Review of Security Threat and Solution in WiMAX (802.16e)

Aditya Kumar , Prof. P S Sharma, Prof Vivek Kumar Gupta

Abstract— IEEE 802.16 is the most eminent technology in wireless metropolitan area network (WMAN), also known as WiMAX. In this paper at first we gives the overview of WiMAX technology followed by architecture, authentication & authorization and then security threats concern with it. Since wireless communication is process through open channel network. So unauthorized objects can easily access the network and caused to be security issues/vulnerability. IEEE 802.16 e basically provides more security as compared to other wireless communication technology. The process where attack or threat is possible is the physical layer and MAC layer of IEEE 802.16e standard. So here we discussed both physical layer and MAC layer security threat and their solution.

Index Terms— WiMAX, IEEE Protocol Structure, Authentication, Authorization, Initial Network Entry, DoS.

1. INTRODUCTION

We are always in the need for higher communication speed. The need of mobility along with a high data transfer speed brings the necessary need of new technology in wireless communication. WiMAX technology is the most recent solution for the provision of fixed broadband wireless services in a wide geographical range and proved to be a real emphatic solution for the establishment of wireless metropolitan area networks (Wireless MAN). Hence WiMAX is a wireless broadband technology designed to enable pervasive, high speed mobile internet access to a very large coverage area.

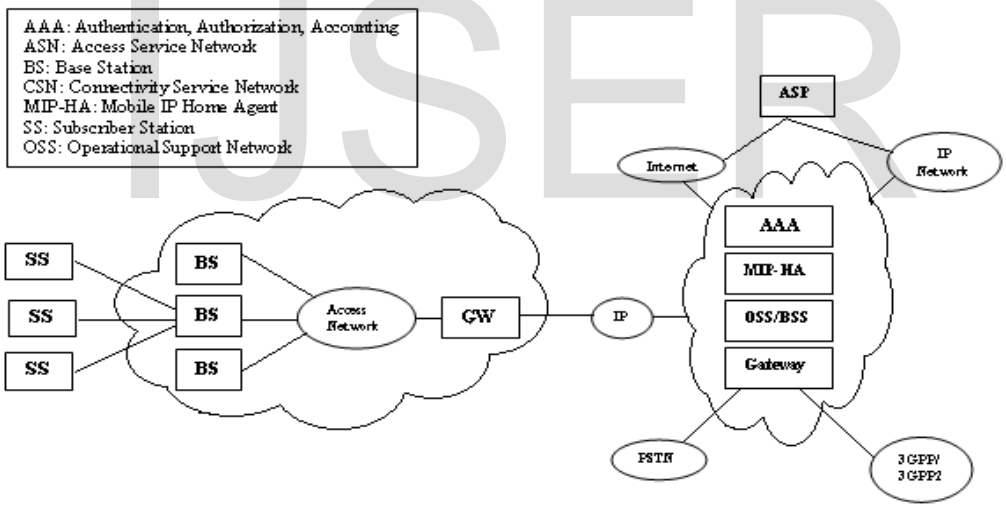

Fig.1: WiMAX Core Network

WiMAX (Worldwide Interoperability of Microwave Access), also known as the IEEE 802.16 protocol, is the latest standard for wireless networks. It was established in 1999 to organize provision for broadband wireless metropolitan area networks. The first 802.16 standard was approved in December 2001 and was followed by three amendments: 802.16a, 802.16b and 802.16c. In 2004 the 802.16-2004 standard (IEEE-SA, 2006) was released and the earlier 802.16 documents including the a/b/c amendments were withdrawn. An improvement to 802.16-2004, IEEE 802.16e-2005 (formerly known as IEEE 802.16e), addressing mobility, was accomplished in 2005. This implemented a number of enhancements to 802.16-2004, including better

