Analysis and Literature Review of IEEE 802.16e (Mobile WiMAX) Security

Reena Dadhich, GeetikaNarang, D.M.Yadav

***Abstract**-IEEE802.16e or Mobile WiMAX, where WiMAX stands on Worldwide Interoperability for Microwave Access, is one of the latest technologies in the Wire-Less World. The main goal of WiMAX is to deliver wireless communications with quality of service in a secured environment. IEEE 802.16e provides the ability for users to use the Broadband Wireless Communication even when the user is moving. Its Mobility feature makes it differ from the previous protocol IEEE 802.16d which was based on Static WiMAX and providedthe Wireless communication at fixed locations.This paper is related to the security issues for IEEE802.16e. Various Threats which occurs at Physical and MAC(Medium Access Control) layer in Mobile WiMAX,what solutions have been proposed in literature related to these threat and what are the shortcomings of these proposed solution. And also at last in proposed work we have proposed solution for one of the main threat called as DoS(Denial of Service)*

Keywords: MIMO, Threats, Protocol Architecture, Security Frame Work.

I. INTRODUCTION TO IEEE 802.16e

IEEEStd 802.16e published on February 28th 2006, provides enhancements to the last version 802.16d which was stationary WiMAX and 802.16e is Mobile WiMAX [5] also called as Mobile WiMAX.It supports subscriber stations moving at vehicular speeds and thereby specifies a system for combined fixed and mobile broadband wireless access. Mobile-WiMAX 802.16e follows Non line of site; its licensed bands are 2.5 GHz (US) and 3.5 GHz licensed bands. Its Channel bandwidth varies from 1.25 to 20 MHz It uses QPSK (Quadrature Phase Shift Key), 16QAM (Quadrature Amplitude Modulation) and 64 QAM
Modulation OFDMA access (Orthogonal Frequency Division Multiple Access), TDD (Time Division Duplexing) for asymmetric traffic and flexible BW allocation. Advanced Antenna Systems (AAS): Beam forming, spatial diversity, spatial multiplexing using MIMO (2x2) (Multiple Input and Multiple Output).

Manuscript published on 28 February 2012.
* Correspondence Author (s)

Dr.Reena Dadhich*, Head Department of MCA., Government Engineering College, Ajmer, Rajasthan, India, Mobile No 992855895,(e-mail id:reena.dadhich@gmail.)

Ms. Geetika Narang, Asst.Prof in Computer Engineering Department,Sinhgad Institute of Technology, Lonavala,India, Mobile No 9689896065, (e-mail id : geetika.narang@gmail.com)

Dr. D. M.Yadav, Principal of JSPM’S Bhivarabai Sawant Institute of Technology, Pune, India, Contact No:9011063944 (e-mail id:dineshyadav_8@yahoo.com)

A. Introduction to MIMO

MIMO stands on Multiple Input and Multiple Output. It is an antenna technology that is used in both transmission and receiver equipment for wireless radio communication. MIMO exploits the space dimension to improve wireless systems capacity, range and reliability.Wireless signals transmitted via single antennas are distorted byhills, buildings, valleys and other landscape features. These alternative signal paths separated in time, multipath, result in distortions such as fading, picketing or cliff effects, but on the other hand MIMO takes the advantage of this Multipath, as per MIMO Multipathis not an enemy but ally [3].

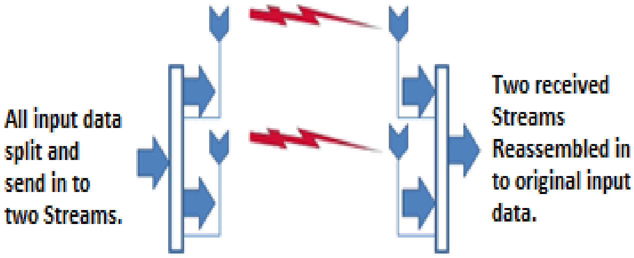
All input data split and send in to two Streams.
Two received Streams Reassembled in to original input data.

Fig1. Multipath in 2 X 2 MIMO

B. How MIMO Works

In MIMO Mathematical algorithms are used to spread the user data across the multiple transmitters. The transmitted signals are three dimensional and described in terms of time, frequency and space. The spatial multiplexing is a common transmission technique in MIMO totransmit independent and separately encoded data signals from each of the multiple transmits antennas. Therefore, the space dimension is reused, or multiplexed, more than one time. At the receiver, a special channel calibration signal at the beginning of the packet allows the different signals to be identified during the recombination process. The technique of separating out different paths in the radio link is what allows the MIMO radio to transmit multiple signals at the same time (as shown in Figure 2)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

on the same frequency, and thereby improve the use of the spectrum many "virtual wires" over which to transmit signals.

