SECURITY ISSUES OF WIMAX

V Venkata Santosh[1], Balajee Maram[2], V KUMAR[3]

[1] B.Tech student, CSE Dept., GMR Institute of Technology, Rajam, AP. venkatasantosh.vummididev@gmail.com

[2] Asst. Prof., Dept of CSE, GMRIT, Rajam, AP, balajee.m@gmrit.org

[3] Asst. Prof., Dept. of Computer Science, Central University of Kerala, Kerala, vkumar@cukerala.ac.in

ABSTRACT

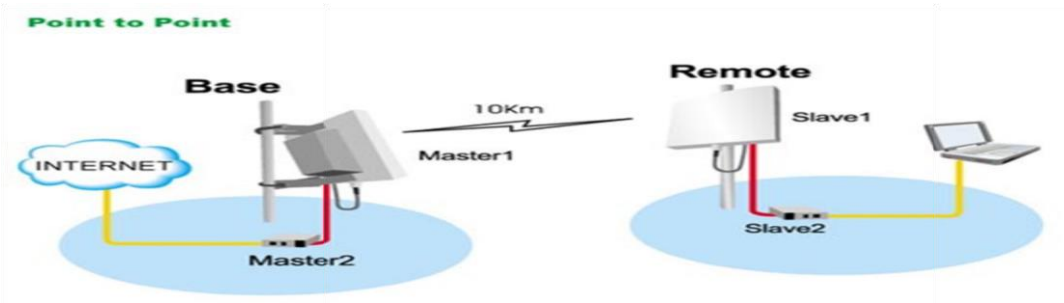
WiMAX: worldwide interoperability for microwave access is newly emerging technology, which is under developing. The main difference from the Wi-Fi to WiMAX is the range i.e. it covers more area than that of Wi-Fi. But in the development process of the newly emerging technology also there are different issues to be considered in order to eliminate threats to security. The actual security techniques have been implementing in the physical and mac layers. So the threats to security also may occur in these two layers only. In this paper we will address the different types of layers and the functions of each layer which is other than protocol architecture, the different types of security solutions, and what are the different types of threats to physical and mac layers.

1.INTRODUCTION

The history of the WiMAX started in 1999 by IEEE Standards Board, the IEEE 802.16 is a working group on Broad Wireless Access (BWA). The first version of WiMAX IEEE 802.16 was released in 2001 with line of sight capability to specialize point to multipoint broadband wireless transmission in the 10-66GHZ spectrum. The IEEE 802.16a published to accommodate the requirement of Non-Line of sight operation. After revising several times the standard was published in 2004 as IEEE 802.16d. In 2005 an amendment to IEEE 802.14 the IEEE 802.16e was released in order to address the mobility so that a mobile station can handover between mobile stations so this standard is called as Mobile WiMAX.

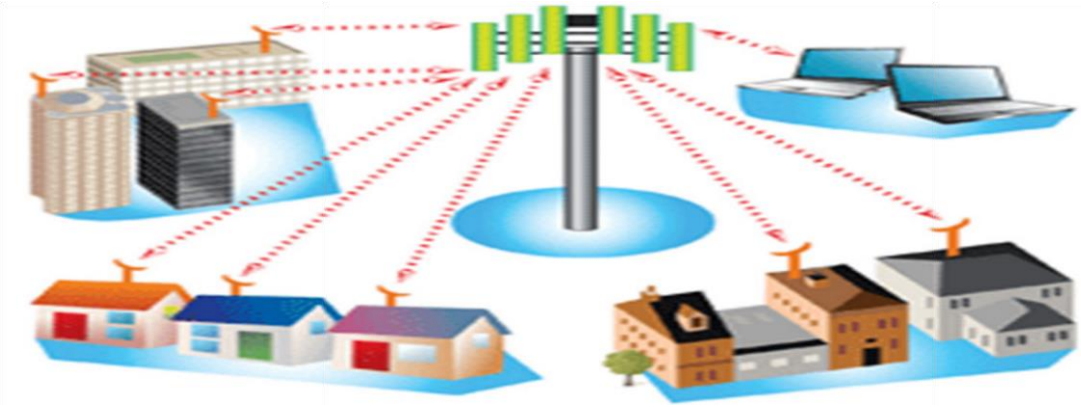
1.1 Notation and Terminology

1.1.1 *POINT TO POINT*: The term point to point to itself saying that the entire communication from a sender to a particular receiver is taking place.