- *Aditya Kumar is currently pursuing masters degree program in Digital Communication from Dehradun Institute of Technology, Dehradun, India. E-mail:* raghudev_ad@yahoo.co.in
- *Co-Author Prof P S Sharma is Assistant Professor at Dehradun Institute of Technology, Dehradun, India. E-mail: pssdeepak@yahoo.com*
- *Co-Author Vivek Kumar Gupta is Assistant Professor at Dehradun Institute of Technology, Dehradun, India. E-mail: vivek_gupta79@rediffmail.com*

support for Quality of Service, Security and the use of Scalable OFDMA, and is sometimes called "Mobile WiMAX", after the WIMAX forum. The major endeavour of IEEE 802.16 is to provide more security in the network. It provides several security features such as scalability, mobility, well-built security, access control, data confidentiality, data veracity, robust user verification and strong QoS guaranteed service. Many sophisticated authentication and encryption techniques have been set in IEEE 802.16 but it still exposes to several attacks. WiMAX basically operates on two layers: Physical layer (PHY) and MAC layer (MAC), of which security is implemented at the security sub layer of the MAC. Both the layers of WiMAX are susceptible to several attacks. The security sub layer of the IEEE 802.16d standard defines the security mechanisms for fixed and IEEE 802.16e [1] standard defines the security mechanisms for mobile network. The security sub layer supports to: (I) verify the user when the user enters in to the network, (II) Authorize the user if the user is provisioned by the network service provider and then (III) endow with the necessary encryption support for the key transfer and data traffic. The latest standards for WiMAX IEEE 802.16e already offers noteworthy enhancement over 802.16d [2].The previous IEEE 802.16d standard security design is based on PKMv1(Privacy Key Management) protocol but it has major security problems. Many issues are resolved by the later version of PKMv2 protocol in IEEE 802.16e standard which provides a flexible solution that supports device and user confirmation between a subscriber station (SS) and the home connectivity service network (CSN). Even though both of these standards concise the medium access control (MAC) and physical (PHY) layer functionality, they mainly focus on point-to multipoint (PMP) networks. In the concern of security, mesh networks are more susceptible than the PMP network. IEEE 802.16e uses superior encryption methods and has a more secure key management protocol. A new authentication method based on EAP (extensible authentication protocol) was added [3] [4]. But still many security issues remain to be solved. Security, and particularly authentication and authorization, is essential to every wireless technology, because without excellent security the technology is not advantageous at all.

2. PROTOCOL ARCHITECHTURE

The IEEE 802.16 protocol [5] is structured first of all in the Physical (PHY) and the Medium Access Control (MAC) layers. The MAC layer can be further separated into three sub layers, the first one is Service Specific Convergence Sub-layer (CS), and the second is Common Part Sub-layer (CPS) and third is the Security Sub layer. CS is the sub-layer that communicates with upper layers to obtain network data. In the process it transforms these data into MAC Service Data Units (SDUs). The format of the CS payload itself is CS depended.CPS provide mainly the core MAC functionality being answerable for function such as bandwidth allocation, connection establishment and connection maintenance. The Security Sub-layer addresses procedures such as verification, approval, key establishment, allocation and management. It is also responsible for encryption and decryption of traffic passing from the PHY to the MAC layer and vice versa. It exchanges MAC PDUs with the physical layer. Security sub layer (SSL) defines two protocols Encapsulation and PKM protocol, whereas physical layer is answerable for receiving and transmitting MAC frames. The physical layer permits great flexibility to service providers in matters of cell planning, cost, radio capabilities, services, and network capacity. It supports both Time Division Multiplexing (TDD) and Frequency Division Duplexing (FDD) configuration. The uplink (UL) channel is based on TDMA burst transmission and is divided into a number of time slots (their number may vary over time that are assigned for specific purposes such as registration, argument, and user traffic. Each burst carries MAC PDUs of changeable size. The Downlink (DL) channel makes use of Time Division Multiplexing (TDM). The multiplexed data of each SS forms a single stream that is received by all SS within the same network cell.

