective of WiMAX is to promote wide-scale deployments of point-to-multipoint networks operating between 2.5 and 66 GHz by leveraging new global consensus standards (802.16) and certifying the interoperability of various products and technologies from multiple manufacturers.

- WiMAX[7] = Worldwide Interoperability for Microwave Access.
- Mission: To promote deployment of BWA by using a global standard and certifying interoperability of products and technologies.
- Principles:
  - Support IEEE 802.16:
    - Initially above 11 GHz, but now also includes 2 – 11 GHz;
  - Propose access profiles for the IEEE 802.16 standard;
  - Guarantee known interoperability level;
  - Promote IEEE 802.16 standard to achieve global acceptance; and
  - Open for everyone to participate.
- Currently Developing and submitting baseline test specifications.
- WiMAX comprises of industry leaders who are committed to the open interoperability of all products used for broadband wireless access.
- Will certify interoperability levels both in network and the cell.

[7] http://www.wimaxforum.org/about/index.asp

The Test specifications developed will be used to:

- Ensure that equipment and systems claiming compliance to the standard or a profile have been sufficiently tested to demonstrate that compliance.
- Guarantee that equipment from multiple vendors has been tested the same way, to the same interpretation of the standard, increasing the interoperability of the equipment.
- Enable independent conformance testing, giving further credibility to the previous two items.

4.9.1 What's Next for 802.16

- Complete the 2 – 11 GHz work.
- Enhance the 10 – 66 GHz specifications:
  - Interoperability test protocols.
- Complete the 802.16c and the 802.16d interoperability testing projects.
- Complete the PICS and test protocols (P1802.16.1, P1802.16.2).
- New enhancements (initiated):
  - Mobility, repeaters, etc.
- Build a basis for 4G wireless.

An update on the latest plans and developments related to 802.16 can be found on the IEEE WirelessMAN web site.[8,9]

4.9.2 802.16 Commercial Products

Given that the 802.16 standard is so new, and in some bands (e.g. 2 – 11 GHz) is still under development and may experience further changes, very few products (if any) exist that can claim to be fully 802.16 compliant. Most commercial products that were found claim some partial compliance, or have plans to migrate to become compliant in the future.

Annex B provides a short description of some of these systems (the list is not exhaustive, but presents a few examples of systems and sub-systems that plan to be compatible with 802.16-2001 or 802.16a).

Some manufacturers also plan to migrate their 802.11a products to support the 802.16a standard.

4.9.3 Security and Encryption in 802.16

In both 802.16 and 802.16a, the MAC layer contains a separate Security Sublayer that provides authentication, secure key exchange, and encryption. For the purpose of privacy, there are two component protocols:

- An encapsulation protocol for encrypting packet data across the fixed broadband wireless access network.

[8] IEEE 802.16 Project Development Milestones: http://ieee802.org/16/milestones.html

[9] IEEE 802.16 Published Standards and Drafts: http://ieee802.org/16/published.html

- A key management protocol (Privacy Key Management, or "PKM") providing the secure distribution of keying data from the Base Station (BS) to the Subscriber Stations (SSs). Through this key management protocol, SS and BS synchronize keying data; in addition, the BS uses the protocol to enforce conditional access to network services.

Overall, security and privacy n the 802.16 can be summarized as follow:

- Secure over-the-air transmissions.
- Protocol descends from BPI+ (from DOCSIS).
- Designed to allow new/multiple encryption algorithms.
- Authentication:
  - X.509 certificates with RSA;
  - Strong authentication of SSs (prevents theft of service); and
  - Prevents cloning.
- Data encryption:
  - Currently 56-bit DES in CBC (cypher block chaining) mode; and
  - Initialization Vector (IV) based on frame number.
- Message authentication:
  - Most important MAC management messages authenticated with one-way hashing (HMAC with SHA-1).

Hence, it can be seen that many security issues have been addressed in the 802.16 standard. Although this security implementation may be sufficient to provide privacy in commercial networks, it does not address some of the requirements needed to make this communications systems a robust military system. This is discussed further in the conclusion below.

4.10 CONCLUSIONS

The use of a commercial technology for military applications should not be based strictly on its known vulnerabilities. These vulnerabilities can sometimes be overcome with additional measures. It should also be considered that given enough time, almost any potential attackers will be able to find holes in most systems. The anticipated tactical use of a communications system must be the main consideration when determining whether the benefits of such a system outweigh the risks associated with the vulnerabilities. Rather than attempting to acquire the perfect system, which most likely does not exist, it is the program manager's responsibility to acquire one that meets the requirements, as required by the operational environment.

With this frame of reference, it is worthwhile undertaking to try to evaluate the impact of the WMAN potential vulnerabilities on the entire communication network. Because the WMAN is based on the 802.16 standard, which only defines operations at the physical and MAC layers, the vulnerabilities explored below are restricted to those two levels.

