Prevention of Security Threats in IEEE 802.16 Standards

Rajesh Srivastava, Deepak Kumar Mehto

Abstract— ***The WiMAX IEEE 802.16 (e) is defined as the Worldwide Interoperability for Microwave Access by the WiMAX Forum, formed in April 2001 to promote conformance and interoperability of the IEEE 802.16 standard, officially known as WirelessMAN. An authentication and authorization model provides protection for a network or technology and protects its resources from unauthorized use. This article examines the threats which are associated with MAC layer and physical layer of WiMax and also proposes some enhancements to the existing model for improving the performance of the encryption algorithm.***

Index Terms—WiMAX802.16, Authentication, PKMv1& PKMv2, Security mechanisms etc.

I. INTRODUCTION

During the last decade, remarkable growth in the field of wireless communication has changed our life styles. Different aspects of applications and services are explored and new standards emerged to address specific scenarios. The current trend is towards personalization and research in this field focuses on user centricity. The near future devices will be able to support many interfaces. Work is going on [5], how to link applications to different interfaces based on the application requirements. In other words, modern devices and applications will be able to select the best service from a list of available services. Analysis of various communication technologies reflects that no single technology can be claimed as the Best-Fit solution. So, a possible way to step forward is WiMAX emergence has launched a series of debates and discussions at various fronts about the future of many other to design a suitable Interworking architecture for competitive technologies in way so that they can supplement each other. technologies. With so many prominent features like higher data rate (up to 70 Mbps) and large coverage area (up to 30 miles), it initially provided Fixed wireless broadband access. The new IEEE standard 802.16e provides support for mobility which is another breakthrough. Mobile broadband wireless access (802.16e) will attract many vendors and users because of its appealing and useful features. Although WiMax has farther transmission distance and faster speed than those of IEEE802.11 [1], due to using radio signals to transmit data, it is also now facing network security issues. In fact, its security is fragile as that of Wi-Fi. So, the IEEE802.16 standard [2] was drawn up a security mechanism called Privacy Key Management version1 (PKMv1) which mainly manages keys and defines particular confidential and unidirectional authentication for later message delivery. The IEEE802.16e [3,4] owing to performing mobile authentication has been practiced in the way of 802.16 key management (PKMv1) and set up PKMv2. In PKMv1, the authentication between SS and BS is not a two-way approach, so an SS has the possibility to connect to a fake BS. WiMAX is described in the IEEE 802.16 standard. The IEEE standard 802.16-2001 was first designed to provide the last mile for WMAN with line-of-sight working at 10- 66GHz bands. IEEE standard 802.16-2004 [6] consolidates previous standards and supports non-line-of-sight within 2- 11GHz bands and mesh nodes. The latest WiMAX standard, IEEE 802.16e-2005 [4], provides full mobility in broadband wireless access. In this article , analysis and verification of the IEEE 802.16 authentication and key management protocols (both PKM version 1 and 2) is done. It starts by performing an evaluation of the security objectives and build a clear attack model for various attacks to PKM. Afterwards, analysis of the protocols against such security objectives is done informally to check if there are any inconsistencies in the definitions and extract the main holes that exist in both protocols. The rest of the paper is organized as follows: Section 2 describes the WiMAX security scheme .Section 3 describes the PKM protocols.Section 4 describes the existing security model . Section 5 describes the proposed enhancements in the existing model. Section 6 Analyse the proposed scheme.Finally Section 7 concludes our paper. In last References are given.

II. WIMAX SECURITY SCHEME

The IEEE 802.16 standard consists of a protocol Stack with well-defined interfaces [7]. The scope of Protocol contains MAC layer and PHY layer. MAC layer includes three sub-layers shown in Figure 1. The Service Specific Convergence Sub-layer (MAC CS), the security sub-layer and the MAC Common Part Sub-layer (MAC CPS). The service specific Convergence Sub-layer maps higher level data services to MAC layer service flows and connections. There are two type of CS: ATM CS which is designed for ATM network and service, and packet CS is to supports Ethernet, point-to-point protocol (PPP), both IPv4 and IPv6 internet protocols and virtual local area network (VLAN) [8]. The MAC Common Part Sub-layer (MAC CPS) is the core of the standard. MAC CPS defines the rules and mechanisms for system access, connection management and bandwidth allocation.

Manuscript received May 30, 2011.