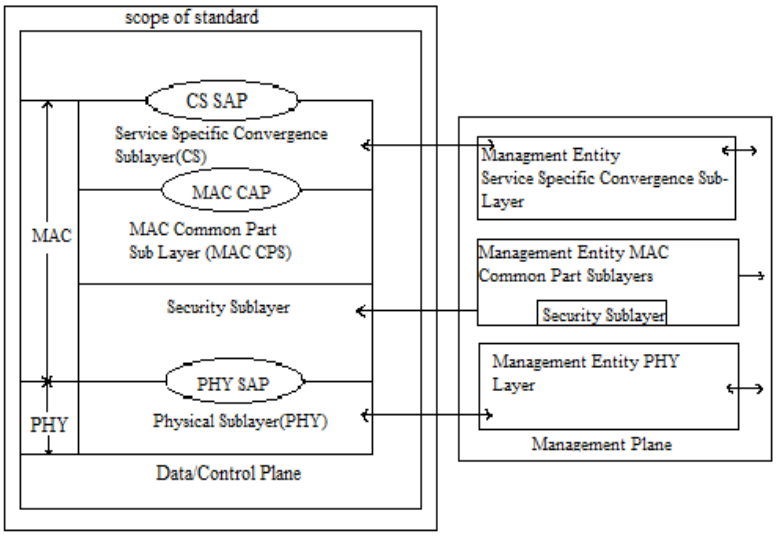

Fig 2: 802.16e Protocol Layer Architecture

When two parties establish a link, they are sheltered via a set of protocols that guarantee privacy and unique access of the authorized parties. The unique handshaking between the base station (BS) and subscriber station (SS) is done at the MAC layer through security sub layer.

3. AUTHENTICATION AND AUTHORIZATION

We will first explain the essential security facet of WiMAX considering authentication and authorization. Authentication addresses establishing the authentic identity of the device or user want to join a wireless network. Authorization addresses determining whether the authenticated user or device is allowed to join the network [3].When a subscriber station (SS) wants to connect to a WiMAX base station (BS) [6], at first a connection is established between them. The next step is the authentication of the SS, so it can enter the network. SS sends a so-called X.509 certificate [7] to BS to recognize itself. The certificate is like a signature for the SS. It contains data like a serial number, the certificates issues, the public key of the sender, its MAC address etc. After the confirmation message SS sends an approval message to BS. This message contains SSs supported authentication and data encryption algorithms. If BS determines that SS is authorized it sends a message back containing an authentication key (AK), a 4-bit sequence number and a lifetime for it containing the number of seconds before it expires [6].When all these steps have been done successfully, the SS has entered the network of BS and it can communicate with all the subscriber in its network.

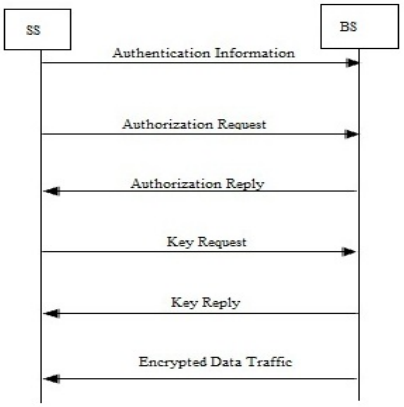

Fig 3: Authentication and Authorization

The communication between SS and BS is protected by the so called security associations (SAs). These SAs perform encryption on the data between SS and BS using a 'traffic encryption key' (TEK).

4. SECURITY ASSOCIATION

A security association (SA) is a set of security information parameters that a BS and one or more of its client SSs share in order to support safe communications. Data SA has a 16 bit SA identifier, a Cipher (DES in CBC mode) to protect the data during transmission over the channel and two traffic encryption keys (TEKs) to encrypt data: One is the current operational key and the other is TEK [8]. When the current key expires, TEK a 2 bit key identifiers is used. A 64 bit initialization vector (IV) is used for each TEK. Three types of SAs are defined [9] [10]: primary, static, and dynamic. Each convenient SS establishes a Primary Security association during the initialization process. Static SAs are provisioned within the BS. Dynamic SAs are used for transport connections when needed. Both Static and Dynamic can be shared by multiple SSs. It may use separate SAs for uplink and downlink channels [11].BS ensures that each SS has access only to its authorized SAs.

5. SECURITY THREATS AND SOLUTION

In Mobile-WiMAX (IEEE 802.16e), Security issues occurs at both Layer i.e. at physical as well as MAC Layer. Possible PHY level attacks contain jamming of a radio spectrum, causing denial of service to all stations, and flooding a station with frames to drain its battery. At present, there are no proficient techniques available to prevent PHY layer attacks. Therefore, the focus of WiMAX security is completely at the MAC level [12].The following sub-sections discusses the PHY layer security threats and MAC layer security threats along with counter measures.