1.1.2 BASE STATION:

A Base station is providing its network to a large area. Any wireless device with the required privileges can access the network services provided by the base station.



1.1.3 *SUB STATION:* A Substation in a WiMAX network is nothing but a receiver while the base station is acting as a sender. This should connected to the base station in order to get the network services provided by the base station and this should be within the network coverage area of the base station.

Fig 1: Substations connected to a base station

1.2 ENCRYPTION: the translation of the data from its original form to a different form (secret code) in order to provide secure transmission. To read an encrypted file we need to first decrypt it and also we should have permissions like password to read it.

1.3 AUTHENTICATION: The process of identification of a particular person through some particular ways like username and password. The authentication and authorization are purely different from one another in the security world.

1.4 AUTHORIZATION:

This is the process of giving permission to an individual who is an authorized user access the resources. This will be done only after the successful authentication.

1.5 LINE OF SIGHT: A line along which no obstacles are present in a communication.

1.6 NON LINE OF SIGHT: There may be some obstacles along the communication line.

2.SECURITY ISSUES RELATED TO PHYSICAL AND MAC LAYERS

The physical layer in IEEE 802.16e supports four PHY SPECIFICATIONS.

They are:

1).Wireless-MAN-SC (single carrier).

2). OFDM (orthogonal frequency division multiplexing).

3). OFDMA (orthogonal frequency division multiple access).

4).W Most PHYs are designed for non-line-of-sight (NLOS) operation in frequency bands below 11 GHz, except -SC, which is for operation in the 10-66 GHz frequency band. To support multiple subscribers, IEEE 802.16 supports both time-division duplex (TDD) and frequencydivision duplex (FDD) operations. [1]

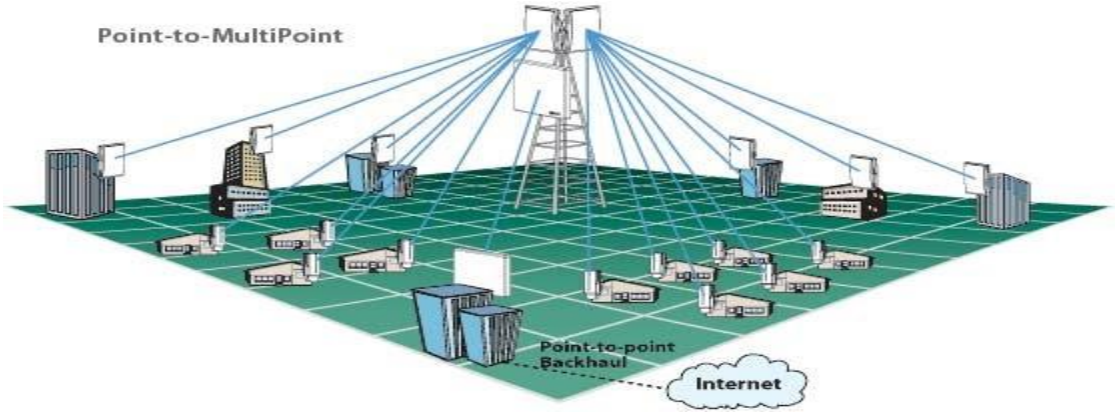
In the medium access control (MAC) layer, IEEE 802.16 supports two modes:

They are:

1. Point-to-multipoint (PMP).
2. Mesh mode.

2. 1. Point-to-multipoint: The point to multipoint network will be in such a way that the communication or the transmission of data from a single source to different receivers

with different requirements. This may be useful in order to connect the same networks such as LANs at different floors of the same building.