Rajesh Srivastava, Asst . Professor, Comp. Sci. & Engg. Dept.,ShriRam Institute of Technology, Jabalpur(M.P.), India, (email: rajesh_5479@rediffmail.com).

Deepak Kumar Mehto, M.E. (S.S.), ShriRam Institute of Technology, Jabalpur (M.P.), India, (e-mail: deepak_mtech@rediffmail.com).

Functions like uplink scheduling, bandwidth request and grant, automatic repeat request (ARQ) and connection control is also defined here. Communications between the CS and the MAC CPS are done by MAC Service Access Point (MAC SAP).

The Security Sub-layer lies between PHY layer and MAC CPS [9]. This sub-layer is responsible for decryption and encryption of data traveling to and from the PHY layer and it is also used for authentication and secure key exchange. WiMAX system based on the IEEE 802.16e-2005 amendment has more improved security features than previous IEEE 802.16d-based WiMAX network system. Almost all the security issues in Mobile WiMAX are considered in security sub-layer.

A.Authentication

Authentication is achieved by using a public key interchange protocol which ensures not only authentication but also the establishment of encryption keys. Once the SS has established a connection to the BS, a management channel using the PKM protocol is opened. The management channel is used by the SS to register itself with the BS. The SS then uses a built-in X.509 certificate to authenticate through the BS and is allowed to join the network upon successful authentication. 802.16e based-on Mobile WiMAX defines Privacy Key Management (PKM) protocol in security sub-layer, which allows three types of authentication.

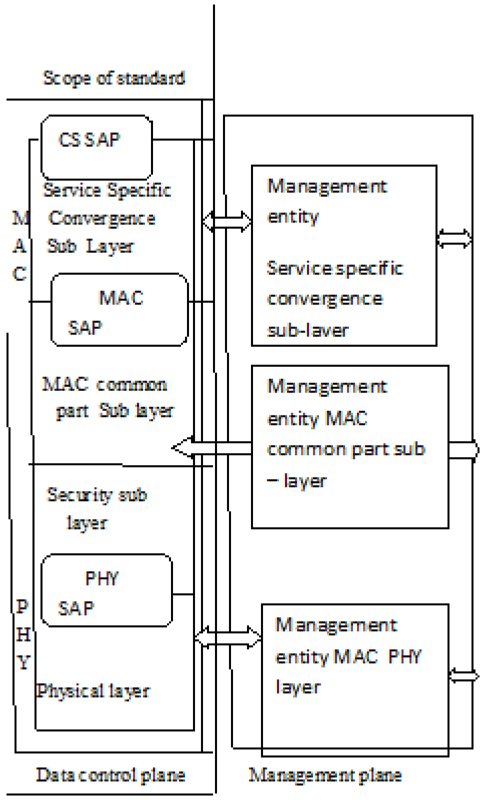
Scope of standard
CS SAP
Service Specific Convergence Sub Layer
M A C
MAC SAP
MAC common part Sub layer
Security sub layer
PHY SAP
P H Y
Physical layer
Management entity
Service specific convergence sub-laver
Management entity MAC common part sub – layer
Management entity MAC PHY layer
Data control plane
Management plane

Fig. 1 .Protocol layering in 802.16

B. Authorization:

Following authentication is the authorization process. In this process, M.S. requests for an AK as well as an S.A. (Security Associations) identity (SAID) from B.S. The Authorization Request message includes M.S's X.509 certificate, encryption algorithms and cryptographic ID. In response, the B.S. interacts with an AAA (Authentication, Authorization and Accounting) server in the network to carry out the necessary validation and sends back an Authorization reply that contains the AK encrypted with the M.S's public key, a lifetime key and an SAID.

C.Traffic encryption

The previous authentication and authorization process results in the assignment of and Authorization Key, which is 160 bits long. The Key Encryption Key is derived directly from the AK and it is 128 bits long. The KEK is not used for encrypting traffic data; so SS require the Traffic Encryption Key (TEK) from BS. TEK is generated as a random number generating in the BS using the TEK encryption algorithm where KEK is used as the encryption key. TEK is then used for encrypting the data traffic.

D. WiMAX security process

Security process is divided into three steps:

01. Authentication
02. Data Key exchange.
03. Data Encryption.

III. PKM PROTOCOL DESCRIPTION

Ensuring wireless networks protection means that we need to protect this network against different aspects that can destroy information integrity.The security objectives which are essential to SS are [11] :

• *Pseudonymity* This means that an outsider, who keeps track of the communication, cannot relate the traffic to a specific SS.