Fig 2.In MIMO Each Virtual multipath route is treated as a separate channel

II. PROTOCOL ARCHITECTURE OF IEEE 802.16e

Ifwe consider the Protocol Architecture of IEEE 802.16e then it mainly contains two layers MAC and PHY as shown in Fig3. MAC layer is further divided in to three layersCSL (Convergence Sub layer), MAC Common Part Sub layer and Security Sub layer or SSL.

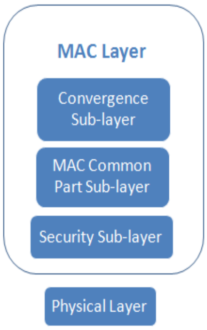

Fig3. Protocol Architecture of IEEE 802.16e

ConvergenceSub layer [1] receives the data from higher layer and forwardsto CPS (Common Part Sublayer) [12]. The Convergence layer also sorts the incoming MACSDUs (Service Data Unit)by the connections to which they belong.Next Sub layer of MAC layer is CPS layer. 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. CSL is tightly integratedwith the Security sub layer.Last Layer of MAC Layer isSSL (Security Sub Layer).The Security sub layer addresses theauthentication, establishment ofkeys and encryption. It exchanges MAC PDUs with the Physical layers. SSL defines two protocols Encapsulation and PKM Protocol. Whereas physical layer is responsible for receiving and transmitting MAC frames.

III. SECURITYTHREATSIN IEEE 802.16e

In Mobile-WiMax(IEEE 802.16e), Security issues occurs at both Layer i.e. at physical as well as MAC Layer.

A. At Physical Layer

Scrambling and Jamming are two threats.

- InScrambling [11]attackersscramble the uplink slot of other MS's (Mobile station) by their own data and make it unreadable for BS (Base Station).
- Whereas Jamming[11] at PHY layer acts like DoS(Denial of Service attack) thatusesintentionally interfering radio communication by introducing the noise to disrupt the reception of message in both uplink and downlink.

B. At MAC Layer

Now, if 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 [12] mentioned that MAC Layer Security issues arise due to Un-encrypted Management Process and leads towards the following threats.

- *RNG-RSP vulnerability/DoS attack.*

DoS is one of that threats which occurs at the time of Initial Network entry. It occurs because of RNG –REQ (Ranging Request) and RNG- RSP (Ranging-Response) messages which are used in the initial ranging process.RNG-REQ message is used by the MS for requesting the BS to join the network and RNG-RSP message is used by the BS in response to the RNG-REQ message to the MS containing basic and primary CID(Connection Identifier). These ranging messages are not encrypted and hence the attacker can access it and modify it accordingly.In RNG-RSP vulnerability, the attacker can modify this message and set the status as failed. The attacker can resends this message to the MS, which indicates the MS that it has to go for initial ranging again. An attacker may intercept the RNG-RSP message again and again with the status providing as failed [14]. Hence, the MS cannot join the network and leads to the DoS attack.

The solution to this problem is to use DiffieHellmanKey exchange algorithm has been mentioned by Authors [13] [14].

- *Authorization Request and Invalidvulnerability*

In Authorization-Request and Invalid vulnerability the attacker intercept Auth-Request message and resends itto the BS continuously. As the BS gets Auth-Request message continuously, it would be confused and sets the Auth-Response message as failed. In some cases, an attacker may intercept the Auth-Response message and resend it to the MS after time out period [13].

The solution to this problem is to use the time-stamps [15]. By adding the time-stamps to the authorization messages, MS and BS can verify that whether the authorization message is proper. Hence the attacker also cannot modify the message.Use of time stamps avoids the replay attack.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- *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 spoofingcan make a masquerade attack possible.

Specifically, there are two techniques to perform this attack: *identity theft and rogue BS attack*. By The rogue attack BS makes the MSs believing that they are connected to the legitimate BS, thus it canintercept MS's whole information by the *Id entity theft* an attacker reprograms a device with the hardware address of another device. The address can be stolen by interfering the management messages.