2.2 Mesh Mode: A mesh network topology is a decentralized design in which each node on the network connects to at least two other nodes.

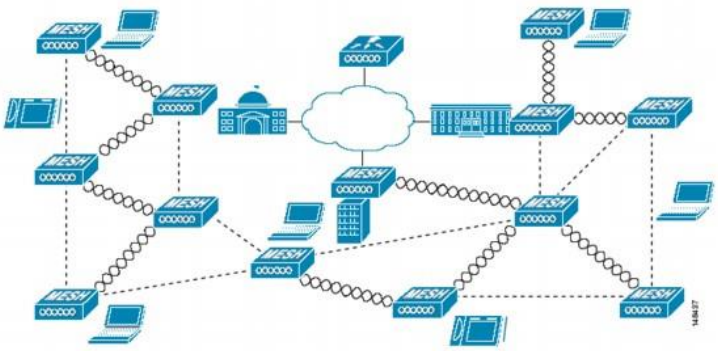


Figure 2: Mesh Mode

There are two stations which have been involving in the entire network, they are Base Station (BS) and Subscriber Station (SS).

The channels are also divided into two types they are: uplink and downlink. Uplink is between sub-station and base station. Similarly the downlink is between base-station and sub-station. The uplink and downlink channels are shared among the sub-stations also..

In point to multipoint mode all the substations to be with in the transmission range and they also should have clear line of sight.(LOSs)

In mesh mode all the nodes i.e. the substation and base stations will act as routers along with their sender and receiver roles. The multi hop communication is becoming more and more important in WiMAX system in view of cost-effectiveness. In order to have the multi hop networks security has become the major challenge that must be addressed. [1]

3. PROTOCOL ARCHITECTURE

All the security mechanisms have been implementing in the physical and mac layers. So in order to know what security issues involved in the design of the WiMAX first we need to know the protocol architecture of the data link and physical layer.

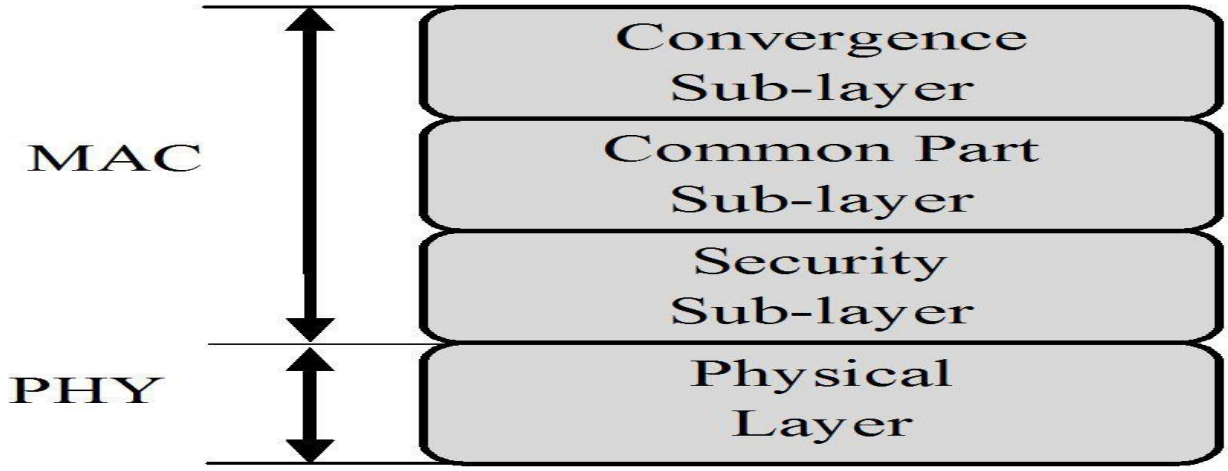


Figure 3:The IEEE 802.16 Protocol Structure [2] The

IEEE 802.16 protocol architecture is divided into two main layers:

