Review Paper on Mobile WIMAX Security Threats and Solutions

Himani Yadav
Department of Computer Science & Engineering and Information Technology B.P.S.M. University, Khanpur Kalan, Sonepat, Haryana
Email: raohimani.10@gmail.com

Abstract

Mobile WIMAX (IEEE802.16e), where WIMAX stands for Worldwide Interoperability for Microwave Access, is one of the latest technologies in the Wire-Less World. IEEE 802.16e provides the ability for users to use the Broadband Wireless Communication even when the user is moving. The main goal of WIMAX is to deliver the wireless communications with the quality of service in a secured environment. WIMAX has many salient advantages such as: high data rates, quality of service, scalability, security, and mobility. Many sophisticated authentication and encryption techniques have been embedded into WIMAX but it still exposes to various attacks in. In this Paper we have discussed about various threats related to security of IEEE 802.16e and what solutions have been proposed.

Keywords- Authentication, Authorization, Base station (BS), Encryption, Mobile station (MS), Security, Subscriber station (SS), WIMAX.

1. Introduction

WIMAX is the emerging broadband wireless technologies based on IEEE 802.16 standards [1]. Mobile WIMAX (IEEE802.16e), where WIMAX stands for Worldwide Interoperability for Microwave Access, is one of the latest technologies in the Wire-Less World. IEEE 802.16e provides the ability for users to use the Broadband Wireless Communication even when the user is moving. IEEE 802.16e standard defines the security mechanisms for mobile networks. WIMAX will also enable greater mobility, higher speed data applications, range and throughput than its counterpart, Wi-Fi. There are several advantages that can be derived from the deployment of WIMAX. Firstly, it supports higher throughput rates, higher data speed rates, and wider operating range. These make the technology very useful for deployment in bad terrain areas or in environments with limited wired infrastructure. Moreover, WIMAX supports and interfaces easily to other wired and wireless technologies such as Ethernet, ATM, VLANs, and Wi-Fi [2]. In Mobile-WIMAX, Security issues occur in both layers at Physical (PHY) as well as MAC Layer.

1.1 Threats to the PHY layer

1.1.1 In Scrambling attackers scramble the uplink slot of other MS's (Mobile station) by their own data and make it unreadable for BS (Base Station) [3] [5]. Solution-Since scrambling is intermittent, it is more difficult to detect scrambling than jamming.

Fortunately, we can use anomalies monitoring beyond the performance norm (or criteria) to detect scrambling and scramblers [10].

1.1.2 In Jamming at PHY layer acts like DOS (Denial of Service attack) that uses intentionally interfering radio communication by introducing the noise to disrupt the reception of the message in both uplink and downlink[5]. Solution- We can prevent jamming attacks by increasing the power of signals or by increasing the bandwidth of signals using spreading techniques such as a frequency spread spectrum (FSS) or direct sequence spread spectrum (DSS) [10].

1.1.3 In Water torture attack According to D. Johnson and J. Walker, this is also a typical attack in which an attacker forces a SS to drain its battery or consume computing resources by sending a series of bogus frames. This kind of attack is considered even more destructive than a typical Denial of Service (DOS) attack since the SS which is a usually portable device is likely to have limited resources [8]. Solution-To prevent this kind of attack, a sophisticated mechanism is necessary to discard bogus frames, thus avoiding running out of battery or computational resources [10].

1.2 Threats to the MAC layer

1.2.1 BS or MS Masquerading- Masquerade attack is a type of attack in which one system assumes the identity of another. The certificate can be programmed in a device by the manufacturer. Therefore sniffing and spoofing can make a masquerade attack possible [3].

1.2.2 Man in the Middle attack or Eavesdropping-This attack is also possible through rogue BS attack by sniffing Authorization-related message from SS (subscriber station) [3].

2. Protocol Architecture and WIMAX Security Architecture of IEEE 802.16e

The Protocol Architecture of IEEE 802.16e mainly contains two layers MAC and PHY as shown in Fig1. MAC layer is further divided into three layers CSL (Convergence Sublayer), MAC Common Part Sublayer and Security Sublayer or SSL. Convergence Sub layer receives the data from higher layer and forwards to CPS (Common Part Sublayer). The next sub layer is CPS, in this layer, MAC protocol data units (PDUs) are constructed, connections are established and bandwidth is managed i.e. here Bandwidth and Connection Management are defined. The Security sub layer addresses the authentication, establishment of keys and encryption. It exchanges MAC PDUs with the Physical layers. SSL defines two protocols Encapsulation and PKM Protocol. Where as physical layer is responsible for receiving and transmitting MAC frames [3].

