International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Editorial Board

Mr. SANJAY ASATI
Dept of ME, M. Patel Institute of Engg. & Tech., GONDIA(M.S.)

Mr. G. Y. KUDALE
N.M.D. College of Management and Research, GONDIA(M.S.)

Editorial Advisory Board

Title

THE DESIGN OF A TRUSTED AUTHENTICATION SCHEME FOR WIMAX NETWORK

Author(s)

Mr. Rajesh Shrivastava
Asst. Professor,
Comp. Sci. & Engg. Deptt.,
Shri Ram Institute of Technology, Jabalpur

Deepak Kumar Mehto
M.E. (S.S.),
Shri Ram Institute of Technology, Jabalpur

Abstract:

As a promising broadband wireless technology, WiMAX has many salient advantages over such as: high data rates, security, and mobility. Many sophisticated authentication and encryption techniques have been embedded into WiMAX but it still exposes to various attacks in. IEEE802.16 provides a security sublayer in the MAC layer to address the privacy issues across the fixed BWA (Broadband Wireless Access). In this paper, we first overview the IEEE802.16 standard, and then investigate possible attacks on the basic PKMprotocol in IEEE802.16. We also give possible solutions to counter those attacks.

Key Terms: Wimax, , PKMv1,PKMv2, User Authentication etc.

Introduction:

Established by IEEE Standards Board in 1999, the IEEE 802.16 is a working group on Broadband Wireless Access (BWA) developing standards for the global deployment of broadband Wireless Metropolitan Area Networks. In December 2001, the first 802.16 standard which was designed to specialize point to- multipoint broadband wireless transmission in the 10-66 GHz spectrum with only a light-of-sight (LOS) capability. But with the lack of support for non-line-of-sight (NLOS) operation, this standard is not suitable for lower frequency applications. Therefore in 2003, the IEEE 802.16a standard was published to accommodate this requirement. Then, after being revised several times, the standard was ended in the final standard: 802.16-2004 which corresponds to revision D. These standards define the BWA for stationary and nomadic use which means that end devices cannot move between base stations (BS) but they can enter the network at different locations. In 2005, an amendment to 802.14-2004, the IEEE 802.16e was released to address the mobility which enable mobile stations (MB) to handover between BSs while communicating. This standard is often called “Mobile WiMAX .

Based on the IEEE 802.16 standard, the WiMAX (Worldwide Inter-operability for Microwave Access) is “a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access”[Wiki_WiMAX]. The WiMAX is supported by the WiMAX forum,

which is a non-profit organization formed to promote the adoption of WiMAX compatible products and services . WiMAX is a very promising technology with many key features over other wireless technologies [Jain08]. For instance, WiMAX network has the capability of working on many bands: 2.3 GHz, 2.5 GHz, etc, and provides scalability and mobility with high data rates with NLOS operation. It also provides strong security and strong QoS guaranteed services for data, voice, video, etc. However, in order for WiMAX to achieve a maturity level and become a successful technology, more research on security threats and solution to these threats need to be conducted.

The rest of the paper is organized as follows. Section 2 describes the Related work. Section 3 describes the vulnerabilities in IEEE 802.16. Section 4 describes solution and improvement. In section 5 analysis of the method is performed & finally section 6 concludes the paper. In last references are given.

Related Work:

From the publication of the first version of IEEE 802.16, a few papers have been published to introduce this new standard. In [5], Roger Marks gives a technical overview of 802.16. There are also some other papers and books that review this standard, such as [6] and [7]. However, few of them tackle the security issues. It is clear that so far WMAN has been less investigated than WLAN. With its great potential in the future's wireless service, WMAN deserves more attention than what it gets now.Since the publication of the IEEE 802.16 standard [1] in 2004 until so far, few research activities about the security of 802.16 have been published. The majority of these research activities addressed mainly the PMP mode and, particularly, the Privacy and Key Management (PKM) protocol. A new node, aiming to join the network and make use of the available resources, must go through the authorization and authentication process.

WiMAX security solutions:

By adopting the best technologies available today, the WiMAX, based on the IEEE 802.16e standard, provides strong support for authentication, key management, encryption and decryption, control and management of plain text protection and security protocol optimization.