3.1 MAC layer: It consists of three sub-layers.

(a) **Service Specific Convergence Sub-layer (CS)**:

Which maps higher level data services to MAC layer service flow and connections. [1]

(b) **Common Part Sub-layer (CPS)**:

Which is the core of the standard and is tightly integrated with the security sub-layer. This layer defines the rules and mechanisms for system access, bandwidth allocations and connection management. The MAC protocol data units are constructed in this sub-layer. [1]

(c). **Security Sub-layer**:

Which lies between the MAC CPS and the PHY layer, addressing the authentication, key establishment and exchange, encryption and decryption of data exchanged between MAC and PHY layers. [1]

3.1 The PHY layer: It provides a two-way mapping between MAC protocol data units and the PHY layer frames received and transmitted through coding and modulation of radio frequency signals.

PHY features include support for multiple-input multiple-output (MIMO) antennas in order to provide good non-line-of-sight propagation (NLOS) characteristics (or higher bandwidth) and hybrid automatic repeat request (HARQ) for good error correction performance. [1]

4.SECURITY SOLUTIONS

The support for authentication, key management, encryption and decryption, control and management of plain text protection and security protocol optimization according to new technologies available today. Actually the security issues are addressed and handled in the security sub layer. [11]

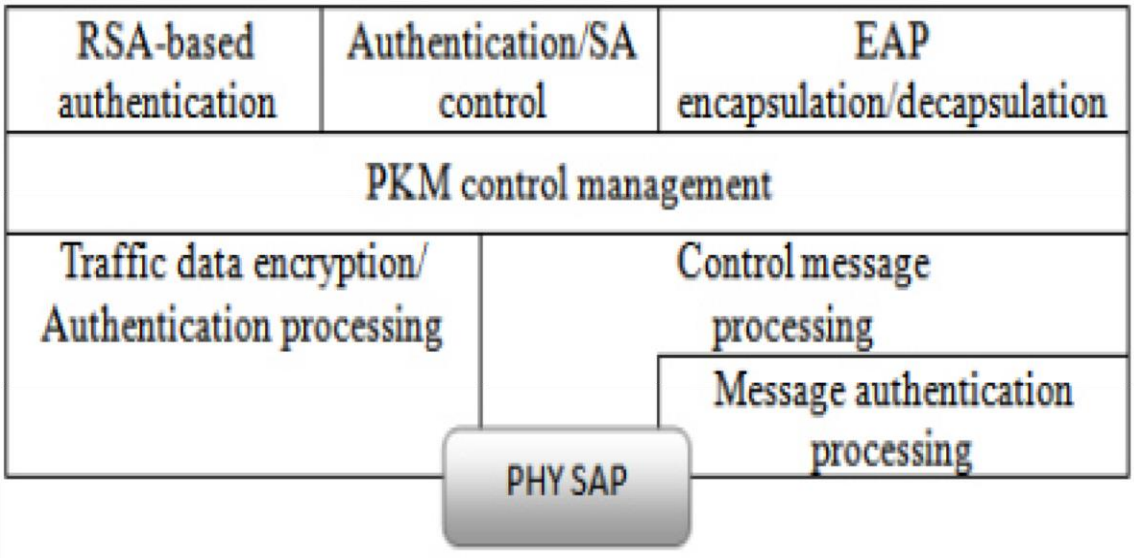


Figure 4: **MAC Security sub-layer**

The main entities in the network like Base station (BS) and Sub Station (SS) are protected in the IEEE 802.16e by the following security features.