Solution to avoid this problem is ECDH (Elliptic Curve Diffie-Helllman) Algorithm [15]

- *Man in the Middle attack or eavesdropping*

This attack is also possible through rogue BS attack by sniffing Authorization-related message from SS.

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

IV. SECURITY PROCESSFOR IEEE 802.16e

At higher level view WiMax Security Process is divided in to following three steps as shown in the Figure below too.

i. Authentication
ii. Key Establishment
iii. Data Encryption

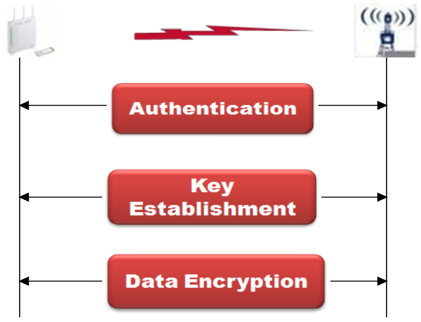

Fig4. Security Framework for IEEE802.16e

A. *Authentication*

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 sub-layer, which allows three types of authentication [13].

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 AuthenticationProtocol) based authentication. In the caseof EAP based authentication, the MS is authenticated either by virtue of a unique operator issued credential, such as a SIM subscriber identity moduleor 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.

B. *Data Key Exchange*

Once authentication is complete, the BS and MS share an activated AK (Authentication key) which can be called as Key Establishment or Data Key Exchange. This step is considered as Initial Network Entry Procedure and the initial network entry procedure mainly consists of four processes [15]:

- Initial Ranging process.
- MS basic capability negotiation -process.
- PKM authentication process.
- Registration process.

Following Flow Chart shows a detail picture of Initial Network Entry Procedure.

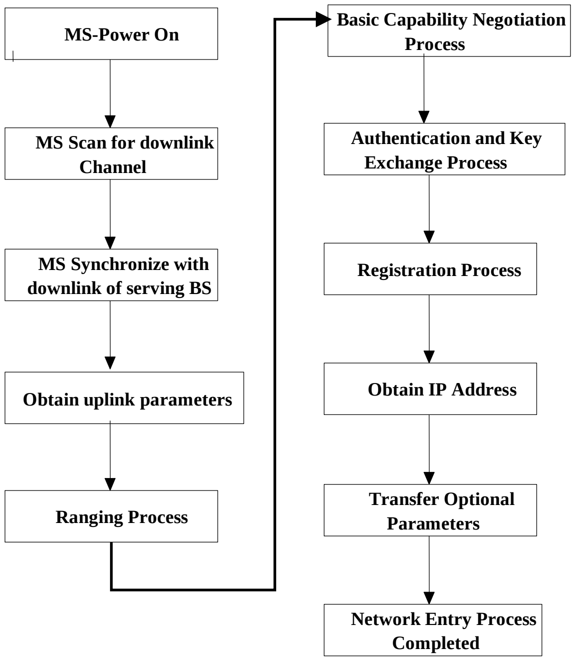
MS-Power On
MS Scan for downlink Channel
MS Synchronize with downlink of serving BS
Obtain uplink parameters
Ranging Process
Basic Capability Negotiation Process
Authentication and Key Exchange Process
Registration Process
Obtain IP Address
Transfer Optional Parameters
Network Entry Process Completed

Fig. 5 Initial Network Entry Procedure [15]

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Step 1: When MS is powered on, it firsts scans the downlink channel to determine whether it is currently in the coverage of base station.

Step 2: Each MS stores the list of optional parameters, such as DL(Downlink) frequency. So in next step MS synchronizes with the stored DL frequency of most suitable BS [7].

Step 3: Once the DL synchronization is completed, MS can listen to the various control messages from which itobtains the UL(Uplink) parameters. Based on these UL parameters, MS decides whether the channel is suitable or not.

Step 4: If the channel is suitable MS performs next step, otherwise it goes back to the scanning step that is step 1.

Step 5: Next step is to perform ranging process. Ranging is the process to acquire timing and power leveladjustment to maintain the UL connection with the BS. To perform initial ranging, MS send a RNG-REQmessage to the BS with the CID parameter [2].

Step 6: In response to this message, BS sends the RNG-RSP message to the MS with the basic and primaryCID.

Step 7: After initial ranging, next step is to perform basic capability negotiation process. Here MS firsts sendsthe SBC-REQ (Subscriber Basic Capability-Request)message to the BS through which MS informs the BS about its basic capabilities in terms of PHY Parameters and Bandwidth Allocation.