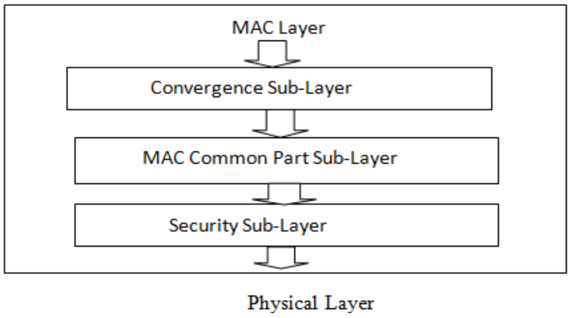


Fig1. Protocol Architecture of IEEE 802.16e [3]

3. WIMAX Standards & amendments

Version	Year	Frequency Band	Features
802.16	2001	10-66 GHz	Initial version of WiMAX based on the single-carrier physical layer and the burst TDM MAC layer . Uses LoS towers to fixed locations.
802.16a	2003	2-11 GHz	Operates with NLoS (Lower freq. band can easily penetrate barriers. Max Transmission rate is 75 Mbps.
802.16c	2003	10-66 GHz	Broadband Wireless Access (BWA). Interoperability specification.
802.16d	2004	2-11 GHz	Based on 802.16a standard with some improvements and supports both TDD and FDD transmissions.
802.16e	2005	2-6 GHz	Mobile WIMAX supports mobile stations (MS). Operates with NLoS transmission, Multicast and broadcast services. Mobility support for 65 mph with data transfer rate up to 15 Mbps and coverage area of 1-3 miles. Privacy Sub-Layer for N/W security and Power saving modes for MS.
802.16f	2005	2-11 GHz	Introduces the mesh networking and Management Information Base. Ability to bypass obstacles, which improves the coverage area.
802.16g 802.16h 802.16i 802.16j 802.16k 802.16m	2007-2011	2-11 GHz	Management Planes Procedure and Services, Mobility at higher layer. Improved Coexistence Mechanisms for License Exempt Operation [. Mobile Management Info. Base. Multi-hop Relay specifications. Advance Air Interface (WiMAX2.0). Data transfer rate of 1Gbps of fixed subscribers and 100Mbps for mobile subscribers.

Table1. WIMAX Standards [6] [7]

4. Security Issues and Security Enhancement

Security threats may occur in both the PHY and the MAC layers. The attacker attacks with Radio

Frequency (RF) channel for PHY layer threats. For MAC layer threats, the attackers spoof, modify and reply the MAC layer messages [1]. In mobile WIMAX there are some unauthenticated and unencrypted management messages which threat the reliability of the system [4].

Unencrypted management Messages- The complete management communication between the MS and BS is unencrypted. In WIMAX security architecture, there is no common key for the authentication of Broadcasted management messages [4].

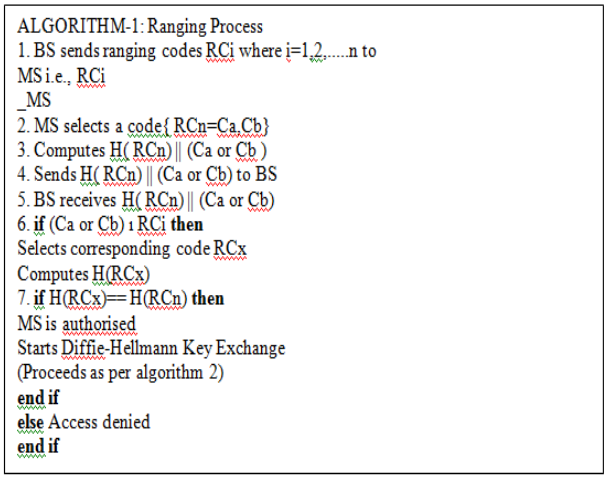
Unauthenticated messages- Mobile WIMAX includes some unauthenticated messages. Their forgery can constrict or even interrupt the communication between the mobile station and base station [4].

