# Global Information Assurance Certification Paper

**“Security Implications in WirelessMAN™ Technology”**
**(IEEE 802.16 Standard)**

Bruno Paranhos
Date: July 2, 2003

GSEC Practical Assignment, Option 1
Version: 1.4b

## Abstract

The 802.16 standard, developed by IEEE (Institute of Electrical and Electronics Engineers, Inc.), which is named as WirelessMAN™, gives a new perspective in accessing the internet in high-rates without depending on wired networks. As it is supposed to cost less than other broadband technologies like: xDSL and Cable Modem, and WirelessMAN™ offers higher-rates especially in uplink (requests from the subscriber station to the base station).

But the speed of the connection or all the improvements brought by the technology are not the only important aspects that have to be evaluated, due to the fact that wireless transmission is known as a unsafe method for communication. The security issues need to be considered when deciding which broadband technology is the best for Internet access. In this scenario, this article focus in the security implications of the WirelessMAN™ technology based on the specifications of the 802.16 standard.


## The IEEE 802.16 Standard

Before getting into the security implications it is important to talk about the 802.16 standards. The IEEE 802.16 Workgroup, has been working on this standard since 1999, and until the beginning of 2003 two standards had been developed:

The IEEE 802.16 WirelessMAN™ Standard ("Air Interface for Fixed Broadband Wireless Access Systems") addresses Wireless Metropolitan Area Networks. Following a two-year effort, the initial standard, covering systems between 10 and 66 GHz, was approved, in December 2001, for publication. IEEE Standard 802.16 was published on 8 April 2002. The Working Group is currently developing an amendment 802.16a to expand the scope to licensed and license-exempt bands from 2 to 11 GHz. The 802.16c amendment is in progress, developing 10-66 GHz system profiles to aid interoperability specifications[1].

The IEEE 802.16.2 is a Recommended Practice on "Coexistence of Fixed Broadband Wireless Access Systems" covering 10-66 GHz. IEEE Standard 802.16.2 was published on 10 September 2001 and is now available for download without charge. In developing, Amendment 802.16.2a, the Working Group is expanding the scope include to licensed bands from 2 to 11 GHz as well as enhancing the recommendations regarding point-to-point systems[1].

In 2002, The WiMAX (Worldwide Interoperability for Microwave Access) forum was created, with the purpose of advancing the broadband wireless market through the use of a global standard, ensuring that the vendors will follow the 802.16 standard, the organization is composed by systems integrators interested in Wireless market[2].

---

[1] Chang, D., *IEEE 802.16 Technical Backgrounder*, p. 4

[2] Skarp, M., *An Introduction to the World Interoperability for Microwave Access (WiMAX) Forum*, p. 5

The market is expecting the first WirelessMAN™ commercial implementation in the middle of 2004, until now only tests and experiences had been developed.

**"How does it work?"**

The WirelessMAN™ covers a 30 miles area where thousands of subscribers will share the channels and signals to transmit their data and offers speeds of up to 155 Mbps. The security aspects involved in the technology are very important and will be evaluated by the possible clients that have to decide between keeping accessing the Internet by ADSL or Cable Modem technologies, for example, or subscribe to the WirelessMAN™ technology.

This standard defines the physical and data link layer for a network architecture, where there are fixed Base Stations (BS), distributed by the city area, which perform point-to-multipoint communication with mobile clients (SS). And the BS is connected to the public network.

Basically, the WirelessMAN™ traffic can be divided in three parts (*Fig. 1*):

1. A subscriber sends wireless traffic as speeds ranging from 2 Mbps to 155 Mbps from Subscriber Station (SS) to a Base Station (BS);

2. The BS receives transmissions from multiple sites, and sends traffic over wireless or wired links to a switching center using 802.16 protocol;