In WiMAX, most of security issues are addressed and handled in the MAC security sub-layer as described in the fig:1. Two main entities in WiMAX -

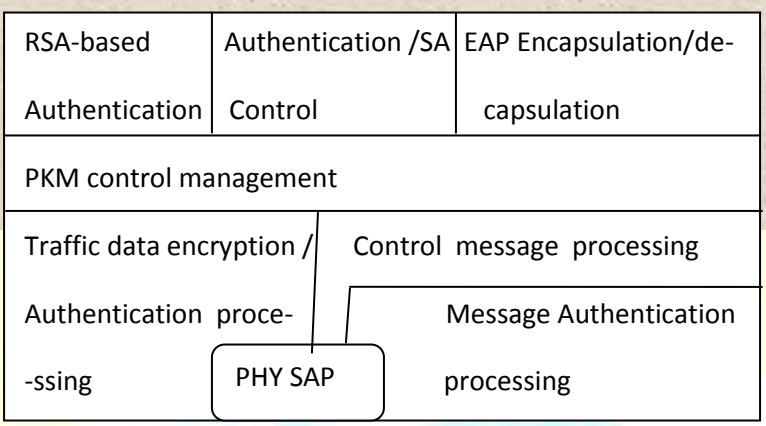

Fig 1. MAC Security sub layer

Including Base Station (BS) and Subscriber Station (SS), are protected by the following WiMAX security features:

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).

Public key infrastructure:

WiMAX uses the Privacy and Key Management Protocol (PKM) for secure key management, transfer and exchange between mobile stations. This protocol also authenticates an SS to a BS. The PKM protocol uses X.509 digital certificates, RSA (Rivest -Shamir-Adleman) public-key algorithm and a strong encryption algorithm (Advanced Encryption Standard - AES). The initial draft version of WiMAX uses PKMv1 which is a one-way authentication method and has a risk for Man-in-the-middle (MITM) attack. To deal with this issue, in the later version(802.16e), the PKMv2 was used to provide two-way authentication mechanism.

Device/User Authentication:

Generally, WiMAX supports three types of authentication which are handled in the security sub-layer. The first type is RSA-based authentication which applies X.509 certificates together with RSA encryption. The X.509 certificate is issued by the SS manufacturer and contains the SS's public key (PK) and its MAC address. When requesting an Authorization Key (AK), the SS sends its digital certificate to the BS, the BS validates the certificate, and then uses the verified PK to encrypt an AK and pass it to the SS. The second type is EAP (Extensive Authentication Protocol) based authentication in which the SS is authenticated by an X.509 certificate or by a unique operator-issued credential such as a SIM, USIM or even by user-name/password. The network operator can choose one of three types of EAP: EAP-AKA (Authentication and Key Agreement), EAP-TLS (Transport Layer Security) and EAP-TTLS MS-CHAP v2 (Tunneled Transport Layer Security with Microsoft Challenge- Handshake Authentication Protocol version 2. The third type of authentication that the security sub-layer supports is the RSA-based authentication followed by EAP authentication.

In fact, according to IEEE 802.16 [1], the authorization and authentication protocol (PKM) defines the exchange of a three messages: Authentication Information (Auth- Info), Authorization Request (Auth-REQ) and Authorization replay (Auth-RSP)

The overall exchanged messages are depicted in table I.

Message 1 (Auth info) SS→BS : Cert (SS, manufacturer)
Message 2 (Auth REQ) SS→BS :Cert (SS) Capabilities SAID
Message 3 (Auth RSP) BS→ SS : RSA Encrypt(Public key ($S) ,AK) | AK Lifetime AK seq no. SAID List

Table 1. Authentication protocol messages in 802.16

In table 1, Cert(SS. Manufacturer) is the X.509 certificate of SS's manufacturer, and Cert(SS) is SS's X.509 certificate. Capabilities are the SS supported authentication and data encryption

algorithms. RSAEncrypt(PubKey(SS),AK) is the Authentication key (AK) encrypted with the public key of the SS. The authors of [2]–[4] pointed out the limitation of the proposed PKM protocol, claiming to be vulnerable to replay and man-in-the middle (MiTM) attacks. To avoid replay attacks on messages Auth-REQ and Auth-RSP, the authors of [3], [4] proposed to add Timestamps, in messages 2 (Auth-REQ) and message 3 (Auth-RSP), to ensure the freshness and liveness of the exchanged messages. Also, in order to avoid messages forgeries and MiM attacks, authors of [3], [4] added to message 2 the SS signature, and to message 3 the BS certificate and signature. This will allow message 2 and 3 authentication and mutual authentication between the SS and the BS. The overall scheme proposed by [3], [4] is depicted in table II.