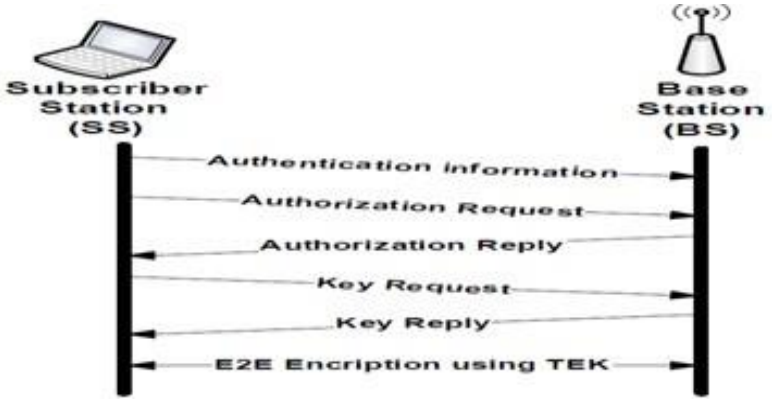
They are:

4.1 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. Each SA has its own identifier SAID) and also contains a cryptographic suite identifier for selected algorithms), traffic encryption keys (TEKs) and initialization vectors. [1]

4.2 PUBLIC KEY INFRASTRUCTURE

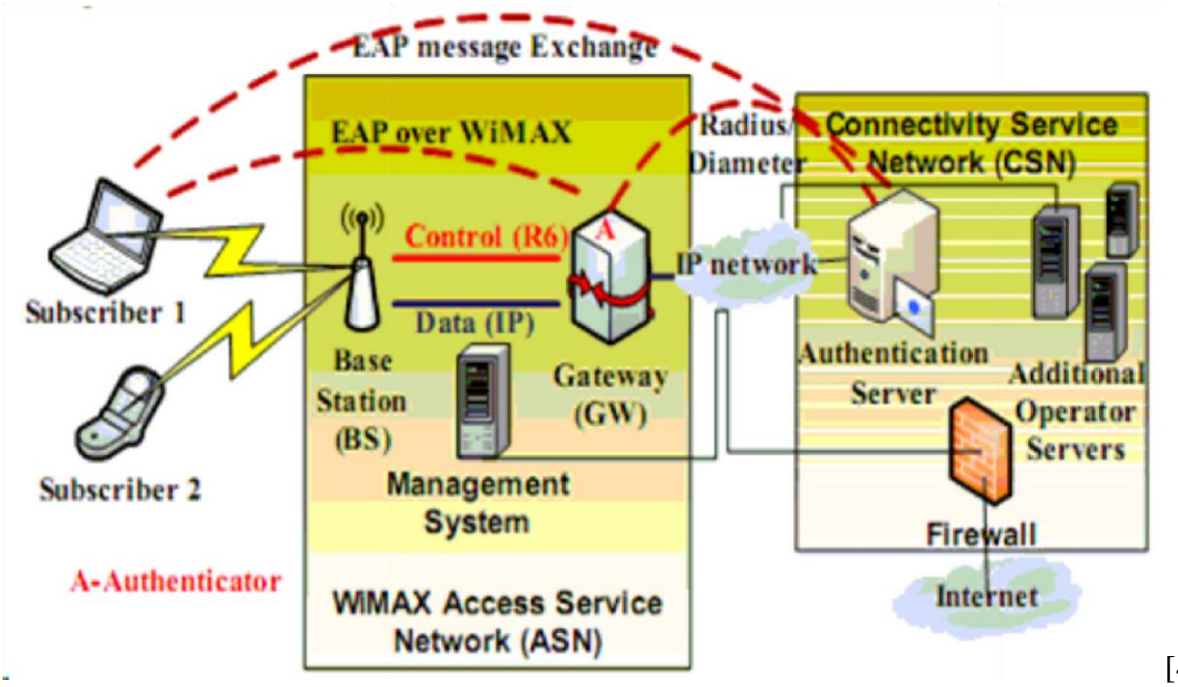
WiMAX uses public key management for the secure key management, transfer and exchange between mobile stations. This will also authenticates the base stations to mobile stations. The first of draft version of WiMAX uses the PKMV1 protocol which is a one way authentication mechanism it also may have a chance of Man In the middle attack. In PKMV1 the substation only required to authenticate itself to the base station. In order to avoid the situation like man in the middle the new technology PKMV2 was released and used in IEEE 802.16e.[2] In the PKMV2 two way authentication protocol was used, in this both substation and the base station need to authenticate and authorize each other.