3. The switching center sends traffic to an ISP or the public switched telephone network.

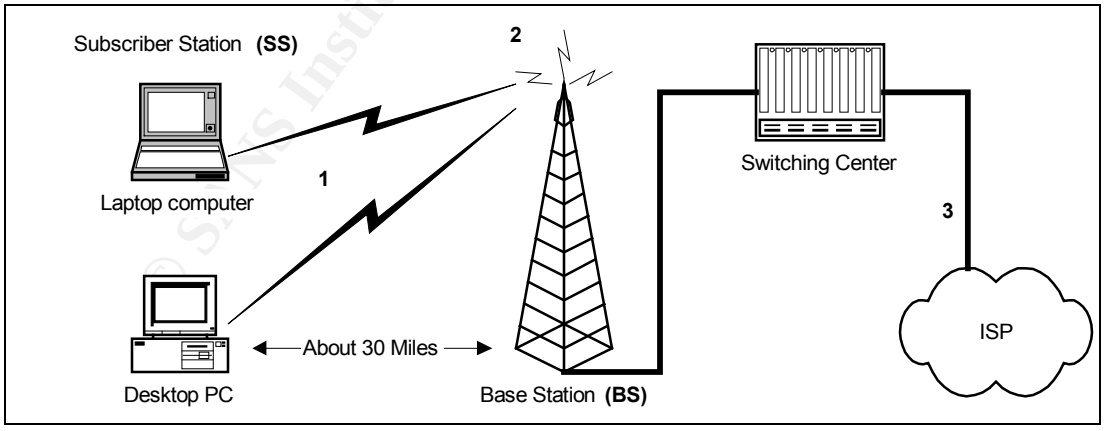


Figure 1 – How does it work?

**Major Threats**

In a WirelessMAN™ implementation, there will be an *unwired* MAN (Metropolitan Area Network) covering almost all the city area, where thousands of subscribers will be sharing the same media – the air – for transferring data. The most important challenge for the engineers, that developed the standard, is to guaranty that data from one user will not be available for other clients.

In the communication between the SS and the BS the TDMA technology is used. TDMA is the short for *Time-Division Multiple Access*; this technology is used by the 2G mobile phones and is famous for its cloning problems. To guaranty the confidentiality of the subscriber data, the standard states that all the traffic between the SS and BS is encrypted using X.509 digital certificates with RSA public key encryption.

The X.509 technology is an ITU recommendation, which means that has not yet been officially defined or approved. As a result, companies have implemented the standard in deferent ways.

Based on the WirelessMAN™ standard the major threats to the subscribers are:

- Theft of the signal and/or service;
- Theft of the user's data;
- Cloning.

To address each one of these threats the IEEE 802.16 workgroup decided to adopt a method that includes: Authentication, Authorization and Encryption to improve the security in the standard. The standard consider the utilization of strong authentication at SS utilizing X.509 certificates with RSA Public-Key Cryptography Standard (PKCS), this is to prevent theft of service and cloning[3].

Authentication and Authorization to the Subscriber Station is implemented by the utilization of the SS manufacturer's X.509 certificate binding the SS's public-key to its other identifying information (such as: UserID, SS's name,). It is supposed to exist a trust relation between the SS and the BS. Although, it is not presented in a basic WirelessMAN™ infrastructure, the presence of a "root authority" could be accommodated.

The third part of the security associated with IEEE 802.16 standard is encryption, the IEEE 802.16 Workgroup decided to encrypt the data using a 56-bit DES in CBC mode[4], a cipher this big can be easily exportable. The cyphertext errors are not propagated in plaintext to make difficult for other clients to "listen" the communication. The standard was designed to allow new or multiple encryption algorithms.

[3] Marks, R., *The IEEE 802.16 WirelessMAN™ MAC: It's Done, But What Is It?*, p. 59-68
[4] Pereira, R., Adams, R., *The ESP CBC-Mode Cipher Algorithms*, p. 1

The key MAC management messages are authenticated with one-way hashing, according to the standard (HMAC with SHA-1).

**SS Authentication and Registration**

Each Subscriber Station (SS) contains both a manufacturer-issued factory-installed X.509 digital certificate and the certificate of the manufacturer. These certificates, which establish a link between the 48-bit MAC address of the SS and its public RSA key, are sent to the BS by the SS in the *Authorization Request* and *Authentication Information* messages. The network is able to verify the identity of the SS by checking the certificates and can subsequently check the level of authorization of the SS. If the SS is authorized to join the network, the BS will respond to its request with an Authorization Reply containing an Authorization Key (AK) encrypted with the SS's public key and used to secure further transactions.[5]

After a successful authentication and them an authorization the SS is registered in the network. After the registration a secondary management connection is established between the SS and the BS and determine capabilities related to connection setup and MAC Operation.

Only after a successful authentication and registration the subscriber will receive an IP Address, by a DHCP server, and will get the access to the Wireless MAN.