Messge 1 (Auth -info) SS → BS : Cert (SS ,Manufacturer) Message 2(Auth-Req)
SS → BS : Ts | Cert(SS) | Capabilities | SAID | $SIG_{SS}(2)$ Message 3(Auth- RSP)
BS → SS: Ts | Tb | RSA – Encrypt | (Pubkey | (SS),AK) Seq No. | Lifetime Seq No. SAIDlist Cert (BS) $SIG_{BS}(3)$

Table 2 . Revised 802.16 Authentication Protocol Message using Timestamps

In table 2, TS and TB are timestamps generated by SS and BS respectively. SIGSS(2) is the SS signature over Auth-REQ message and SIGBS(3) is the BS signature over Auth-RSP message. Cert(BS) is the BS X.509 certificate. Authors of [2] suggested that both SS and BS participate on Authentication key (AK) value derivation by sending nonces on the messages 2 and 3. The new AK derivation scheme will be based on SS and BS MAC addresses, exchanged nonces and a pre-AK value. This will avoid replay attacks and ensure both BS and SS about the liveness of the AK value. The whole proposed scheme is depicted by [2] .

In (2) , NS and NB represents the nonces generated by the SS and BS respectively. The pre-Ak is the pre-generated Authentication key which will be used in addition to nonces and MACs Address to derive the value of the AK by both the BS and the SS. The authors of [8] review the 802.16 standard, and analyze its security in many aspects, such as vulnerability in authentication and key management protocols, failure in data encryption, and lack of explicit definition. Mutual authentication is the major contribution to PKM protocols proposed by [8], which enables SS to authenticate BS as well. In fact, the need for mutual authentication in wireless network is not a novel topic. It has been widely studied in the scope of WLAN. In WLAN, WS needs to authenticate AP while AP authenticates WS. However, the authentication and key management protocols in 802.11 and 802.16 are based on different methods. IEEE 802.11 applies the shared-key authentication method, while IEEE 802.16 is based on publickey authentication algorithm, specifically, X.509 certificate.Therefore, the authentication and key management in IEEE

802.16 needs separate study.

Vulnerabilities in IEEE 802.16 :

This section explains vulnerabilities found in Mobile WiMAX by our analysis. These vulnerabilities are:

• **Unauthenticated messages:**

Mobile WiMAX includes some unauthenticated messages. Their forgery can constrict or even interrupt the communication between mobile station and base station.

• **Unencrypted management communications:**

The complete management communication between mobile station and base station is unencrypted. If an adversary listens to the traffic, he can collect lots of information about both instances.

• **Shared keys in the multi- and broadcast service:**

For symmetric traffic encryption, the multi- and broadcast service in Mobile WiMAX shares keying material with all group members. This introduces the Vulnerability that group members

can forge messages or even distribute own traffic keying material, thus controlling the multi- and broadcast content.

Solution & Improvement :

Privacy & KeyManagement Protocol version 1

The PKM v1 protocol complies with the 802.16d-2004 standard and is operating in the Fixed WiMAX networks [9[. This protocol is a 3-step protocol which involving 1-way authentication. The figure 1 shows the PKM v1 authentication model and messages involved. The detailed operation of PKM v1 can be found in [9], [10] and [4]. PKM v1 is based on X.509 certificate based Public Key Infrastructure (PKI). The individual components of the message have been addressed in [9] and [4].