• *Information Confidentiality* Only authorized users have access to information.

• *No theft of Service should be possible*, Where neither an unauthenticated user should gain access to the services provided, nor should an unauthenticated user be able to impersonate another user. The security objective which is essential to both the BS and the SS is:

• *Session Key Establishment*, where the shared session keys must be secret, and identify the protocol sessions, in the sense that there is exactly one execution of every protocol role sharing the session key. There are several attack techniques that face wireless networks, and some of these attacks are: Active eavesdropping, man-in-the-middle- attack, replay attack and multiplicity attack. In the case of IEEE 802.16, message replay and man-in-the-middle attack are the most famous attacks on PKMv1. Multiplicity and simple replay attack are the typical attacks on PKMv2, as well as the interleaving attack.

PKMv1Authentication Protocol

According to the authentication protocol of PKMv1 (fixed version) shown in Fig. 1, the SS begins authorization by sending an Authentication Information message which contains the SS manufacturer's X.509 certificate [12] (Cert (Manufacturer (SS))) to the BS to demonstrate that it is a trustworthy device.

Afterwards the SS sends its own certificate (Cert (SS)), its cryptographic capabilities and a 16 bit security association identifier (SAID), this message is called Authorization Request message (Auth-REQ). The certificate of the SS contains its RSA Public Key, MAC address, serial number, and manufacturer ID. In response to an Auth-REQ, the BS validates the requesting SS's identity, uses the certificate of the SS to determine if the SS is authorized, determines the encryption algorithms and protocols to be shared with the SS, generates an Authentication Key (AK), and sends the AK (128 bits), which is RSA encrypted with the received public key of the SS {AK}pk(SS), the lifetime of the AK, a 4-bit sequence number, used to distinguish between successive generations of AKs, and a list of SAIDs which contains the identities and the properties of the SA list the SS authorized to access.

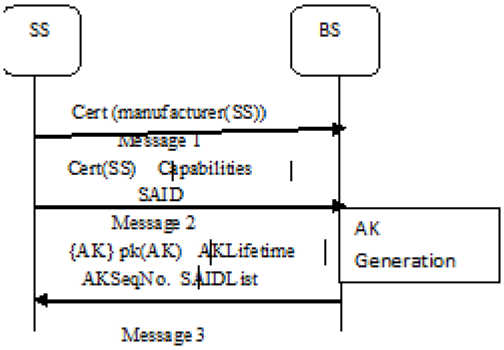

Fig 2. PKMv1 Authentication Protocol

A. Analysis of PKMv1 Attacks

1) Message Replay Attack: If the messages exchanged in an authentication protocol do not carry appropriate freshness identifiers, then an adversary can easily get himself authenticated by replaying messages copied from a legitimate authentication session. BS may face a replay attack from a malicious SS who intercepts and saves the authentication messages sent by a legal SS previously. Although an adversary eavesdropping the messages cannot derive the AK from messages because it does not have the corresponding private key, the adversary still can replay the message 2 multiple times. Therefore, the Deny of Service occurs to the SS who owns that Cert(SS). The SS cannot detect a replay attack, because nothing in the protocol leads to this conclusion. To avoid these replay attacks, the authors in [10] proposed adding a nonce to message together with a signature of SS. However, the exchange of nonces only assures SS that message 3 is a reply corresponding to its request. The BS still faces the replay attack because BS cannot tell whether message 2 is sent recently or it is just a replayed message. Thus, it is proposed to send a pre-AK to SS instead of AK, and let SS and BS derive AK from the pre-AK at both ends.

2) Man in the Middle Attack: One of the Most important security flaws is the one way authentication, which only authenticates the SS to a BS and not vice versa. SS however has no way of knowing whether the entity sending the AK is a legitimate BS or not. This design lack opens the protocol to forgery attacks, where an unauthorized BS can communicate with a SS. Mutual authentication can eliminate this vulnerability, i.e., SS needs to authenticate BS as well. This can be done by adding BS's certificate in message 3.