4.1 Security Enhancement

4.1.1 Modified Initial Network Entry Process [4]

The Initial Network Entry procedure is the first stage in establishing connection in any WiMax network. Since key exchange is done through Diffie- Hellman, possibility for Man in Middle attack makes the network weak from eavesdropping, interception and interruption of the management messages, resulting in a breach in the reliability of the entire network as it involves the transmission of unencrypted management messages. Also, there is no appropriate method to secure the critical information. Hence it results in lack of confidentiality. To overcome this, it is proposed to modify the Diffie-Hellman key exchange process by including Hash based authentication. Once the MS/SS is powered on, it starts scanning the down link channel to determine whether it is currently in the coverage of the base station (BS). Each MS stores the list of optional parameters such as DL frequency. MS synchronizes with the stored DL frequency of the suitable BS .Once the DL synchronization is completed, MS can listen to various control messages, from which it obtains the UL parameters. Based on these UL parameters, MS decides whether the channel is suitable or not. If the channel is suitable MS performs, ranging, otherwise it again starts scanning the channel. Ranging process acquires timing and power level adjustment to maintain the UL connection with the BS.

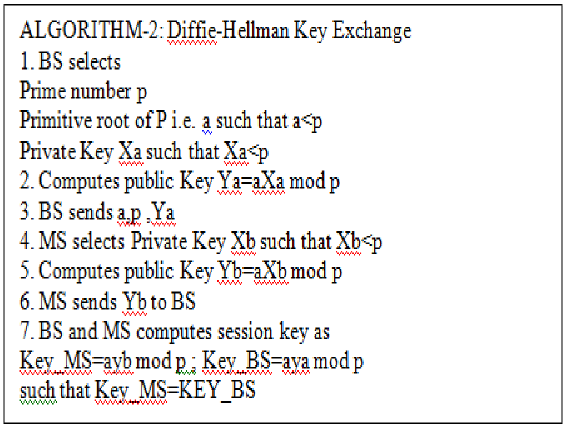
In the proposed model SS selects any one of the ranging codes say RCn where RCn=CaCb. If the ranging code contains two parts, SS selects any one part and sends the hashed value of the ranging code together with this. On reception BS compares the received ranging code part with the pool of ranging codes and identifies the corresponding complete ranging code. Then it hashes the ranging code and compares it with the received hashed ranging code. If it matches, common key will be shared through Diffie-Hellman key exchange. Else it will be declared as unauthorized use and access will be denied.



```
ALGORITHM-1: Ranging Process
1. BS sends ranging codes RCi where i=1,2,....n to
MS i.e., RCi
_MS
2. MS selects a code{ RCn=Ca,Cb}
3. Computes H( RCn) || (Ca or Cb )
4. Sends H( RCn) || (Ca or Cb) to BS
5. BS receives H( RCn) || (Ca or Cb)
6. if (Ca or Cb) ı RCi then
Selects corresponding code RCx
Computes H(RCx)
7. if H(RCx)== H(RCn) then
MS is authorised
Starts Diffie-Hellmann Key Exchange
(Proceeds as per algorithm 2)
end if
else Access denied
end if
```

Fig2a. Algorithm- Modified Initial Network Entry Process [4]

With this key exchange, shared common key called “pre-TEK” is generated which could be used for further encryption of ranging messages for secure communication. Therefore, the proposed method protects the SBC security parameters and PKM security contexts using the shared traffic encryption key (pre-TEK) during the initial network entry procedure. The algorithm for this process is illustrated in Figure.2a, 2b.



```
ALGORITHM-2: Diffie-Hellman Key Exchange
1. BS selects
Prime number p
Primitive root of P i.e. a such that a<p
Private Key Xa such that Xa<p
2. Computes public Key Ya=aXa mod p
3. BS sends a.p .Ya
4. MS selects Private Key Xb such that Xb<p
5. Computes public Key Yb=aXb mod p
6. MS sends Yb to BS
7. BS and MS computes session key as
Key_MS=ayb mod p ; Key_BS=aya mod p
such that Key_MS=KEY_BS
```

Fig.2b. Algorithm- Modified Initial Network Entry Process [4]

4.1.2 Authentication [3]-Authentication is achieved

using a public key interchange protocol that ensures not only Authentication but also the establishment of encryption Keys. 802.16e based-on Mobile WIMAX defines Privacy Key Management (PKM) protocol in security sublayer, which allows three types of authentication.

The first type is RSA (Rivest-Shami-Adleman) based authentication. RSA based authentication applies X.509 digital certificates together with RSA encryption. In this authentication mode, a BS authenticates the MS through its unique X.509 digital certificate that has been issued by the MS manufacturer.