Privacy & Key Management Protocol version 2

PKM v2 protocol was defined in 802.16e-2005 and is implemented in Mobile WiMAX networks [9]. This protocol is not essentially a variant of PKM v1. PKM v1 and v2 share a common service authorization structure. PKM v2 is a 4-step, 3-way authentication protocol. The operational mechanism of PKM v2 is illustrated in [11] and [12]. The major enhancements in PKM v2 are the inclusion of digital certificates and authorization acknowledgement step.

We can describe the Attacks on authentication by the way which a network can be intruded and the privacy of the users be compromised. The secure access of network services is becoming an important issue in the present communication infrastructures. Any attempts of an intruder to get registered with the network illegitimately or to create chaos in it, is possible; if the user authorization and authentication is compromised.

The security architecture of previous IEEE 802.16d standard is based on PKMv1 (Privacy Key Management) protocol, but it has many security issues like rouge BS introduction. Most of these issues have been resolved by the later version of PKMv2 protocol in IEEE 802.16e standard. IEEE 802.16e provides a flexible solution that supports device and user authentication

between a MS and the home connectivity service network (CSN) to solve the rouge BS issue. Both fixed and mobile WiMAX have two-component protocols:

(i) An encapsulation protocol for data encryption and authentication algorithms,

(ii) A key management protocol (PKMv2) providing the secure distribution of keying data from the BS to the MS. MS will send the ranging request (RNG-REQ) message in a specified contention slots. Once the BS receives the RNG_REQ, it informs the frequency, time and power offset values in the RNG_RSP message. If any collisions occur in a contention slot, BS sends the failure notification in the RNG_RSP message and the message will repeat the ranging process. Once the MS succeeded in ranging process, it negotiates for basic capabilities in the SBC_REQ and the SBC_RSP messages. The subsequent process, Extensible Authentication Protocol (EAP) based authentication is described below.

***EAP based Authentication*:** Authentication addresses establishing the genuine identity of the device or user wishing to join a wireless network. The Device and User Authentication using EAP provides support for credentials that are subscriber ID module (SIM)-based, universal SIM (USIM)-based or X.509 Digital Certificate. The message flows in EAP-TTLS (Tunneled Transport Layer Security) based authentication is

shown in Figure 1. The authenticator in access network gateway (ASN GW) sends an EAP Identity request to the MS and the MS will respond to the request by sending PKM-REQ (PKMv2 EAP-Transfer) message. PKM-REQ message contains the subscriber ID module or X509 certificate. Then ASN GW forwards PKM-REQ to AAA server over radius protocol. The AAA server authenticates the device and provides the master session key (MSK) in an EAP-TTLS protocol. Then it forwards MSK to the authenticator. The authenticator generates AK from MSK and forwards to the BS. At the same time MS also generates the same AK from MSK. Now the BS and MS can mutually authenticate each other

using AK.