5.1 Physical Layer Security issues

802.16 securities are implemented as a sub layer at the bottom of MAC layer in order to guard 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 vested vulnerability of wireless links. Scrambling and Jamming are two main threats at physical layer.

Jamming is achieved by introducing a source of noise sturdy enough to appreciably reduce the capacity of the WiMAX channel. The information and equipment required to perform jamming are not difficult to attain.

Scrambling [12] is similar to jamming but this generally instigated for short intervals of time and is targeted to particular WiMAX frames or parts of frames. WiMAX scramblers can selectively scramble control or management messages with the aim of affecting the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit.

Another typical attack against the PHY layer, so called water torture attack [11], pushes a SS to exhaust its battery or dissipate computing resources by sending bogus frames. This type of attack against a mobile station could be even more harmful than a typical Denial-of-Service (DoS) attack against a wired machine because portable devices are likely to have limited resources.

The PHY layer attacks can be prevented or detracted by several minor countermeasures. Increasing the power of signals can oppose jamming attacks. For this, monitoring equipment can be used to detect radio jamming, and upon an irregular state of radio spectrum the power of signals is increased in order to override despiteful signals. Bandwidth increases with the help of spread spectrum techniques i.e. Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS). 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 essentially have to reside in a fixed point and monitoring the irregularity becomes more difficult. Though intended scrambling is more complex than jamming, the prospect for scrambling to occur is possible due to natural noise obstruction and the availability periods of the attack. These attacks can be exposed by analyzing discrepancies in the systems performance.

5.2 MAC layer security issues

Now we look at Security threats at MAC Layer which is Connection Oriented. At MAC layer two kind of Connection occurs Management Connection and Data Transport Connection. Authors [13] mentioned that MAC Layer Security issues arise due to Un-encrypted Management Process and leads towards the following threats.

1. DoS/Reply attacks during MS Initial network entry
2. Latency during handover and unsecured pre authentication
3. Downgrade attack
4. Cryptographic algorithm computational efficiency

5. Bandwidth spoofing
6. Key space vulnerability
7. Man in middle attack or eavesdropping

Each security issue and its counter measures are discussed below:

5.1.1 DoS/Reply Attacks during MS Initial Network Entry

The initial network entry procedure is crucial since it is the first gate to establish a connection to Mobile WiMAX by performing several steps including: Initial Ranging process, SS Basic Capability (SSBC) negotiation, PKMv2 authentication and registration process. When the SS enter into the network, it scans the downlink channel and synchronizes with it. In the downlink, BS announces the range of initial ranging code for SS. The SS selects any one of the ranging code and sends it to BS for initial ranging. The BS responds to the successful reception of ranging code by Ranging Response (RNG-RSP) message. The RNG-RSP message is used to nullify the offsets of frequency, time and power used by the SS. Then the SS goes for SBCREQ and other procedures. The message flows before SA-TEK are un-encrypted nature. So the attacker can decode the MAC messages, modify and re-send it to BS or SS. The security issues during initial network entry are: (i) RNG-RSP vulnerability (ii) Auth-Request and Invalid vulnerability and (iii) Rogue BS.

In RNG-RSP vulnerability, the attacker mutates the RNG-RSP message and sets the status as failed, then re-sends it to SS. So the SS goes for initial ranging again. If the attacker again and again sets the RNG-RSP status as failed, the SS cannot access the network. This leads to the DoS attack. This RNG-RSP vulnerability is solved by Diffie-Hellman (D-H) key agreement [14] as shown in figure.