PKMv2 Authentication Protocol

The latest standard, IEEE 802.16e-2005, includes a new version (PKMv2) of the protocol that caters for the shortcomings of the first version. PKMv2 supports two different mechanisms for authentication: the SS and the BS may use RSA-based authentication or Extensible Authentication Protocol (EAP) -based authentication. Here , RSA based authentication is prefered for PKMv2 authentication protocol.

E. Analysis of PKMv2 Attacks

1) Interleaving Attack: Without SS signature, the request message is easy to be modified or impersonated. This is similar to what is discussed before on PKMv1 and it is refered to as simple replay attack. Even with the signature from SS served as message authentication, attack still exists. Such attack is similar to the one proposed in [14], which is classified as Interleaving Attack in [15]. This attack uses the messages from previous protocol sessions being run concurrently to the main protocol session, in order to provide the messages in the main protocol session.

2) Multiplicity Attack: A new attack on the original X.509 3-way authentication protocol was found by [13] when one agent is mistaken about the multiplicity of sessions. This attack can be eliminated by adding the BS's identity. From the above discussion, it can be concluded, that Basic PKM has many flaws such that it provides almost no guarantees to SS about the AK. PKMv2 adds an additional message at the end of the protocol, intending to assure BS the freshness of the first message. However, this goal fails and interleaving attack still applies. So it can be concluded, that the SS's signature and the BS's certificate are critical to all versions of authentication protocols.

IV. EXISTING SECURITY MODEL

The purpose of WiMax network is to expand the range and access of wireless systems. The existing security model is about the security association and security keys generation or establishment when the MS is entering the network range of a BS. Here it is desired to eliminate the above mentioned attacks on the PKM Protocols. The Model shows the main key elements as entities and the relationship between them is also shown. Three types of security associations are sketched in the model namely primary, static and dynamic. These three security associations are types of data SA (Security Association). WiMax architecture uses different mechanisms, to establish a secure communication between BS and MS. Security Associations (SAs) are used by both MS and BS to establish a new connection.

A Security Association (SA) is defined as the set of security information shared between a BS and one or more of the MS's connected to that BS in order to support secure communications across the WiMax access network [16]. There are two main types of security association; first one is Data Security Association and second is Authorization Security Association. Data SA is further divided into three types, namely Primary SA, Static SA and Dynamic SA. Each MS has one primary SA, and primary SA is established when the MS is initialized. The Static SA is created when the BS initializes the MS. And the last SA, Dynamic SAs are dynamically generated by the BS and are used for transport connections when needed. Second type of Security Association is Authorization SA which is used for the authorization purposes. The BS uses the Authorization SA to establish the Data SA between MS and BS. Other entities shown in Figure 2 are AK (Authorization Key), X.509 certificates, HMAC etc. X.509 certificate is held by the MS, the public key of the MS is present in its digital certificate, which is used for access control, authentication and confidentiality. MS uses it's public key for communication with the BS. When authenticated the MS sends an authorization request message to the BS, the BS generates an AK (Authorization Key) having a sequence number and a life time and passes it to the MS in an encrypted form with public key of MS having sequence number 0-15. The hashing technique used in this model is HMAC which is not providing message replay protection. Another key which is KEK (Key Encryption Key) used for encryption purpose. The KEK and HMAC both are calculated from the AK. In last the TEKs are generated and KEK encrypt these TEKs at the time of TEK request reply. When the TEK is obtained the exchange of data or information is started and communication is established [2].

V. PROPOSED ENHANCEMENTS IN THE EXISTING MODEL

Due to some complexities in various models of WiMax networks, security has been more stringently placed into WiMax. It is the responsibility of the network service provider to develop comprehensive security strategies for designing a secure network. Otherwise, the network and the users will become vulnerable to threats and hackers. To study the security of WiMax it is required to understand the primary protection methods of WiMax security. In the existing model some of the enhancements are done to enhance the performance and security of the model. For this purpose some mechanisms are proposed in the existing model by keeping in mind their level of security and functionality. The model is based on the communication of BS and MS. And the main theme of this model is security. When an MS enters the network range of a BS, the SS and BS communicate with each other to provide authenticity and to authorize one another. The model is subdivided into three phases. 1st Phase discus the Data security association, Authorization security Association (SA) is in 2nd phase while the 3rd phase is about the Exchange of KEYS.