Step 8: When BS receives this message, it responds with the SBC-RSP message consisting of the parameters are required for the UL and DL transmission.

Step 9: After negotiating the basic capabilities, authentication and key exchange process will be performed.

Step 10: Once the key exchange process is completed, MS registers itself with the BS, for which it sends theREG-REQ message to the BS.

Step 11: In response to this message, BS sends the REG-RSP message to the MS. When MS receives thismessage, it can obtain the IP address.

Step 12: Finally the service flow will be established, which is either initiated by the MS or BS.

C. Data Encryption

Encryption in WiMAX Technology involves taking a stream or block of data to be protected, called plain text, and using another.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. Both symmetric and asymmetric key encryptions are typically used each serving different needs.

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 acceptablefor protecting data message confidentiality. [17]. But as per the study of various papers like [18], [19].Advanced Encryption Standard (AES) which is the data encryption standard adopted by the National Institute of Standards as part of Federal Information Processing Standard (FIPS) and is specified as a link-layer encryption method to be used in WiMAX Technology. Advanced Encryption Standard (AES) is based on the Rijndael algorithm, which is a block ciphering method believed to have strong cryptographic properties. Besides offering strong encryption, Advanced Encryption Standard (AES) is fast, easy to implement in hardware or software, and requires less memory than do other comparable encryption schemes. The computational efficiency of Advanced Encryption Standard (AES) has been a key reason for its rapid widespread adoption. The Advanced Encryption Standard (AES) algorithm operates on a 128-bit block size of data, organized in a 4 x 4 array of bytes called a state. The encryption key sizes could be 128, 192, or 256 bits long; WiMAX Technology specifies the use of 128-bitkeys.

V. LITERATURE REVIEW

After discussing about the IEEE 802.16e Introduction, its Security Threats and Security Process. In this section we are briefing about Literature Survey on the various Solutions proposed by Researchers / Authors, and which problems still exist in Mobile WiMAX.

In Paper [7], 2007 Authors have analysed security issues in the family of IEEE 802.16 standard that has not been addressed so far.

Problems discussed: They have mentioned about Lack of message integrity code (MIC) for data packets and authentication packets. Lackof authentication at the base station(BS)'s side.

Proposed Solution: Authors have only suggested some changes, such as the introduction of EAP (Extensible authentication protocol) protocol to harden the authentication phase.

Limitations: Here Authors have not proposed any solution only they have discussed about the problems.

In Paper[2] 2008, Authors have mentioned that although IEEE 802.16e has a very robust and promising security Architecture; there are still some creases which need to be ironed out.
Problem discussed: They have more discussed about two problems DoS(Denial of Service), Key Space Vulnerability and Downgrade Attack.
Proposed Solution: For DoS attack Authors have proposed Timestamp approach along with Signature of BS and SS for Authentication. For Key Space Vulnerability they have suggested to use more number of bits for Acknowledgment.To overcome the problem of Downgrade Attack, Authors have argued to ignore the messages which are having security capabilities under a limit.
Limitations: Addition of Timestamp and Signature requires modification in Standard.
Increased number of bits for Acknowledgment requires changes in encryption and decryption.
And proposed solution for downgrade attack will ultimately leads towards DoS attack.

In Paper[5]2009, Authors have design a novel and efficient rekeying scheme for WiMAX networks. They have mentioned DoS attacks on the BS could happen during the PKMv2.
Problem discussed: Authors have argued that Multicast and Broadcast Rekeying Algorithm (MBRA) don’t scale well.
Proposed Solution: Authors have suggest Tree Base Rekeying Scheme for handling DoS attack.
Limitation: Tree Base Rekeying Scheme leads towards storage overhead.

In Paper[9]2010, Here also Authors specifically focused on the Multicast and Broadcast Rekeying Algorithm (MBRA) of 802.16e.
Problem discussed: They have argued that although this algorithm has been designed with efficiency and power saving in mind, but it has several security problems.
Proposed Solution: Authors have suggested use of multiple decryption key in asymmetric group key management protocol.
Limitation: Handling of multiple key at decryption is another big issue.
Problem discussed: Authors have discussed
Attacks on Physical Layer Jamming and scrambling, at MAC layer DDoS attack (Distributed Denial of service), Traffic Encryption Key (TEK) and Authorization Key(AK) issues.
Proposed Solution: Author advised Intrusion Detection System, but the paper was just a review, Issues related to WiMAX and Converged network are mentioned and suggestions are given that a lot of security concerns should be provided

In Paper [8] 2010, Authors have discussed about the security issues for WiMAX and Converged Network. They have focused on the threats to both the technologies and security measures for these threats.