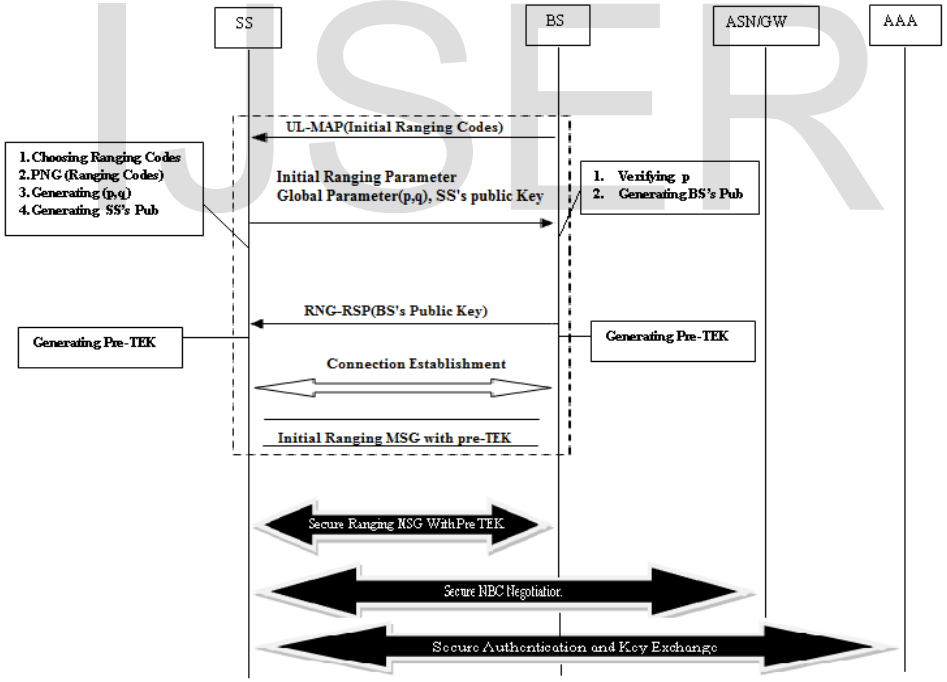

Fig 4: Initial Network Entry Approach [13]

The Diffie-Hellman key agreement scheme will be used for SS and BS to generate a shared common key called "pre-TEK" separately and set up secret communication channels in the initial ranging procedure. After that, the SBC security parameters and PKM security contexts can be exchanged securely.

For Auth-Request and Invalid vulnerability, the attacker captures the Auth-Request message and re-sends it to BS continuously. So the BS would be confused with the continuous request and sets the Auth-Response as failure. Some time the attacker may captures Auth-Response message from BS and re-sends to SS after time out period.

Solution: This issue can be solved by either introducing nonce [11] or time stamps [15]. By adding nonce or time stamp, SS and BS identifies if the authorization message is correct. So the attacker cannot change the messages. When comparing nonce and time stamp, time stamp is more secure and avoids the replay attack. If the attacker captures the authorization response message and resends it after the time of expiry, the SS can identify with the time stamp value.

Rogue BS or Masquerading: Rogue BS or 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. There are two techniques to perform this attack: identity theft and rogue BS attack. In rogue BS attack, the SS cannot verify that any authorization protocol messages it receives were generated by an authorized BS. So any rogue BS can create a response. To solve this issue, the SS has to authenticate the BS [11]. The PKMv2 in Standard 802.16e solves it by mutual authentication. To avoid this problem is ECDH (Elliptic Curve Diffie-Hellman) Algorithm used [11].

5.2.2 Latency During Handover and Unsecured Pre-Authentication

When handover occurs, the MS is re-authenticated and authorized by the target BS. The re-authentication and key exchange procedure increase the handover time, which affects the delay sensitive applications. In handover response message, BS informs the SS whether SS needs to do re-authentication with the target BS or not. If the SS is pre-authenticated by target BS before handover, then there is no need of device re-authentication but user authorization is still necessary. The authors [16] proposed two schemes to avoid the device re-authentication. The first scheme adopts the standard EAP but instead of standard EAP method used in handover authentication, a proficient shared key-based EAP method is used using EMSK. Let MSK_I and $EMSK_I$ be the master and extended master session keys in the I^{TH} authentication phase, then MS and AAA will generate the MSK_{I+1} and $EMSK_{I+1}$ from the existing MSK_I and $EMSK_I$ keys before handover takes place. So the device authentication and key (MSK, EMSK) exchange is avoided. The second method skips the standard EAP method and the device authentication is done by SA-TEK three-way handshake in PKMv2 process. Since this method avoids the standard procedures, it is not appropriate for implementation. The handover latency can be mitigating by simple pre-authentication schemes [17]. But pre-authentication techniques are ineffective and unprotected [16].Except that there are two more techniques for reducing handover latency i.e.; PKI infrastructure and Mobile IP scheme. In PKI infrastructure [18] for mutual validation between target ASN and the SS before handover. Since the messages are encrypted using the public key, security is guaranteed. Mobile IP (MIP) scheme [19] is the new approach to solve the above issue. In this scheme, pre-negotiation with the target BS is in layer 3 MIP tunneling protocol.