4.3 USER AUTHENTICATION

There are two types of authentication which are being implementing in the security sub layer. The first type is RSA based authentication which implies X.509 certificates .In this when the substation wants the services from the base station, it sends the digital certificate to the base station. The base station then validates the certificate, the base station uses the verified Public Key to encrypt an Authorization Key and sends that to the substation. The second type is

Extensive Authentication Protocol (EAP) based authentication, in this the base station is authenticated using X.509 certificate.[1]



[4]

Figure 5: IMAGE FOR EAP- BASED AUTHENTICATION

4.4 AUTHORIZATION

In this the substation requests for an Authorization key from base station through sending an authorization request message. The base station then interacts with the AAA (Authentication, Authorization and Accounting) server to validate the request from the substation. After a successful validation by the base station the base station sends back an Authorization reply which includes Authorization key encrypted with the substation public key.

5.WIMAX SECURITY ISSUES

All the security mechanisms have been implementing in the physical and mac layer. So if any threats are there they only effect these two layers only. So there are two types of threats in the security issues of WiMAX. They are Threats to the physical layer and threats to the mac layer.

5.1 THREATS TO THE PHYSICAL LAYER

The actual security for the WiMAX has been implementing at the sub layers of MAC layer. So there may not be any protection to the physical layer, because of this the physical layer may be exposed to attacks which target the inherent vulnerability of wireless links.

1. Jamming is a type of attack to the physical layer in which can be defenseless [2]. It can be achieved by introducing a source of noise strong enough to reduce the capability of the WiMAX channel. The equipment required which can be used to perform jamming is not difficult to acquire [1].
2. Scrambling is a just as like as jamming but this will be in action for short intervals of time. This will be done with the aim of attacking the normal operation of the network [1]. This will cause the retransmission of the bits by scrambling the slots of data traffic which are belonging to the targeted substation. [2]
3. Water torture attack will causes the substation to exhaust its battery by sending the bogus frames to it i.e. by dissipate the computing resources. This will be more serious in case of mobile station because the portable devices may have limited number of resources.[3]

The attacks to the physical layer can be prevented by taking several countermeasures like

- By increasing the power of signal which will oppose the jamming attack. We can increase the power of the signal in such a way that by using a monitoring device which will detect the jamming and the irregular state of the radio spectrum, after detecting we can increase the power of the signal.
- The scrambling attacks can be exposed by analyzing the discrepancies in the system performance [3]. In the latest standard 802.16 the mobility for mobile stations was included, so by residing in a fixed place and to monitor the network becomes difficult for an attacker.

5.2 SECURITY ISSUES OF THE MAC LAYER

Since MAC layer is connection oriented, there are two types of connection in the mac layer.
They are management connections and data transport connections.

Management connections are again of three types: basic, primary and secondary.

A basic connection and primary connection will be created for each mobile station when it joins with the network and these can be used for short and management messages and for delay-tolerant management messages respectively [1]

The secondary connections will be used in the time of IP encapsulated management messages.

Coming to the different types of attacks to the MAC layer, are as follows

1) DOS/ REPLY attacks during the entry of the mobile station into the network.
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.