**The Layered Structure**

The first layer, the physical layer, specifies the frequency band, the modulation scheme, error-correction techniques, synchronization between transmitter and receiver, data rate and the time-division multiplexing (TDM) structure.

Above the physical layer are the functions associated with providing service to subscribers. These functions include transmitting data in frames and controlling access to the shared wireless medium, and are grouped into a media access control (MAC) layer. The MAC protocol defines how and when a base station or subscriber station may initiate transmission on the channel. Because some of the layers above the MAC layer, such as ATM, require quality of service, the MAC protocol must be able to allocate radio channel capacity to satisfy service demands.

Located between the Physical Layer and the MAC Layer, the *Privacy Sublayer* is responsible for most of all the security that is implemented in WirelessMAN™ technology. The security is established by encrypting the connection between the subscriber station (SS) and the base station (BS).

[5] Marks, R., *IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access*, p. 106-107

## The Privacy Sublayer

The *Privacy Sublayer* provides the security needed by the mobile clients across the broadband wireless network (BWA), it does this by encrypting the connections between the SS and BS.

In addition, Privacy sublayer provides operators with strong protection against theft of service. The BS protects against unauthorized access to these data transport services by enforcing encryption of the associated service flows across the network. The Privacy Sublayer employs an authenticated client/server key management protocol in which the BS, the server, controls distribution of keying material to client SS. Additionally, the basic privacy mechanisms are strengthened by adding digital-certificate-based SS authentication to its key management protocol[6].

The Privacy Sublayer is divided in two parts (protocols):

1. The encapsulation protocol responsible for encrypting the data through the BWA network;

2. A key management protocol (Privacy Key Management, or PKM) that provides a secure key distribution between BS and SS.

## Privacy Key Management (PKM) Protocol

The Privacy Key Management (PKM) Protocol is based on DOCSIS 1.1[7], but received enhancements to achieve the desired security for IEEE 802.16 standard and to accommodate stronger cryptographic methods.

An SS uses the PKM protocol to obtain the Authorization by the BS, it includes other operations such as: periodic re-authentications and key refresh. When a SS wants to log on to the BS, it will send an Authentication Information (AI) message to the BS. This message contains the SS's unique X.509 certificate issued by the SS's manufacturer. After the SS has shown its identity to the BS, it then sends an Authorization Request (AR) message. This message requests the BS to grant access to the network and contains more detailed security related information such as the supported encryption methods at this SS. When the BS receives both the AI and AR messages, it then validates the SS's identity and checks its permission. If permission is granted, the BS will issue a security association identity (SAID) with the requesting SS and an authorization key (AK) encrypted with the SS's public key. The authorization reply has a sequence number to avoid reply attacks. Also, the key has a definite lifetime and re-authorization is required periodically. This protects the network from replay

[6] Marks, R., *802.16 IEEE Standard for Local and Metropolitan Area Networks*, p. 169-199
[7] Gummalla, A., *DOCSIS Overview*, p. 17-19

attacks and enforces frequent changing of private keys. Before the current key expires, the SS would need to obtain new authorization from the BS to avoid service disruption. (*Fig. 2*)