Solution: For the above issue, MIP scheme [19] is more efficient than the other methods, since the messages are more secured by tunneling protocol and it further reduces the latency during IP connectivity phase. If the SS doesn't have the MIP support, shared key-based EAP is efficient.

5.2.3 Downgrade Attack [20]

The first message of the authorization process is an unsecured message from SS telling BS what security capabilities it has. An attacker could send a spoofed message to BS containing weaker capabilities in order to convince the BS and the attack SS to agree on an insecure encryption algorithm. The standard does not specify a concrete solution for the situation that two valid answer received by BS.

Solution: A possible solution for downgrade attack is that the BS could ignore message with security capabilities under a certain limit [20].

5.2.4 Cryptographic Algorithm Computational Efficiency

The number of bits needed for encryption in RSA is more than Elliptic Curve Cryptography (ECC) for a required encryption which increases the computation time.

Solution: ECC is the good substitute for RSA-based public key cryptography [21] [22]. ECC can achieve the same level of security as RSA with smaller key sizes. 160-bit ECC provides comparable security to 1024-bit RSA and 224-bit ECC provides comparable security to 2048-bit RSA. Another advantage of ECC is that it offers faster computational efficiency and well as memory, energy and bandwidth savings.

5.2.5 Bandwidth Spoofing

In bandwidth spoofing the attacker grabs the available bandwidth by sending the un-necessary bandwidth request message to BS [23].

Solution: To unravel the bandwidth spoofing, we recommend that the radio resource management in the BS

should check the local policy function (LPF) and then allocates the bandwidth only if the SS has essentially provisioned. This new recommendation is based on QoS model suggested by the WiMAX forum [24].

5.2.6 Key Space Vulnerability

In 802.16e a 4-bit sequence and 2-bit sequence number is issued to discriminate between successive generations of AKs. Also, a 2-bit key sequence number is used for the same reason with TEKs. The size of the key is inadequate to protect the keying material from attacks [25].

Solutions: No solutions were found in literature, which is strange, because the problem can easily be solved by increasing the number of bits for both keys. They could be for example both 8 bits. This would mean a few more bits to send, but not enough to reduce the performance drastically. The major disadvantages are however, that the used encryption and decryption mechanisms will have to be modified. This will perhaps increase the Complexity and will require a standardization action.

5.2.7 Man in Middle Attack or Eavesdropping

Most of the management messages defined in IEEE 802.16e are integrity protected. This is done by a hash based message authentication code (HMAC), or alternatively by a cipher based message authentication code (CMAC) [16]. However, some messages are not covered by any authentication mechanism. This introduces the man-in-middle vulnerability. Eavesdropping of management messages is a critical security issue for users and a major threat to a system. Eavesdropping mostly affects the transfer of information and rarely causes system outage.

Solution: Solution is to have EAP (Extensible Authentication Protocol) which can handle this because it provides legacy password based authentication protocol.

6. CONCLUSION

In this paper we have studied security vulnerability & threat and their solution. IEEE 802.16e provide better security as compared to 802.16d in user authentication, access control, data privacy and data integrity using sophisticated authentication and encryption technology. Here we discussed D-H Key arrangement method for initial network entry threat.MIP scheme is best suited among the shared key based EAP scheme and PKI infrastructure for latency and pre authentication attacks. For cryptography computational threat ECC is better than RSA based public key cryptography. For downgrade threat we do not have solution which gives best performance results. Our paper gives the survey about security issues and their solution. Even though some security issues do not have the most suitable solution. So we need to further research to improve the security performance of IEEE 802.16e WiMAX.