A. Data Security Association

Before starting the connection process the MS uses the Data SA to communicate for connection request. Three types of data Security Associations are shown in the model namely Primary SA, Static SA and Dynamic SA. Data SA has a 16 bit SA identifier SAID, a cryptographic cipher identifier, which uses Data Encryption Standard (DES) in CBC mode for protection of data during transmission. Also have two TEKs (Traffic Encryption Keys), one is used as current operational key and the other as TEK. A 64 bit initialization vector (IV) is used for each SA. The life time of the TEK is from 30 minutes to 70 days. Generally an MS can have two or three SAs (Security Associations).

B. Authorization Security Association

Authorization SA is used for authentication purpose, to provide authentication between MS and BS. In 802.16e/Mobile WiMax there is mutual authentication, so the BS will authenticate the MS and the MS will also authenticate the BS. The Authorization SA consists of an AK (Authorization Key) of size 60 bits, having a life time range from 1 to 70 days. The default life time value of an AK is 7 days. Another key KEK (Key Encryption Key) is also used having a size of 112 bits 3DES key, the KEK is used for the distribution of TEKs. An authorization SA also uses hash functions to provide authenticity between MS and BS. [17] States that BS use Authorization SAs to configure Data SAs on the SS (Subscriber Station). In the original model the X509 certificates are send to the BS by the MS but here in the proposed model the usage of X509 certificate are changed and WTLS certificate is used instead of X.509 certificate. WTLS reduces the space occupied by the X509 certificates because it has a small serial number and issuer unique ID etc. Another change regarding the original model is the changing of the encryption algorithm, ECC (Elliptic Curve Cryptography) is of 163 bits and having the same encryption strength as compared to the RSA. So here the memory is saved due to small key size. The hashing function used instead of RSA (Rivest, Shamir, and Adleman) encryption. RSA using 1024 bit of key but on the other side ECC is using only a key size used in the existing model is HMAC (Hash function-based Message Authentication Code) but OMAC (One-key CBC MAC) can also be used for the hashing purpose. This OMAC algorithm is extremely simple, and has proven to be quite secure against message replay attack.

C.Exchange of KEYS

To encrypt the data a key is needed known as TEK which uses AK (Authorization Key). The Message Authentication Key (HMAC Key) and the KEK are derived from the AK by the BS and MS individually. The TEK is generated by BS after the request of MS from the BS and is sent in an encrypted form to the MS. The TEK is encrypted by 3DES having 112 bits KEK or AES (Advanced Encryption Standard) is used for the encryption purpose using 128 bits KEK. The Authentication of Key Exchange message is done by HMAC hashing technique. At last the communication is established and the exchange of information is started in a secure way.