1. In dos/reply attack during the entry of the mobile station into the network and it is very necessary because it is the first gate to establish a connection to mobile WiMAX by performing several steps like initial ranging process, substation basic capability and negotiation and PKMv2 authentication and registration process.[3]
2. Latency during handover and unsecured pre authentication: while the process of handover, the main station will be re-authenticated and authorized by the target base station. Because of the re-authenticated and key exchange mechanisms the handover time increases which will seriously affect the delay sensitive applications.
3. Downgrade attack: The substation have to send a message to the base station telling the base stations about what security capabilities it has. An attacker can send a spoofed message to the base station stating weaker capabilities in order to convince the base station and to attack the substation in such a way that it can obey for the insecure encryption algorithm.
4. Cryptographic algorithm computational efficiency: in the current existing features of the security, the number of bits needed for encryption in RSA is more than Elliptic Curve

Cryptography (ECC) for a required encryption which will lead to the more computation time.

5. Bandwidth Spoofing: in the bandwidth spoofing the attacker can grabs the available bandwidth by sending the spoofed messages to the base station.
6. Key space vulnerability: in the IEEE 802.16e a four bit sequence and two bit sequence number are using to discriminate between the two successive generations of AKs. The same two bit sequence number is used for the same reason with TEKs. Here the size of the key is inadequate to protect the keying material from attacks.[3]
7. Man in the middle attack: in the IEEE 802.16e the management messages defined are integrity protected. This can be done using the hash based message authentication code (HMAC) or using the cipher based message authentication code (CMAC) [3]. In this there is chance in which there will be some messages which are not covered by any authentication mechanism. This will lead to the man in the middle attack.

6. CONCLUSION

In this paper we have seen the existence of the current standard i.e. 802.16e, the different types of modes of propagation, the important mechanisms involved in the communication, the protocol architecture, the security solutions which are currently using, and different types of security issues related to both the physical and mac layer. After reading all these we can say, the security solutions need to be improved in such a way that the establishment of connections between mobile station, substation and base station should follow some more rules which should be followed only after having some certification for the substation and mobile station by the base station. We need further research on the security solutions the current standard, in order to reduce the security threats.

REFERENCES

[1] Mohammed shafeeq ahmed, department of computer science, Gulbarga university" A STUDY ON IEEE 802.16(WiMAX) ABD UTS SECURITY ISSUES",2014.

[2] Mitko bogdanoski,pero latkoski. Aleksandar risteski,"IEEE 802.16 Security Issues:A survey" 2008.

[3] Aditya Kumar, Prof. P S Sharma, Prof vivek Kumar Gupta **"**Review of Security Threat and

Solution in WiMAX (802.16e)**"** International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 2 February, 2014 Page No. 3965-3970.

[4] Jamshed Hasan Edith **"**Security Issues of IEEE 802.16 (WiMAX)**"** 2006.

[5] H. Kaur and J. Saini, **"**Review Paper on Performance Improvement of WiMAX using Coding Techniques, International Journal of Current Engineering and Technology, Vol. 3, No. 4**"**, October 2013.

[6] A. Kumar, P. S. Sharma, V. K. Gupta, **"**Review of Security Threat and Solution in WiMAX (802.16e), International Journal of Scientific and Engineering Research, Vol. 4**"**, July 2013. [7] M. Barbeau, "WiMAX/802.16 threat analysis," in Proceedings of the 1st ACM international workshop on Quality of service security in wireless and mobile networks, Quebec, June 2005 . [8] J. K. T. T. Andreas Deininger, Shinsaku Kiyomoto, "Security vulnerabilities and solutions in mobile wimax," vol. 7, no. 11, Nov 2007.

[9] M. E.-H. A. E.-H. Mahmoud Narsreldin, Heba Aslan, "Wimax security," in 22nd International Conference on Advanced Information Networking and Applications, 2008, pp. 1335–1340.

[10] W. C. Taeshik Shon, "An analysis of mobile wimax security: Vulnerabilities and solutions," in Lecture notes in computer science, Springer, 2007

[11] R. Poisel, "Modern communications jamming principles and techinques," in Artech House Publishers, 2003.

[12] A. A. Ayesha Altaf, Rabia Sirhindi, "A novel approach against dos attacks in wimax authentication using visual cryptography," in The Second International Conference on Emerging Security Information, Systems and Technologies, securware, Cap Esterel, France, 2008.