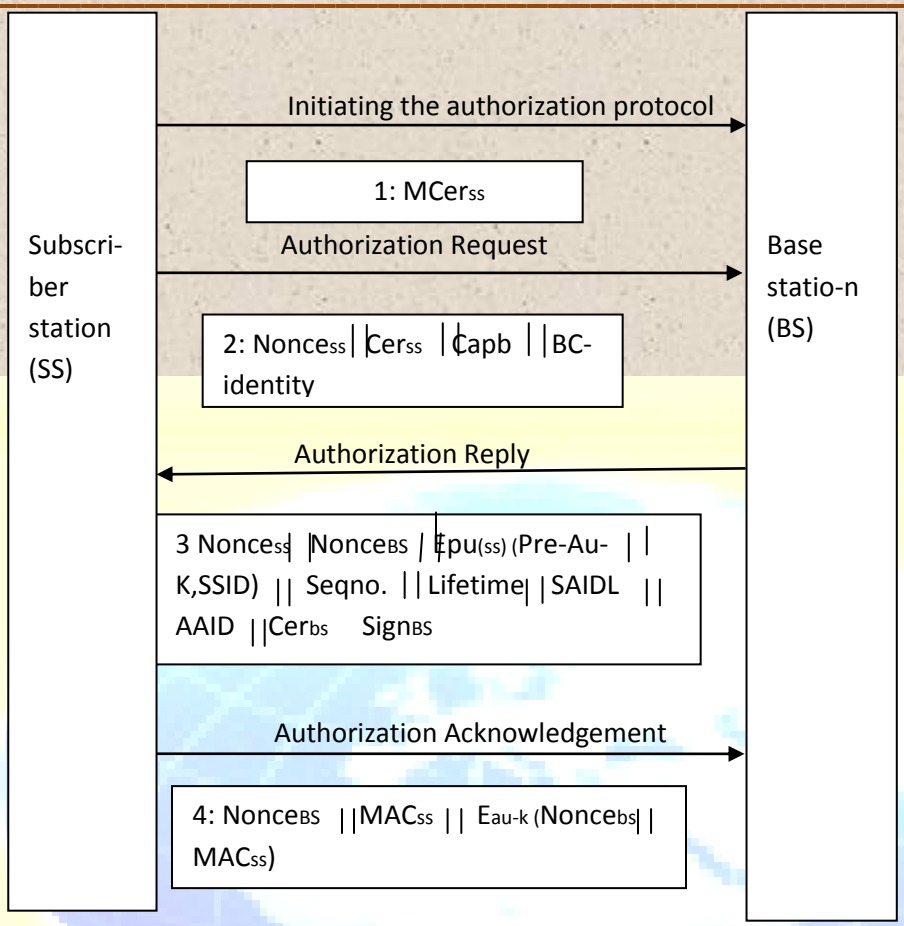

Fig 2 : Authorization protocol of PKM V2 Protocol

Only in message 3 of Figure 2, digital signature is sent to SS from the BS. Nonce is a good option for avoiding attacks in authorization protocol rather than using timestamp only. Systems should be synchronized before using timestamp. But timestamp can be a better option than nonce to prevent replay attacks. In this case, the security depends on resynchronization schemes, system clocks and methods which are used for synchronizing these clocks. It will also create the storage overhead for maintaining the timestamp table. Nonce is random, so it is very difficult to produce the same nonce in the replay attack. The attack can be prevented by adding signatures in message 2. Attack that is defined and presented by researchers in [3, 13, 14] is called an interleaving attack. The authors in [3] changed the protocol PKM for these attacks and used timestamp instead of nonce. The solution proposed in this paper can avoid both attacks; interleaving and replay. As in interleaving attack on PKMv2, intruder gets message 2 and sends

it to the BS. BS replies with its own nonce and other related information encrypted with the public key of SS. Signatures are also attached with reply message from BS. Then intruder forces SS to communicate with it. Intruder sends the same message to SS which BS sent to intruder. SS will decrypt this message as it was encrypted with its public key. The same response, that intruder gets from the SS will be sent to the BS in order to complete the authorization protocol. Using sequence numbers in message 2 of Figure 3 can be a better option but this protocol will become complicated. But for obtaining better security, as described in this paper, nonce and timestamp both should be used in parallel. Timestamp will guarantee that it is a fresh message and nonce will assure that it is a reply of previous message and ensure that if attacker synchronizes his clock with the SS or BS still he will not be able to get nonce. The changed and proposed authorization protocol is shown in Figure 3.