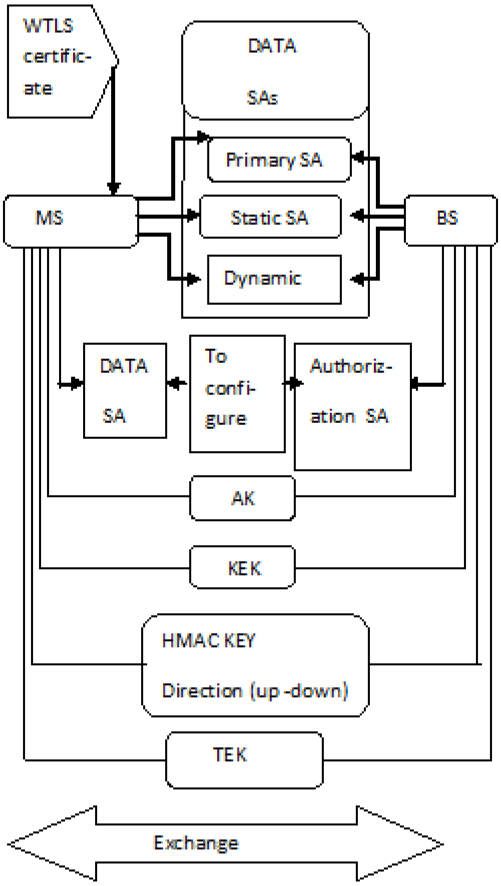

Fig. 3: Proposed model General view

VI. ANALYSIS & DISCUSSION

The communication between the BS and MS takes place in steps. Security Association, Authorization, Authentication and lastly the data encryption are followed in a sequence. In fixed WiMax, unilateral authentication is followed where BS authenticate the MS only, means one sided authentication but in mobile WiMax the technique for authentication is mutual authentication where BS authenticate MS and MS authenticate BS. The purpose of WiMax network is to expand the range and access of wireless systems. The existing security model is about the security association and security keys generation or establishment when the MS is entering the network range of a BS. The original model uses primary SA, Static SA and Dynamic SA at the start. In the proposed model shown in Figure 2, the Security associations are the same. Both models are using Authorization Key (AK) for authorization purpose. Other entities like KEK (Key Encryption Key) and the TEK are the same as in the original model. Just few of enhancements are done in the existing model to save memory, to get fast communication and to communicate securely. In the original model the MS uses X.509 certificates for authentication purpose. X.509 certificate is held by the MS, the public key of the MS is present in its digital certificate, which is used for access control, authentication and confidentiality. Here the WTLS certificate is proposed, instead of X.509 Certificate. The main difference between a X.509 certificate and a WTLS certificate is that WTLS has reduced size and also the processing speed, required in order to better go with the constraints imposed by narrowband radio link and the processing capacity in mobile equipment. The size of the serial number and issuer ID etc are reduced in the WTLS certificate as compared to X.509 certificate, which helps to avoid the usage of extra memory and save store memory. The original model is using a hashing technique named HMAC to make a secure communication but it doesn't provide message replay protection so here OMAC (One- Key message authentication code) which is an efficient hashing technique than HMAC can be also be used.

VII. CONCLUSION

This paper analyses the vulnerabilities in the basic authentication protocol of IEEE 802.16(e) alongwith various attacks on the PKM protocols. Here, the lift of the security level of the WiMax authentication is focused , and an authentication mechanism is developed to improve WiMax authentication by employing WTLS certificate instead of the X.509 certificate. The main difference between a X.509 certificate and a WTLS certificate is that WTLS has reduced size and also the processing speed.

REFERENCES

1. IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std 802.16-2004, http://www.ieee802.org/16/, 2004.
2. M. Barbeau, "WiMax/802.16 threat analysis," ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks, 2005, pp. 8–15.
3. IEEE Std 802.16e-2005, http://ieee802.org/16/published.html, 2005.
4. IEEE Standard for Local and metropolitan area networks Part 16:Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands , 2006.
5. Jukka Ylitalo, Tony Jokikyyny, Tero Kauppinen, Antti J. Touminen, Jaako Laine. "Dynamic Network Interface Selection in Multihomed Mobile Hosts" IEEE 2002.
6. IEEE Std. 802.16-2004: IEEE Standard for Local and Metropolitan Area Networks Part16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, 2004.
7. Whitfield Diffie and Martin E. Hellman: New Directions in Cryptography, Invented Paper.
8. Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka, Andreas Deininger :Security Vulnerabilities and Solutions in Mobile WiMAX, KDDI R&D Laboratories, 2-1-15, Ohara, Fujiminoshi, Saitama 356-8502, Japan.
9. Sanida Omerovic, "WiMAX overview", Faculty of Electrical Engineering, University of Ljubljana, Slovania.
10. D. Johnston and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 40-48, May-June 2004.
11. E. Kaasenbrood, "WiMAX Security - A Formal and Informal Analysis," Master's thesis, Eindhoven University of Technology, Department of Mathematics and Computer Science, Groningen, Netherlands, August 2006.
12. R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3280 (Standards Track), April 2002.
13. G. Lowe, "A Family of Attacks upon Authentication Protocols," Technical Report 1997/5, University of Leicester, UK, 1997.
14. M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication",Proceedings of the Royal
15. S. Xu and C. T. Huang, "Attacks on PKM protocols of IEEE 802.16 and its later versions," In Proceedings of 3rd International Symposium on Wireless Communication Systems (ISWCS 2006), Valencia, Spain, September 2006.

16. White Paper “Mobile WiMax Security” by Airspan Networks Inc. 2007.
17. Jamshed Hasan “Security Issues of IEEE 802.16 (WiMax)”,2006 Society of London, vol. 426, pp. 233-271, 1989.

AUTHORS PROFILE

Rajesh Shrivastava: He has completed his M.E. from R.G.P.V. Bhopal in Computer Science & Engineeting . His area of interest is security in mobile communications. He had published several research journals in international conferences. He is pursuing his P.hD. in mobile communication.

Deepsk Kumar Mehto: He is pursuing his M.E. from R.G.P.V. Bhopal in Software System. His area of research interest is wireless security & mobile computing.