International Journal of Computing and Network Technology

@ 2013 UOB
SPC, University of Bahrain

Analysis of Attacks in Authentication Protocol of IEEE 802.16e

Kamran Sameni[1], **Nasser Yazdani**[2], **Ali Payandeh**[3]

[1] *University of Tehran: Kish International Campus IT and Computer Engineering Department, Tehran, Iran*
Email Address: k.sameni@ut.ac.ir

[2] *University of Tehran: Electrical and Computer Engineering Department, Faculty of Engineering, Tehran, Iran*
Email Address: yazdani@ut.ac.ir

[3] *University of Tehran: Kish International Campus IT and Computer Engineering Department, Tehran, Iran*
Email Address: payandeh@mut.ac.ir

Received: 6 Nov. 2012, Revised: 20 Nov. 2012. 2012; Accepted: 2 Dec. 2012

Abstract: Security support in wireless systems is a vital necessity to protect users and network in some applications. Since wireless media are available to all, attackers can easily reach the network and network will be more vulnerable for users and service providers of the network. This article discusses on the analysis of PKM (Privacy Key Management) protocols and its second version (PKMv2) which has been proposed after publication of IEEE 802.16e. This protocol is vulnerable against some attacks. In this article, standard security sub layer (IEEE 802.16) is first studied and then, WiMAX authentication protocol is explained. Finally, possible attacks to PKM Protocol in IEEE 802.16 will be studied. Also, solutions presented against relevant attacks are explained. Analysis of security mechanisms in authentication protocol and comparing between them is the main objective of this paper. In fact, this paper can be used as guidelines for the future research activities and security of WiMAX.

Keywords: Security, Authentication Protocol, Attack, IEEE 802.16

I. Introduction

WiMAX is of growing wireless broadband technology which is based on IEEE 802.16 standards. [1]

In security sub layer, WiMAX media access control layer defines fixed security mechanism with IEEE 802.16d standard and mobile networks security mechanisms with IEEE 802.16e standard.

In the beginning, security architecture of IEEE 802.16d standard, based on PKMv1 Protocol, had faced problems. Many of these problems were resolved in the next version of PKM Protocol in IEEE802.16e standard. The new standard causes a type of flexibility which supports validity of the device and user between a Mobile Station (MS) and Domestic Communication Service Network (CSN).

Various methods have been presented to remove security flaws existed in standards, but lack of a comprehensive view of all solutions and comparing them is evident. Comprehensive presentation for researchers is important, based on which, they can identify basic and effective problems and also can probably present more effective security mechanisms in future. [1]To understand WiMAX security issues, it is necessary to study WiMAX architecture and how to create a security profile in WiMAX at first.

In this part, background and detailed information is presented on the security specifications of WiMAX in security sub layer .In Part 2, security solutions will be discussed. Then, WiMAX authentication protocol will be explained in Part 3. At the end, attacks to the authentication protocols will be analyzed and PKM Protocols will be compared in terms of various security and attacks.

A. IEEE 802.16 Protocol Architecture

IEEE 802.16 Protocol Architecture has been composed of two main layers. Media Access Control layer (MAC) and Physical Layer which have been shown in Fig.1 [2]

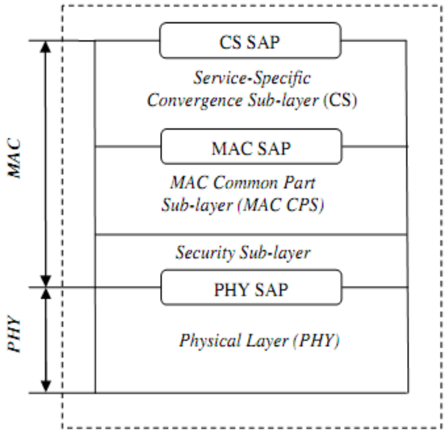

CS SAP
Service-Specific Convergence Sub-layer (CS)
MAC SAP
MAC Common Part Sub-layer (MAC CPS)
Security Sub-layer
PHY SAP
Physical Layer (PHY)
MAC
PHY

Figure 1. Structure of IEEE 802.16 Protocols [1]

MAC layer includes three sub layers. Convergence Layer Service (CS) is the first sub layer which maps higher-level data services to the communications and media access control layer (MAC).

Common Part Sub-Layer (CPS) is the second layer which is considered as standard kernel and has been integrated severely with a security sub-layer. This layer defines rules and mechanism to achieve this system, allocation of bandwidth and management of the relationship. Data units of MAC (Media Access Control) Protocol are created in this sub layer. Security sub layer is the last sub layer of MAC layer which has been located between two layers of MAC and physical layer and considers authentication, changing and creating key, encoding and decoding data transferred between the two MAC and physical layers. [2]

In the physical layer, there is a two-strain mapping between data units of MAC Protocol and forms of physical layer while receiving and transmitting is performed from code and modulation of radio frequency signals.