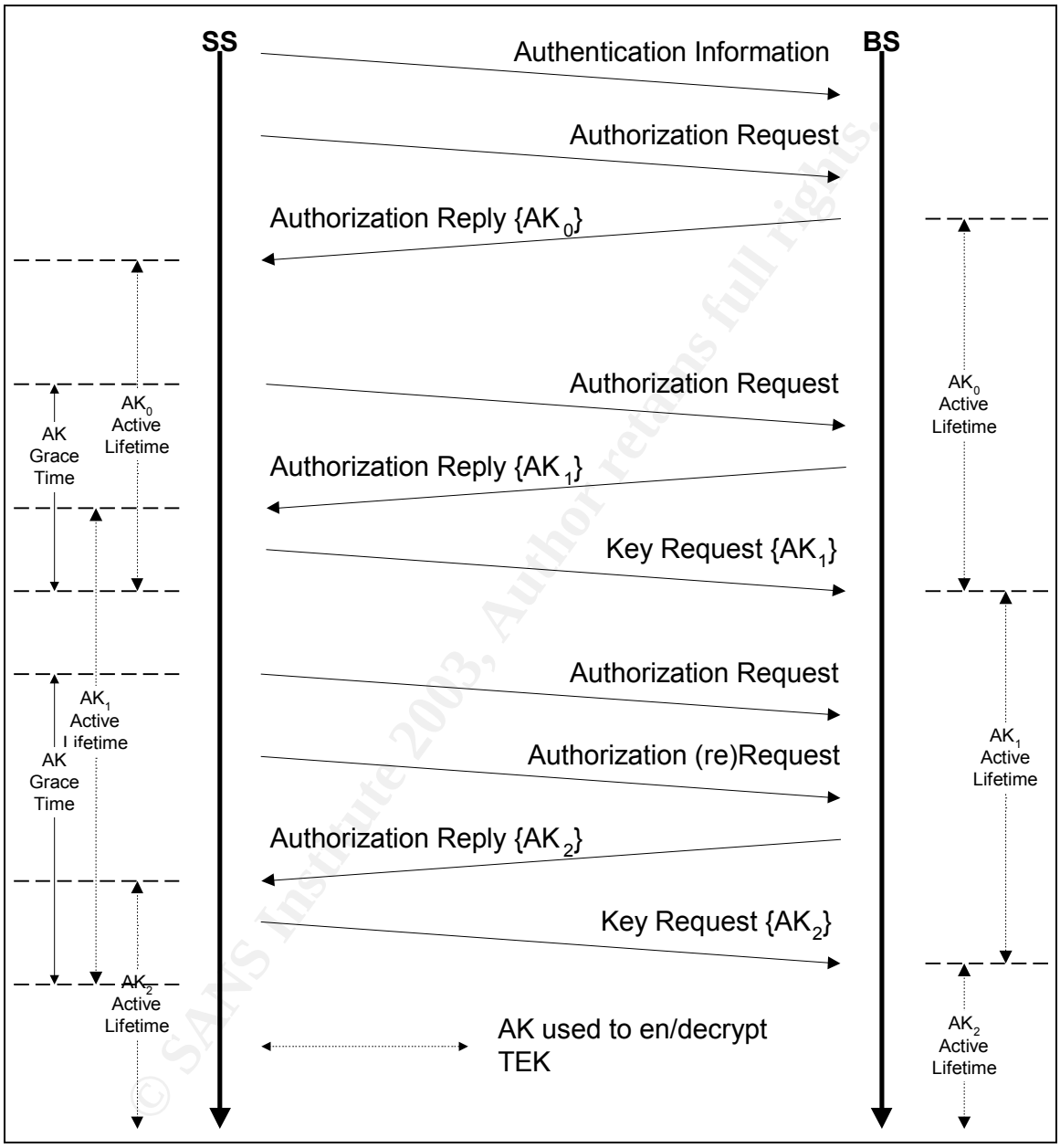


Figure 2 – Authentication Method[6]

The PKM protocol follows the client/server model, where the SS is the PKM client and the BS the PKM server, the client requests the keying material to the server,

[6] Marks, R., *802.16 IEEE Standard for Local and Metropolitan Area Networks*, p. 169-199

and the server must assure that the client receives only the keying material it is authorized to.

The PKM protocol uses public-key cryptography to establish the authorization key between SS and BS. This shared secret is then used to secure the exchanges of traffic encryption keys.

As long as BS authenticates the SS, it can protect against an attacker by a *cloned* SS, pretending to be an official SS. And the use of the X.509 certificates also increase the security, preventing a *cloned* SS from passing false certificates to the BS.

All SSs shall have factory-installed RSA private/public key pairs or provide an internal algorithm to generate such key pairs dynamically. If an SS relies on an internal algorithm to generate its RSA key pair, the SS shall generate the key pair prior to its first Authorization Key (AK) exchange. All SSs with factory-installed RSA key pairs shall also have factory-installed X.509 certificates. All SSs that rely on internal algorithms to generate an RSA key pair shall support a mechanism for installing a manufacturer-issued X.509 certificate following key generation[6].

**Security Associations**

The PKM protocol is based on the concept of the Security Associations (SA). The SA is a set of cryptography methods and the associated keying material, that is, it contains the information about which algorithms to apply, which key to use, and so on. A SS establishes at least on SA during the process of initialization, every connection, with the exception of the basics and management connections, is mapped to a SA[3].