REFERENCES

[1]. IEEE 802.16-2005, "IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed and Mobile broadband wireless system," IEEE press, 2005

[2]. IEEE, "IEEE Std. 802.16-2004, IEEE standard for WiMAX 802.16-2004, Oct. 2004.

[3]. Ram Dantu et al., "EAP Methods for Wireless Networks," Computer Standards & Interfaces-29, pp: 289-301 (2007).

[4]. Jeff Mandin, "Enhancement of 802.16e to Support EAP-Based Authentication, Suggestion for Improvement of 802.16e security," On Behalf of Security Ad Hoc group.

[5]. C Kolias at al. "Attack and Countermeasures on 802.16: Analysis and assessment".

[6]. Arkoudi-vafer Aikaterini, "Security of IEEE 802.16 Royal Institute of Technology," 2006.

[7]. Housley, et al., "RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," The Internet Society, April 2002.

[8]. J. Hasan, "Security Issues of IEEE 802.16 (WiMAX)," School of computer and Information Science, Edith Cowan University, Australia, 2006.

[9]. IEEE Std. 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems," October 2004.

[10]. S. Adibi et al., "End-to-End (E2E) Security Approach in WiMAX: Security Technical Overview for Corporate Multimedia Applications," Handbook of Research on Wireless Security (2 Volumes), pp: 747-758,, 2008.

[11]. D. Johnston and J. Walker, "Overview of IEEE 802.16 Security, IEEE Security & Privacy," Magazine May/June 2004.

[12]. M. Barbeau, "WiMAX/802.16 Threat Analysis," Proceedings of the ACM Int. Workshop on Quality of Service & Security in Wireless and Mobile Networks, Q2SWinet 2005, ACM Press, and pp: 8-15, 2005.

[13]. Gaurav Soni et al., "Analysis of Security Issues of Mobile WiMAX 802.16e And Their Solutions," International journal of Computing and Corporate Research. ISSN 2245 054X, Volume 1 issue 3 manuscripts 3 November 2011.

[14]. T.Shon and W.Choi, "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", 2007, pp: 88–97.

[15]. S.Xu, et al., "Security Issues in Privacy and Key Management Protocols of IEEE 802.16," Proc. of ACM 44th Annual Southeast Regional Conf., 2006, pp: 113–118.

[16]. H-M. Sun et al., "Efficient Authentication Schemes for Handover in Mobile WiMAX," Proc. of 8th Int'l Conf. on Syst. Design and Applications, 2008, pp: 44–49.

[17]. J. Hur et al., "Security Considerations for Handover Schemes in Mobile WiMAX Networks," Proc. of Int'l Conf. on Wireless Comm. and Networking, 2008, pp: 2531–2536.

[18]. H-M. Sun et al., "Secure and Fast Handover Scheme Based on Pre- Authentication Method for 802.16-WiMAX," Proc. of IEEE Region of 10 Conf., 2007, pp: 1–4.

[19]. C-K.Chang and C-T.Huang, "Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks," Proc. of Int'l Conf. on Parallel Processing, 2007, pp: 46–46.

[20]. Bart Sikkens, "Security Issues and Proposed Solutions Concerning", 8th Twente Student Conf. on IT, 2008.

[21]. Y.Zhou and Y.Fang, "Security of IEEE 802.16 in Mesh Mode", Proc. Of IEEE Military Comm. Conf., 2006, pp: 1–6.

[22]. F.Liu and L.Lu, "A WPKI-based Security Mechanism for IEEE 802.16e, IEEE Communications Society," Proc. of Int'l Conference on Wireless Comm., Networking and Mobile Computing, 2006, pp: 1–4.

[23]. L.Maccari et al., "Security Analysis of IEEE 802.16, Communications," Proc. of Int'l Conf. on Comm., 2007, pp: 1160–1165.

[24]. WiMAX Forum, "WiMAX End-to-End Network Systems Architecture," (Stage 3: Detailed Protocols and Procedures) Release 1, V.1.3.0, 2008.

[25]. Fuqiang Liu, Lei Lu, "A WPKI-based Security Mechanism for IEEE 802.16e," IEEE Communications Society, Wuhan University, China 2006.