II. WIMAX SECURITY SOLUTIONS

WiMAX based on IEEE 802.16e standard has provided a strong support in validation, key management, encoding and decoding, managing and controlling simple texts and optimizing security protocol. MAC sub layer is described according to the Fig.2. [2]

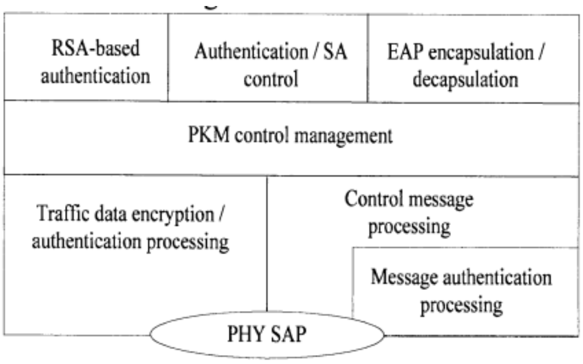

RSA-based authentication
Authentication / SA control
EAP encapsulation / decapsulation
PKM control management
Traffic data encryption / authentication processing
Control message processing
Message authentication processing
PHY SAP

Figure 2. MAC Security Sub layer [2]

BS1 and ***SS2*** are WiMAX two major attributes which are supported with the following security features: [3]

A. Security Association

Security Association (***SA)*** is a set of security data parameters which shares a ***BS*** and one or more SSs of customer. Each of SAs owns its feature (SAID). In addition, each of SAs enjoys one suitable hiding feature (for the selected algorithms), Traffic Encoding Keys (TEKs) and the initial vectors.

B. Public Key Infrastructure

WiMAX uses key management protocol and privacy policy in order to manage safety key, transfer and exchange between mobile stations. Also, this protocol authenticates SS to BS. PKM Protocol uses digital certificate (X.509), Public Key algorithm (RSA) and one Accurate Encoding Algorithm (AES). WiMAX initial version was used PKMv1 which is a unidirectional and risky authentication method against MITM attacks. To solve this problem in the next version, PKM2 was used for providing mutual authentication mechanism.

Fig.3 presents an overview of public key structure in WiMAX.

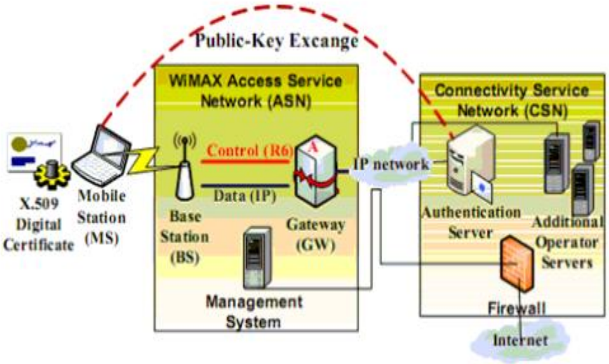


Figure 3. Public Key Structure in WiMAX [2]

C. Authentication of Device/User:

Generally, WiMAX supports three types of authentications, all of which are controlled in the security sub layer. Authentication based on RSA is of the first type which uses X.509 certificate along with encoding RSA.

X.509 certificate is issued by SS manufacturer and includes SS public key and its MAC address. If an authentication key is requested, SS will send its digital certificate to BS and BS confirms this certificate and uses approved PK for encoding AK and transferring it to SS.

Authentication of EAP type is of the second type, in which, SS is authenticated by X.509 certificate or with a unique operator certificate like SIM, USIM and/or even with user name and password. The operator of network can select one of three types of EAP: EAP-AKA, EAP-TLS and/or EAP-TTLS MS-CHAP v29.

- EAP-AKA: for authentication based on SIM
- EAP-TLS: for authentication based on X.509
- EAP-TTLS for MS-CHAP v2 (Microsoft-Challenge Handshake Authentication Protocol)

EAP-TLS security architecture has been defined in RFC 5216 and it remains stable as long as user understands invalid warnings of potential credit. [4]

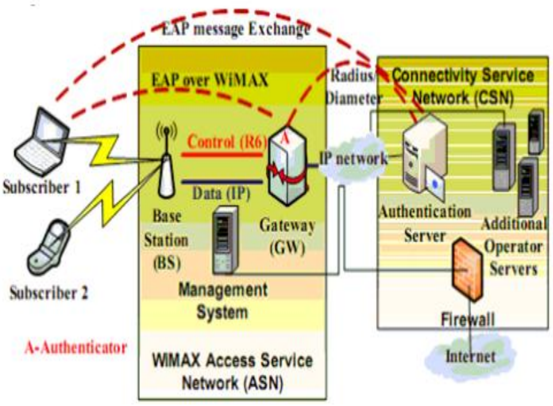


Figure 4. Authentication Based on EAP [2]

Authentication based on RSA is of the third type of authentication which is supported by the security sublayer.*Fig.4 shows general structure of EAP-based authentication in WiMax.*

Developing domain and accessing wireless systems is the main objective of WiMAX network. The existing security model is related to the security organization and formation or production of security keys. This model shows main key elements entitled “identities”.