In Paper [1] 2011, Authors have described the security mechanisms present in the WiMAX. Description of different security issues in PKM (Privacy and Key Management protocol) and the various solutions proposed in literature.
And at last conclude that lots of research work is still required for the security of IEEE 802.16e
Problem discussed: Key Space Vulnerability and Downgrade Attack, also argued about efficiency of Cryptographic Algorithm-RSA (Rivest Shamir Adleman)
Proposed Solution:Authors have mentioned already existing solution like use of 8 bit sequence number instead of 4 bit for Key Space Vulnerability.BS could ignore messages with security capabilities under a certain limit for Downgrade attack and instead of RSA here Authors have prefer the use of ECC(Elliptic Curve Cryptography.
Limitations: Still unable to implement 8 bit sequence number. Proposed Solution of Downgrade attack leads towards DoS (Denial of Service) for SS (Subscriber Station) and use of ECC requires modification in Standard.

As per the literate review we found the major limitations as,

- Adding the timestamps and Signatures require a reasonable modification to the standard.
- For Key space Vulnerabilityusing more number of bits for acknowledgment requires modification on the used encryption and decryption mechanism.
- Tree base Rekeying for avoiding the Denial of Service attack Scheme leads toward Storage Overhead.
- Ignoring the messages as a Solution can leads towards DoS.
- For Malicious Insiders attack use of multiple keys leads towards the problem of handling the multiple keys at decryption.

VI. CONCLUSION and PROPOSED WORK

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 threat. One of the main threat is DoS for which various Solution have been provided for e.g. Timestamp, Tree Base Rekeying but that also leads towards Storage Overhead. It has also been analysed that some of the problems are correlated to each other for e.g. ignoring the message can be a solution for handling Downgrade Attack but it leads towards the DoS attack. In Literature currently there is no solution which can solve both of these problems. In our proposed work we will implement the solution for this attack, we argue that if we will use puzzle approach along with Time Stamp and Nonce variable then up to a great extent we can solve this problem. Here BS will send a Puzzle to MS, Puzzle will be configuring in that way so that if the MS is intruder then it will not be able to solve the puzzle. If the MS is able to solve the puzzle then it will send the solution to BS, BS will evaluate the Puzzle solution and then will go for MS Digital Signature Verification. After this key exchange will occur and transmission will take place.

REFERENCES

[1] FudenTshering and Anjali Sardana Dept.of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, “ **A Review of Privacy and Key Management Protocol in IEEE 802.16e**”, International Journal of Computer Applications (0975 – 8887) Volume 20– No.2, April 2011.

[2] Bart Sikkens,Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, the Netherlands ,sikkensb@cs.utwente.nl **,” Security issues and (IEEE 802.16e)**” proposed solutions concerning authentication and authorization for WiMAX8thTwente Student Conference on IT, Enschede, January 25 , 2008 Copyright 2008, University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science.

[3] Dr. Jacob Sharony,Director, Network Technologies Division. Centre of Excellence in Wireless & IT Stony Brook University,” **Introduction to Wireless MIMO – Theory and Applications**” IEEE LI, November 15, 2006.

[4] Fuqiang Liu, Lei Lu ,School of Electronics and Information Engineering,TongjiUniversity,Shanghai,P.R. China,fuqiangliu@163.com,leilu.cn@gmail.com,”**A WPKI-based Security Mechanism for IEEE 802.16e** “IEEE Communications Society, Wuhan University, China”.

[5] Jeremy Brown,Department of Computer Science,North Dakota State University Fargo, ND 58108,Xiaojiang Du Department of Computer and Information Sciences Temple University Philadelphia, PA 19122, USA Email: dux@temple.edu”**Towards Efficient and Secure Rekeying for IEEE 802.16e WiMAX Networks**”publish in the IEEE "GLOBECOM" 2009 proceedings.