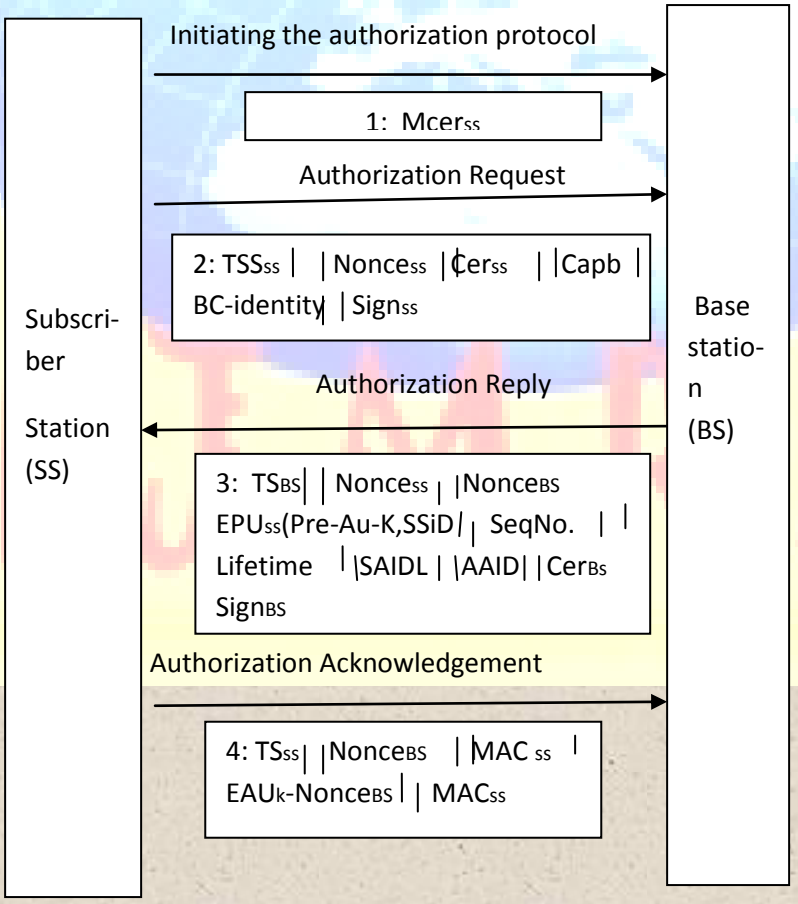

Fig 3 : New proposed protocol using hybrid Approach

Using timestamp as proposed by the author in [3], has an advantage that fewer messages are exchanged between SS and BS than nonce scheme. Security relies on timestamp only. Li Gong [15] clearly states that it is very difficult to ensure perfect synchronization at all times. The author proves that even after resynchronization, the fault remains in system clocks and so systems are vulnerable to suppress replay attack. The solution provided in this paper would prevent systems from these attacks because using proposed hybrid approach, security is not only dependent on timestamp but also on nonce. Nonce linked exchanged messages and timestamp is used to prevent from interleaving attack in proposed solution.

Algorithm for proposed approach:

Now the steps of algorithm are presented below of the proposed scheme to highlight the idea.

1. Request for authentication from SS to BS

   i. Initializing the authorization protocol

   ii. Sending its manufacturer's certificate to BS for validity check

2. Request for AK from SS to BS and authentication of SS

   i. Security parameters including digital certificate.

   ii. Nonce created by SS.

   iii. Timestamp attached by SS when message is delivered to BS.

3. Reply for AK from BS to SS by completing mutual authentication

   i. Encrypted Authorization Key with other security parameters.

   ii. Nonce sent by SS in step 2.

   iii. Nonce created at BS.

   iv. Timestamp from the BS's system at the time of message delivery.

4. Acknowledgment and verification for getting AK

   i. Nonce created at step 3 is encrypted with AK with other defined security parameters in PKMv2 protocol.

ii. Nonce sent by BS in step 3.

iii. Timestamp is created in acknowledgment message by SS.

More precisely, the scenarios are explained by involving an attacker into the message flows. Referring to the Figure 3, an attacker sends message 2 to the BS claiming to be the valid SS. The same message 2 is previously sent by the SS to BS. In the response of this message 2, BS replies an attacker with message 3. In message 3 AK is encrypted using the public key of SS and it has to be decrypted with the private key of SS. Attacker does not have the private key of SS so he cannot decrypt the message. What attacker can do is, he can send the message to the SS for decryption. SS decrypts the message 3 and sends back to the attacker. Now the attacker has the message to complete the message exchange procedure with the BS for acquiring AK. By using the timestamp as explained by the Sen Xu and Chin-Tser Huang in [3], the attack can be avoided. Message will not be replayed after adding the timestamp to BS.