Each service requires its own security association. After the SS is authorized, it then initiates the Traffic Encryption (TEK) state machine for each security association. After the initial authorization, each SS has its own primary SA. New service can dynamically add more SA later. TEK is responsible for managing the keys used for encryption for the actual data traffic of each service. The SS sends a Key Request to the BS, and the BS replies with a randomly generated private key to the SS. This key is encrypted with 3DES using the key obtained during the authorization process.

After the private encryption key is obtained for each SA, all data traffic is encrypted with symmetric key algorithms. Currently the specification only supports 56-bit DES in CBC mode, which has already been shown to be breakable. However, the encryption algorithm can be easily changed by specifying a different encryption algorithm in the authorization messages.

[3] Marks, R., *The IEEE 802.16 WirelessMAN™ MAC: It's Done, But What Is It?*, p. 59-68

There are three types of SAs: *Primary*, *Static* and *Dynamic*. Each SS establishes a *Primary* SA with the BS during the initialization process. *Static* SAs are provisioned with the BS. And *Dynamic* SAs are established and finished for each started and finished service during the connection. Every SS has a unique and exclusive *Primary* SA with the BS, but all the *Static* and *Dynamic* SAs can be shared by multiple SSs. The BS shall ensure that each client SS only access to the SAs it is authorized to access[6].

The SS uses the PKM protocol to request for the keying material to the BS, the Keying material is composed by the Data Encryption Standard (DES) key and CBC Initialization Vector, and it has a lifetime. The SS is responsible for asking the BS for new material before the actual expires at the BS. The actual keying material has to expire before a new set is received. The PKM protocol is also responsible the keying synchronization between the BS and SS.

**Key Maintenance at BS and SS**

The BS is responsible for maintaining keying information for all SAs and the SS is responsible for sustaining authorization with its BS and maintains an active Authorization Key.

After an SS finishes the basic capabilities negotiation, it shall start an authorization exchange with its BS. The BS's first receipt of an *Auth Request* message from the unauthorized SS shall start the activation of a new Authorization Key (AK), which the BS sends back to the requesting SS in an *Auth Reply* message. This AK shall remain active until it expires according to its predefined AK Lifetime.

If an SS fails to reauthorize before the expiration of its current AK, the BS shall not hold any active AKs for the SS, and shall consider the SS unauthorized. A BS them remove all TEK associated with the unauthorized SS.

The BS shall always be prepared to send an AK to SS upon a request. The BS shall be able to support two actives AKs for each client SS. The BS has two active AKs during an Authorization Key transition period; the two keys have overlapping lifetimes.

AKs have a limited lifetime and shall be periodically refreshed. An SS refreshes its Authorization Key by reissuing an *Auth Request* to the BS[6].

**Cryptographic Methods**

When it was first projected, the PKM protocol was designed to use X.509 digital certificates with RSA public key encryption for SS authentication and authorization key exchange. For traffic encryption, the Data Encryption Standard

[6] Marks, R., *802.16 IEEE Standard for Local and Metropolitan Area Networks*, p. 169-199

(DES) running in the cipher block chaining (CBC) mode with 56-bit keys is present in the IEEE 802.16 standard. The CBC initialization vector is dependent on the frame counter and differs from frame to frame. To reduce the number of computationally intensive public-key processing during normal operation, the transmission encryption keys are exchanged using 3DES with a key exchange key derived from the authorization key[3].

The PKM protocol messages themselves are authenticated using Hashed Message Authentication Code (HMAC) protocol with SHA-1. In Addition, message authentication in vital MAC functions, such as the connection setup, is provided by the PKM protocol[3].

One good aspect of the encryption solution designed for the PKM protocol, is that it is both robust and modular, the 56-bit DES present in IEEE 802.16 standard is acknowledge to have a limited lifetime and new encryption algorithms will be need. The PKM protocol was designed in a way that changing the data encryption algorithm has no impact on overall structure, and has no impact in the PKM protocol operation either. It brings the flexibility in setting the encryption algorithm, the keying lifetimes and/or the key lengths.

**Conclusion**

Wireless technologies have been growing in importance lately; they bring new opportunities for telecommunication without depending on wired networks offered by telephony service providers or cable-TV companies. In this scenario, new solutions such as WirelessMAN™, can be a fast and cheap way of getting a broadband Internet access.