[6] AyeshaAltaf,College of Signals, NUST,ayeshaaltaf@mcs.edu.pk,M.YounusJavedCollege 0f E&ME, NUST,myjaved@ceme.edu.pk,AttiqAhmed,College of Signals, NUSTattiq-mcs@nust.edu.pk” **Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005”.**

[7] Leonardo Maccari, Matteo Paoli, Romano Fantacci,Department of Electronics and Telecommunications - University of Florence Telecommunication Network Lab tel. : +390554796467 - fax : +390554796485 Florence, Italy Email:{maccari,paoli,fantacci}@lart.det.unifi.it” **Security analysis of IEEE 802.16** ”.

[8] MasoodHabib, Masood Ahmad,Department of Computer Science & IT ShaheedZulfikar Ali Bhutto Institute of Science and Technology Islamabad, Pakistan masoodshalmani@gmail.com Department of Computer Science,National University of Computer & Emerging Sciences Peshawar, Pakistan,masood.ahmadpk@yahoo.com**”. A Review of Some Security Aspects of WiMAX& Converged Network”.**

[9] Georgios Kambourakis, lisavet Konstantinou, Stefanos Gritzalis, Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean,83200 Karlovassi, Samos, Greece-2010, _journal homepage: www.elsevier.com/locate/camwa**” Revisiting WiMAX MBS security** ”.

[10] Wen-an ZHOU1, Bing XIE1, Jun-de SONG1'School ofElectronic Engineering, Beijing University ofPosts and Telecommunications, Beijing, P R. China” **Link-level Simulation and Performance Estimation of WiMAX IEEE802.16e“**.

[11] Frank, AIbikunle, **Security Issues in Mobile WiMAX (IEEE 802.16e**), 2009 IEEE MobileWiMAX Symposium.

[12] GauravSoni, Assistant Professor, Department of Electronics and Communication Engineering, SandeepKaushal Amritsar College of Engineering ,India, SandeepKaushal “**Analysis of security issues of mobile WiMAX 802.16e and their solutions”** volume 1 issue 3 manuscript 3 November 2011. International journal of Computing and Corporate Research.ISSN 2245 054X.

[13] Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, Yuan'an Liu Key Lab. OfUniversal Wireless Communications, Ministry of Education (Beijing University of Posts and Telecommunications)” **Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions”**1-4244-2575-4/08/$20.00 © 2008 IEEE.

[14] A.K.M. NazmusSakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, **“IEEE 802.16e Security Vulnerability: Analysis and Solution**”, Global Journal of Computer Science and Technology Vol. 10 Issue 13 (Ver. 1.0), October 2010.

[15] Prof. Pranita K. Gandhewar Computer Science & Engineering Department NYSS College of Engineering & Research Nagpur, India E-mail: pranita.gandhewar@gmail.com,Prof. Prasad P. Lokulwar Computer Science & Engineering Department, J.D Institute of Engineering and Technology Yavatmal, India.E-mail: prasadengg16@gmail.com”. **Improving Security in Initial network entry process of IEEE 802.16 e”.**

[16] Muhammad SakiburRahman,Mir Md.Saki kowsar, Dept. of Computer Science and Engineering,Chittagong University of Engineering and Technology ”**WiMAX Security Analysis and Enhancement**” Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009),Dhaka,Bangladesh.

[17] **Guide to Securing WiMAX Wireless Communications**, Recommendations of the National Institute ofStandards and Technology, Karen Scarfone,Cyrus Tibbs,Matthew Sexton, NIST(National Institute of Standard and Technology),US Department of Commerce.

[18] Federal Information Processing Standards Publication November 26, 2001**" Announcing the Advanced encryption standard (AES)."**

[19] Dr. Brian Gladman, v3.1, 3rd March 2001 "**A Specification for Rijndael, the AES Algorithm,**"

AUTHOR PROFILE

First Author Dr.Reena Dadhich Head of MCA Dept., Government Engineering College, Ajmer. Research Area: Wireless Adhoc Network Contact No-992855895 E-mail id:reena.dadhich@gmail.com

Second Author Ms.GeetikaNarang Asst. Prof,Sinhgad Institue of Technology,Loanavala B.E(CSE), M-Tech(CS) SubEditor of JAES,STES (Journal of Advance Engineering Science) Research Area: Wireless Contact No-9689896065 E-mail id: geetika.narang@gmail.com

Third Author Dr.D.M.Yadav Principal of JSPM'S BhivarabaiSawant Institue of Tech Research Area: Digital Signal Processing, Wireless, Image Processing and Neural Network. Contact No:9011063944 E-mail id:dineshyadav_8@yahoo.com