The second type is EAP (Extensible Authentication Protocol) based authentication. In the case of EAP based authentication, the MS is authenticated either by virtue of a unique operator issued credential, such as a SIM subscriber identity module or an X.509 certificate There are three types of EAP, the first type is EAP-AKA (Authentication and Key Agreement) for SIM based authentication, the second type is EAP-TLS (Transport Layer Security) for X.509 based authentication, the third type is EAP-TTLS (Tunnelled Transport Layer Security) for SS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol).

And the third type is RSA based authentication followed by EAP authentication.

4.1.3. Data Encryption [3]- Encryption in WIMAX

Technology involves taking a stream or block of data to be protected, called plain text. Stream or block of data, called the encryption key, to perform a reversible mathematical operation to generate a cipher text. The cipher text is unintelligible and hence can be sent across the network without fear of being eavesdropped. The receiver does an operation called decryption to extract the plaintext from the cipher text, using the same or different key. When the same key is used for WIMAX Encryption and decryption, the process is called symmetric key encryption. This key is typically derived from a shared secret between the transmitter and the receiver and for strong encryption typically it should be at least 64 bytes long. When different keys are used for encryption and decryption, the process is called asymmetric key encryption. IEEE 802.16-2009 supports DES-CBC (Data Encryption Standard – Cipher Block Chaining) and three AES (Advance Encryption Standard) modes of operation for data encryption: CBC(Cipher Block Chaining), counter (CTR), and CTR with CBC message authentication code (CCM). Any of the three specified AES modes is acceptable for protecting data message confidentiality.

5. Security Requirements

The biggest security issues in WIMAX are privacy & access control to the network. The issue of privacy is resolve by encrypting the connection in between BS & SS. For the access control purpose a keying protocol is used by the base station [9].

6. Conclusion

The IEEE 802.16e based WIMAX network provides better security architecture, compared to 802.16d, and basically secures the wireless transmission using different components such as X.509 certificates, PKMv2, the Security Associations, encryption methods and the Encapsulation Protocol. However, it still lacks complete security solutions due to certain unsecured MAC management messages. In this Paper we have discussed about various threats related to security of IEEE 802.16e and what solutions have been proposed in Literature for handling these threats. One of the main threat is DOS. When discussing the security of wireless broadband network there are several possible solutions. Different authentication, access control and encryption technologies. This paper has been discussed WIMAX security issues, BS Authentication, Replay and DOS Attack. Security mechanisms For WIMAX Encryption, Security Associations, Certificate based authentication, privacy key management protocol.

REFERENCES

1. Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu, Anand Srinivasan "Analysis on Mobile WiMAX Security" Information Assurance in Security and Privacy, September 27-29, 2009 Toronto, Ontario, Canada, pg1-6.
2. Vandana V. Gawit et al, "Wireless Broadband Network, WiMax Security and Applications" International Journal of Computer Science and Mobile Computing, Vol.4 Issue.3, March-2015, pg.1-6.
3. Reena Dadhich, GeetikaNarang, D.M.Yadav "Analysis and Literature Review of IEEE802.16e (Mobile WiMax) Security" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-3, February 2012,pg1-7.
4. B.Sridevi, M.Brindha, R.Umamaheswari, Dr.S.Rajaram "Implementation of Secure & Cost Effective Authentication Processing IEEE802.16e WiMax" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012,pg1-15.
5. Rakesh Kumar Jha, Dr Upena D Dalal "A Journey on WiMax and its Security Issues" (IJCSIT) International Journal of Computer Science and Information Technologies ISSN:0975-9646Vol. 1 (4) , 2010, pg1-8.
6. Rajesh Yadav, S.Srinivasan "Evolution of WiMax Technology, Security Issues and Available Solutions" International Journal of Computer Applications(0975-8887)Volume66-No.2,March2013, pg1-5.
7. Vinod Kumar Jatav, Dr. Vrijendra Singh "Mobile WiMAX Network Security Threats and Solutions: A Survey" 2014 5th International Conference on Computer and Communication Technology 978-1-4799-6758-2/14/$31.00 ©2014 IEEE, pg.1-7.
8. Rakesh Kumar Jha "Performance Analysis of Physical Layer Security Attack on WiMax System" Intl. Jrnl. On Human Machine Interaction vol.1; Iss 1; Year2013, pg.1-12.

9. Saurabh Dubey and Sachin Kumar “Security Issues in WiMax: A Critical Review” International Journal of Information and Computation Technology. ISSN 0974-2239 volume 3, number 3(2013), pg. 1-6.
10. Trung Nguyen “A Survey of WiMax Security Threats” ,pg. 1-15.