

IEEE 802.16/WiMax Security

Hyung-Joon Kim

Dept. of Electrical and Computer Engineering
Stevens Institute of Technology, Hoboken, New Jersey

1. Introduction

IEEE 802.16, an emerging wireless technology for deploying broadband wireless metropolitan area network (WMAN), is one of, if not the most, promising wireless technology for the next-generation ubiquitous network. Not only does 802.16 provide network access anytime anywhere, but it offers a great deal of bandwidth equivalent to a typical wired network. WMAN could be highly survivable compared to cabled networks in case of natural disasters such as the hurricane in New Orleans, 2005, or the tsunami in Southeast Asia, 2004. Moreover, WMAN could be easily and efficiently deployed in underdeveloped countries, with the lack of infrastructure, as the demand for communication is presumably growing exponentially. Hence, 802.16 has the potential for an attractive alternative to the existing broadband connections. Similar to 802.11/WiFi, the family of IEEE 802.16 is commonly known to industry groups as WiMax (thus, hereinafter interchangeably called). This report reviews the fundamentals of IEEE 802.16 and security issues addressed in the paper [1] and [2].

2. The Fundamentals of 802.16

Since the original IEEE 802.16 standard was ratified in 2001, a series of amendments to IEEE 802.16 has been published and the currently active standard, IEEE 802.16e-2005, superseded IEEE 802.16c and 802.16a. Some major issues as to the original 802.16 standards addressed in [1] and [2] have been improved or at least engaged the attention of the 802.16 standards committee. In this report, unless a suffix is explicitly stated, 802.16 refers to the early standards.

Initially, the 802.16 standard was defined to deliver line-of-sight transmission in the 10 GHz to 66 GHz band by different modulation and multiple access techniques. Later, it supports non line-of-sight transmission in the 2 GHz to 11 GHz band, with 256 to 2048 carriers, using Orthogonal Frequency Division Multiplex (OFDM) and Orthogonal Frequency Division Multiple Access (OFDMA). The latest 802.16 also includes a feature for multiple-input and multiple-out (MIMO).

In essence, 802.16/WiMax operates on two layers in the air interface: the physical layer (PHY) and the Media Access Control (MAC) layer, a sub-layer as a part of the data link layer. 802.16 security is implemented as a security sub-layer (at the bottom) of the MAC layer, which also internally has service access point (SAP). At the SAP, higher level protocol data such as IP packets and ATM cells are converged into MAC service data unit (MAC SDU), which is then transformed to MAC protocol data unit (MAC PDU) while passing through the security sub-layer. The MAC PDUs are finally sent to the PHY layer that transmits them in frames by coding and modulation of RF signals.

The network entry of WiMax-enabled subscriber station (SS) requires a sequence of transactions with a base station (BS), which is roughly as follows:

1. The SS scans for downlink signals from the BS. As a downlink signal is found, the SS acquires channel parameter descriptions.
2. During initial ranging, the SS sets proper PHY parameters to communicate with the BS and establishes the primary management channel used for capability negotiation, in terms of security algorithms (authorization, authentication, and key management method to be used).
3. The BS obtains a public-key-based certificate from the SS to authenticate the SS. Upon successful authentication with the BS, the SS is now authorized to the BS and other keys for secure communication are established during authorization.
4. The SS registers by sending a request message to the BS, and the BS responds by sending a connection ID. That is, the registration establishes a secondary management connection.
5. The SS and BS finally create transport connections for data transmission.

As the 802.11 standard turned out to be a big-time failure of designing a wireless security scheme, the 802.16 standard was designed with security in mind, providing robust security protections for access control and confidentiality over the wireless link. 802.16 employs a concept of security association (SA), similar to that of IPsec, which defines security parameters – keys and encryption algorithms. First, the authorization SA, though not explicitly defined by the standard, consists of an X.509 certificate, an authorization key (AK), a key encryption key (KEK), and a hash message authentication code (HMAC) key, which will be used for authorization, authentication, and key management. Second, the data SA for transport connections consists of a SA identifier (SAID), a cipher, traffic encryption keys (TEKs), and initialization vectors for TEKs, which will be used for secure data transmission.

3. Discussions of 802.16/WiMax Security

3.1 Physical Layer Vulnerabilities and Countermeasures

802.16 security is implemented as a sub-layer at the bottom of MAC layer in order to protect data exchanged between the MAC layer and the PHY layer. In essence, it does not protect the PHY layer itself against the attacks which target the inherent vulnerability of wireless links. Thus, jamming a radio spectrum is here again one of the major threats. An attacker's transmission of sufficiently strong signals could significantly decrease the signal to noise ratio, thereby reducing the capacity of the channel enough to disrupt valid communications. Jamming could also occur unintentionally. *Scrambling* [2] is another form of jamming, but for short intervals, and disorders only targeted frames (mostly control or management messages) in order to lead the provisioning operations of the network to fail. Since 802.16/WiMax is designed to interoperate with other wireless technologies such as 802.11/WiFi and 2G/3G cellular networks, the likelihood of interference is considerably low but still present. Another typical attack against the PHY layer, so called *water torture attack* [1], pushes a SS to drain its battery or consume computing resources by sending bogus frames. This type of attack against a mobile station could be even more destructive

than a typical Denial-of-Service (DoS) attack against a wired machine because portable devices are likely to have limited resources. The paper [1] also points out that 802.16 is susceptible to a forgery attack; hypothetically, an attacker with an adequate radio transmitter can write to a wireless channel. In the *mesh* mode, 802.16 is also vulnerable to a replay attack in which an attacker maliciously resends valid frames that the attacker has intercepted in the middle of forwarding (relaying) process.