4.10.1 Physical Layer

There should be little question that the 802.16 standard physical level is highly vulnerable to signal detection and interruption. A commercial standard designed to meet a country's spectrum administration regulatory restrictions and designed to minimize interference will most likely produce, by military standards, a non-robust (vulnerable) signal that could be a significant liability in many tactical situations. Traditional EW techniques of detection, direction finding (DF), and jamming of such a non-robust signal should prove effective and within the capabilities of almost any conceivable adversary. Certain measures can be taken to modify the physical layer of commercial systems, but their effects may be minimal unless major redesign is done. A major redesign would result in a non-commercial, more expensive system, which may have few advantages compared to a system designed from the start for military applications.

4.10.2 MAC Layer

As was seen recently for the 802.11, through a very public debate, MAC layer weaknesses related to inadequate authentication techniques and the use of the WEP protocol showed that this standard was inadequate in providing basic privacy to the users. Although such weaknesses should undoubtedly be a concern in a tactical environment, these weaknesses are more easily correctable than the physical layer vulnerabilities. For example, higher level security protocols and procedures can be implemented or added to the standard to minimize the extent of the MAC compromise.

The 802.16 addresses many of the MAC layer weaknesses discovered in previous standards such as the 802.11, and the design is more robust. It is also more flexible and it allows the use of new/multiple encryption algorithms. Authentication, data encryption and secure over the air transmission provided by the 802.16 may be adequate to protect privacy for the commercial users, but it still does not fully implement the level of security and encryption required by most defense organizations. Adding additional measures of protection on top of the ones provided may reach this goal. It should be noted that the prime motivation for the private sector is the desire for more throughput and low costs, certainly not security at a level as the one required for military operations.

4.10.3 General Conclusions

Many military organizations around the world are experimenting with COTS-based wireless networks to support the next generation of operational concepts which put great emphasis on information superiority. It must be anticipated that a potential adversary will be well prepared with sufficient EW systems and a good understanding of the underlying technology. We could therefore expect to see a resurgence of traditional EW systems, capable of signal detection, DF, and communications jamming. Given this inevitability, it is imperative that a robust RF signal, displaying low probability of detection (LPD) and anti-jam characteristics be employed to ensure the units that will carry out military operation have a reliable means of communications to enable dominant maneuver in the battlefield. With this factor in mind, the impact of the MAC layer security vulnerabilities appears small compared to those of the physical layer.

Some applications that require less advanced capabilities or those that may be conducted in a secure restricted (limited and controlled) physical environment, may well take advantages of COTS systems such as the 802.16. On the other hand, reliable communications in any difficult environment that must go undetected and undisturbed will not be satisfied by this commercial standard. There may also be additional military requirements that need to be implemented and that do not always have their equivalent in the commercial world. An example is the feature of being able to destroy remotely a terminal should it fall into enemy hands.

Notwithstanding the physical layer robustness issues described above, given that the 802.16 is a new, unproven standard, it is also recommended at this time to wait until its widespread deployment before

considering it further for military applications. As we have seen with the 802.11 standard, the first and second generations of the standard implementations contained a number of weaknesses that are only now being corrected (e.g. WEP) by issuing new standards (e.g. 802.11g). Hence, given the limited availability of commercial systems that supports 802.16, the real weaknesses of 802.16 are expected to surface only later, when these systems become widely deployed, and when they are subjected to greater exposure and become the target of hackers. Additional difficulties may also surface with the optional use of the Mesh configuration in 802.16a.

Finally, additional characteristics/limitations and issues that may have to be considered when evaluating the use of a commercial wireless standard such as the 802.16 include:

- The use of the wireless devices in one country may not be approved for use in another country, since each country allocates its frequency resources differently.
- Wireless MANs are susceptible to interference, interception, and can be jammed.
- Wireless MANs may create backdoors into military LANs; also, the various wireless and wired interconnection capabilities of WMAN devices present a significant risk that classified information will be compromised over an unclassified medium.
- Those implementing wireless MANs must investigate additional security measures for data confidentiality and network intrusion protection, such as the use of Virtual Private Network (VPN) gateways.
- Administrator must ensure that the users cannot enter a wireless MAN without strong authentication. As a minimum, strong authentication should include extended service set identifier (ESSID) and a media access control (MAC) address identification with an integrity lock. MAC address resolution alone does not quality as strong authentication.
- Multiple wireless transmission-multiplexing techniques are used in the commercial world. Each transmission standard is incompatible with the others. Equipment operating using one standard cannot communicate with equipment using a different standard.
- Where wireless MANs are to be implemented, thorough analysis, testing, and risk assessment must be done to determine the risk of information intercept/monitoring and network intrusion.
- All users must be provided security awareness training regarding the physical and information security vulnerabilities of the wireless devices.