Analysis & Discussion:

Most of the management messages defined in IEEE 802.16e are integrity protected. But some messages are not covered by any authentication mechanism. This introduces some vulnerability BS will face replay attack from malicious SS, whointercepts and saves the messages sent by a legal SS previously. We name this attack Replay Attack. In [16], when analyzing Kerberos Protocol, the authors claim it is common for designers not to focus on such kind of attacks. They regard it as vulnerability but not serious flaw. However, we find it is not the same situation for PKM Protocols in IEEE802.16, in which it may lead to a severe result. The reason is that, if BS set a timeout value which makes itself to reject Auth-REQ from the same SS in a certain period, the legal request from the victim SS will also be ignored. Therefore, the Deny of Service occurs to the victim SS. Otherwise, if BS accept the request, it will have to generate new AK for SS, which usually involved nonce information. This will exhaust BS' capabilities. To avoid these replay attacks, we suggest adding timestamps. The nonce and timestamp are used in the proposed protocol to prevent the replay & interleaving attack. The nonce will wipe out the possibility of replay attack. If an intruder copies the message and sends it to the BS, the BS can easily reject that message because that nonce value is in his/her buffer list. The nonce helps the

BS to identify successive requests and it enhances the BS capacity to reject those requests which was sent by the intruders or adversaries. BS, thus, can identify the latest requests and it is able to filter out samples of replay attacks, saving him/her from exhausting the resources. The adversary cannot do anything with the message which is sent by the actual MS. The timestamp helps the BS in identifying the latest requests, which prevents reply attacks. It also helps the MS to identify the recent messages, and hence it can identify the AK used by the MS as new or not.

Conclusion:

This paper analyses the vulnerabilities in the basic authentication protocol of IEEE 802.16(e). The analysis of both versions of key management including PKMv1 and PKMv2 indicates that PKMv2 provides better security as compared to PKMv1. There were many flaws in PKMv1 that were handled in PKMv2. Nonce are used in the proposed user authentication method to prevent the replay and interleaving attack. By using nonce and timestamp together, both replay and interleaving attacks can be prevented.

Building defence against additional attacks without causing much overhead is a challenging task for further research.

References:

- "IEEE Standard for Local and Metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001), Oct 2004.
- D. Johnston and J. Walker, "Overview of IEEE 802.16 security," Security & Privacy, IEEE, vol. 02, no. 3, pp. 40–48, May-June 2004.
- S. Xu and C.-T. Huang, "Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions," Wireless Communication Systems, 2006. ISWCS '06. 3rd International Symposium on, pp. 185–189, 6-8 Sept. 2006.
- S. Xu, M. Matthews, and C.-T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16," in ACM-SE 44: Proceedings of the 44th annual Southeast regional conference. New York, NY, USA: ACM, 2006, pp. 113–118.

- A. Marks, "A technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access", IEEE C802.16-02/05, 2002.
- IEEE 802.16 and WiMax: Broadband Wireless Access for everyone, Intel White Paper, 2004.
- Daniel Sweeney, WiMax Operator Manual: building 802.16 Wilreless Networks, Apress, 2005.
- D. Johnston, and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security & Privacy, 2004.
- IEEE Computer Society and the IEEE Microwave Theory and Techniques Society," 802.16TM IEEE Standard for local and metropolitan area networks," Part 16: "Air Interface for Fixed Broadband Wireless Access Systems", June 2004.
- R. M. Hashmi et, "Improved Secure Network Authentication Protocol (ISNAP) for IEEE 802.16", Proceedings of 3rd IEEE International Conference on Information and Communication Technologies, August 2009.
- IEEE Std. 802.16e/D12, "IEEE Standard for Local and Metropolitan Area Networks", part 16:" Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE Press, 2005.
- Ayesha Altaf, M. Younus Javed, Attiq Ahmed, "Security Enhancements for Privacy and Key
- Management Protocol in IEEE 802.16e-2005", 9th ACIS International Conference on software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp. 335-339, 2008.
- Burrows, M., Abadi, M., and Needham, R. M,"A Logic of Authentication", Proceedings of the Royal Society of London A, vol.426, pp. 233-271, 1989.
- Gavin Lowe ,"A Family of Attacks upon Authentication Protocols", Department of Mathematics and Computer Science, University of Leicester, January, 1997.
- Li Gong , "A Security Risk of depending on Synchronized Clocks", ORA Corporation and Cornell University, September 24, 1991.
- M. Abadi and R. Needham, "Prudent Engineering Practice for Cryptographic Protocols", IEEE Transactions on Software Engineering, 1995.