The PHY layer attacks can be prevented or mitigated by several trivial countermeasures. Increasing the power of signals can resist jamming attacks. For this, monitoring equipment can be used to detect radio jamming, and upon an abnormal state of radio spectrum the power of signals comes to increase enough to override malicious signals. According to [2], the bandwidth of signals can be increased by using spreading techniques such as frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). A sophisticate mechanism discarding bogus frames is needed to avoid running out of battery or computational resources by the water torture attack mentioned earlier. The latest 802.16 standard adds support for mobility of SS. This could make 802.16/WiMax more vulnerable to these attacks against the PHY layer because an attacker does not necessarily have to reside in a fixed point and monitoring the anomaly becomes more difficult.

3.2 MAC Layer Vulnerabilities and Countermeasures

There are several significant shortcomings of 802.16 security implemented at the MAC layer. Many serious threats arise from its authentication scheme. To ultimately set up secure transport connections, 802.16 exploits a sequential two-way transactions for controlling, authorization, and authentication. The first problem is that, during the basic and primary connection, MAC management messages are sent in plain-text and not properly authenticated. Thus, the management message can be hijacked over the air and forged by an attacker in the middle. By doing so, the attacker can prepare for further attacks. Secondly, 802.16 uses the X.509 certificate, the standard for Public Key Infrastructure (PKI), that defines a certification path validation to identify a genuine SS. It uses RSA encryption with SHA1 hashing. Typically, a SS's certificate is pre-configured by the manufacture and persistent on the machine. Thus, the certificate could be stolen and tampered by an adversary unless it is kept secret. 802.16 assumes all SSs whose certificates are validly issued by a list of manufactures can be virtually trusted. In addition, 802.16 allows BSs to have a security policy that ignores a SS with certificated by an manufacture that is not known a priori. This flawed security assumption obstructs seamless operation over 802.16. The most noteworthy flaw is in the other side of authentication – from SS toward BS. In short, the 802.16's design lacks of mutual authentication. It never offers a mean for the SS to verify the genuineness of a BS through the messages received from the BS. Thus, a rogue BS can generate and transmit any message to the SS. Mutual authentication must be present in any wireless communication since it's virtually open to anyone. Masquerading could compromise an entire network.

First, for the vulnerability of management message, message authentication code (MAC) techniques can be applied during initial ranging. For example, one-key message authentication code (OMAC) may be preferable since it provides replay protection [2]. To protect 802.16/WiMax against masquerading parties, a mutual authentication scheme is

necessary, and Extensible Authentication Protocol (EAP), a *generic* authentication protocol used in wireless networks, is most commonly proposed. Besides, to enhance general data protection, security designers suggest Advanced Encryption Standard (AES) encryption scheme. As a result, the latest 802.16 amendment employed AES in CCM mode (Counter with CBC-MAC¹) – which constructs a unique nonce during the process of CBC-MAC. According to [1], the advantage of AES-CCM is that the encryption scheme is also capable to protect authenticated but unencrypted data.

4. Other Related Issues and Future Directions

As the latest 802.16/WiMax supports mobility and roaming, like those in cellular networks, cost-efficiency is a rising issue in terms of overhead in authentication. Authentication involves expensive cryptographic operation. In general, the more complex cryptography, the more computational. This applies to not only an attacker but subscribers with resource constraints. Even worse, directly targeting a BS's authentication operations by a DoS attack can be very effective, especially by forcing the BS to digest a massive amount of handoffs. 802.16/WiMax is a fairly new technology, with the potential for a high degree of future success. Thus, competing vendors are very likely to rush to deploy the technology in the market. This may result their hasty implementations, which may fail to fulfill the complete standards and therefore fall short of the intentional security.

Naturally, a WiMax network will be interfaced with a core network, probably a converged all-IP network. Besides, many look forward to carrying other promising technologies such as VoIP, Video Conferencing, and IPTV through WiMax. It's because a large portion of WiMax subscribers (probably enterprise users rather than consumers) would be potential users for those services as well. The anticipation raises two questions: 1) Can those delay-sensitive services be well delivered without suffering from costly authentication and encryption by 802.16? 2) Can 802.16 be fully resistant to external attacks from the converged network? The answer to the first question is related to the consideration of cost-efficiency that we discussed above. The answer to the latter is that it's helpful to deploy firewalls and/or intrusion detection systems on the network perimeter. More fundamentally, it might be a good idea to examine higher level protocols against 802.16 and test security as a whole in order to protect WiMax network against outside networks.

5. Conclusion

While 802.16/WiMax is an appealing alternative to wired networks, there exist critical threats including jamming, eavesdropping and modification of management messages, masquerading as BS, and DoS attacks. Even though some issues are no longer valid since the recent amendments, some remain unsolved and need to be carefully reviewed to avoid the same mistake as 802.11/WiFi.

¹ A Cipher Block Chaining Message Authentication Code (CBC-MAC)

Reference

- [1] David Johnston and Jesse Walker, "Overview of IEEE 802.16 Security," *Security & Privacy Magazine*, vol. 2, Issue 3, IEEE Computer Society Press, pp. 40-48, 2004.
- [2] Michel Barbeau, "WiMax/802.16 Threat Analysis," *Proceedings of the 1th ACM Int. Workshop on Quality of Service & Security in Wireless and Mobile Networks*, Q2SWinet '05, ACM Press, pp. 8-15, 2005.