The IEEE 802.16 standard offers wireless access in high-rates for metropolitan areas, one of the good aspects of the technology is that with just a few Base Stations (BS) a company can cover a big city, offering access to a million of subscribers. Because of this, it is cheaper and faster for a service provider company to built the entire wireless infrastructure than to pass all the wires needed through the city. The WirelessMAN™ can even be a solution for the undeveloped countries and for rural areas, in providing broadband access where the wired network is not widely distributed or available.

Although not designed to be a replacement for local area network, the 802.16 standard can provides insights on possible improvements to 802.11. For example, 802.16 provides strong authentication of clients and encryption.

The IEEE 802.16 standard enforces strong SS authentication. Each SS has its own unique X.509 certificate and it is not easily forgeable assuming the equipment manufacturers are trusted. Also, the double layer of key exchange provides additional security. Each service has a different key. Therefore, even if

[3] Marks, R., *The IEEE 802.16 WirelessMAN™ MAC: It's Done, But What Is It?*, p. 59-68

one service's key is compromised, it does not compromise the entire system. The limited lifetime of the private key prevents the attacker from having enough data to perform statistical cryptanalysis. In addition, the standard allows flexibility in the encryption method: it can be easily upgraded to stronger encryption algorithms if needed in the future. However, the authentication is not balanced. The BS itself is not authenticated.

Until today, there are no commercial implementations of the WirelessMAN™, it is expected to be available for customers in the middle of 2004, so this article was based on the standards and articles posted on Internet, what is going to happen in the future is difficult to say but, in theory, this technology is expected to succeed in the next few years. As this article showed it, an IEEE 802.16 implementation can be a secure option for subscribers that are looking for high-rates for Internet access and are not interested in using the wired infrastructure.

**References**

[1] Chang, Dean. “IEEE 802.16 Technical Backgrounder”. 24 May 2002.
URL: http://wirelessman.dyndns.org/docs/02/80216-02_12r3.pdf

[2] Skarp, Mika. “An Introduction to the World Interoperability for Microwave Access (WiMAX) Forum”. 19 June 2002.
URL: http://www.wimaxforum.org/data/whitepaper_6-19-02_withlogo.pdf

[3] Marks, Roger. “The IEEE 802.16 WirelessMAN™ MAC: It’s Done, But What Is It?”. 12 November 2001.
URL: http://www.ieee802.org/linksec/Docs/Pietilainen_1_122702.pdf

[4] Marks, Roger. “IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access”. 04 June 2002.
URL: http://grouper.ieee.org/groups/802/16/docs/02/C80216-02_05.pdf

[5] Pereira, R., Adams, R. “ESP CBC-Mode Cipher Algorithms”. RFC 2451. November 1998.
URL: http://www.ietf.org/rfc/rfc2451.txt

[6] Marks, Roger. “802.16 IEEE Standard for Local and Metropolitan Area Networks”. 8 April 2002.
URL: http://standards.ieee.org/getieee802/download/802.16-2001.pdf

[7] Gummalla, Ajay. “DOCSIS Overview”. July 2001.
URL: http://www.ieee802.org/3/efm/public/jul01/
presentations/gummalla_1_0701.pdf

[8] Marks, Roger. “Coexistence of Fixed Broadband Wireless Access Systems”. IEEE Recommended Practice for Local and Metropolitan Area Networks. 6 July 2001.
URL: http://standards.ieee.org/getieee802/download/802.16.2-2001.pdf

[9] Dornan, Andy. “Unwiring the Last Mile”. Network Magazine. 06 January 2003.
URL:
http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703464&pgno=1

[10] Dornan, Andy. “Can Wireless Networks Be Too Secure?”. Network Magazine. 04 June 2003.
URL:
http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=10300161&classroom=

[11] Stallings, Willian. “IEEE 802.16 for Broadband Wireless”. Network World Fusion. 03 September 2001.
URL: http://www.nwfusion.com/news/tech/2001/0903tech.html

[12] Abdelrezig, F., Jung, Y., Mohamed Taha, H., “Can IEEE 802.16 become backbone for Wi-Fi?”.
URL:
http://198.11.21.25/capstoneTest/Students/Papers/docs/proceeding313271.pdf

**Other Information can be found at:**

http://www.ieee802.org/16/

http://www.wirelessman.org/

http://www.wimaxforum.org/