X.509 certificate is kept in MS and MS public key exists in its digital certificate which is used for confidentiality, authentication and access control. [5]MS uses its general key to establish relationship with BS.

When MS is authenticated, a request message to determine license is sent to BS. Under such circumstances, BS produces an AK (license key) which owns sequence number and lifetime and sends it as coded form to MS (by MS general key which enjoys a sequential number between 0 to 15). AED-Building technique, used in this model, is called HMAC which does not carry out protection against repetition of message. Another key, which is named Key Encoding Key (KEK), is used for encoding operation. Both KEK and HMAC are calculated through AK. Finally, TEKs are produced and KEK encodes these TEKs at the time of replying TEK request. When TEK is obtained, data and information exchange will be started and communication will be formed. [6]

III. Authentication Protocol in IEEE 802.16

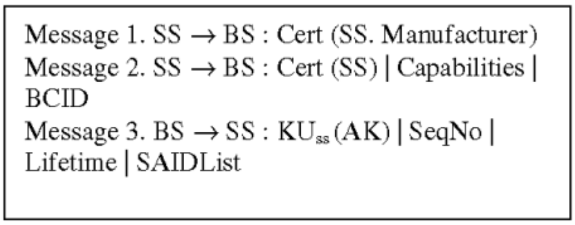
WiMax has been carefully designed with the security but it is still vulnerable against various attacks. Authentication of user of this case is a request for AK and also for SA identifier (SAID) in order to give reputation of user. Authentication request includes X.509 certificate related to MS and encrypting algorithm and hiding ID. In the same direction, BS executes required credit through establishing interaction with AAA server in the network and sends back reply of authentication request which contains AK encrypted with the general MS key.

After initial authentication of AAA, BS will authenticate MS again periodically. [4]

In this part, we will study security issues in WiMax Authentication Protocol. One SS starts authentication through sending authentication information message which includes SS manufacturer X.509 certificate. BS is authorized not to recognize it. Then, SS transmits authentication request (Auth-REQ) message for its BS. [7]

In response to Auth-REQ, BS studies requester’s SS identifier, i.e. it decides that encrypting protocols and algorithms, which should be shared with SS, are valid or not.

Therefore, an Authentication Key (AK) is created and AK is transmitted to SS. The Authentication Protocol has been shown in Fig.5. [7]



Message 1. SS → BS : Cert (SS. Manufacturer)
Message 2. SS → BS : Cert (SS) | Capabilities | BCID
Message 3. BS → SS : KU_{ss}(AK) | SeqNo | Lifetime | SAIDList

Figure 5. Scenario of Authentication Protocol in 802.16 [7,8]

In Fig.5, Cert (SS) is X.509 certificate related to SS. In BCID, CID is SS base which equals to its initial general key. KUss (AK) is the authentication key which has been coded with SS general key. Seq. No. (Sequence Number) is a four-bit number for AK and lifetime gives the second number before AK is expired. SAID list includes SA features and IDs which has been authenticated with SS in order to obtain key information. Fig.6 [7] shows layers of user authentication protocols (PKMv2). PKMv2 transfers EAP with aerial connection of IEEE 802.16 between MS and BS in ASN. Depending on the confirming place of L/C in ASN, one BS can send EAP messages with authentication reply protocol for conforming validity.

In response to confirming the validity, AAA client hides EAP in AAA protocol envelopes and sends them with one or more AAA proxies for AAA server to CSN (customer service network). [7]

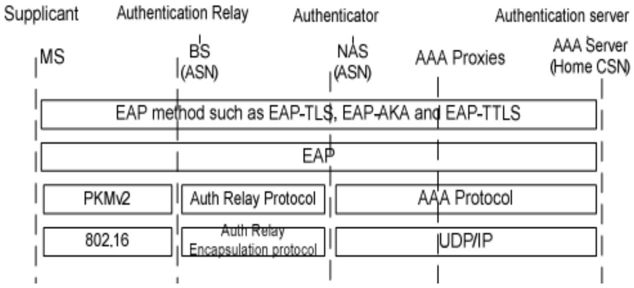


Figure 6. User Authentication Protocols PKMv2 [7]

A. *Authentication Threats*

Threat of Deformation: The deformation attack is a type of attack, in which, one system takes into account ID of the other system. WiMAX supports one-sided level authentication which is based on RSA/X.509 certificate. [8]

Certificate can be certified by the manufacturer in a machine code. So, stealing and misleading can make this attack possible. There are two ways to perform the attack:

- Rogue BS Attack
- ID Theft

ID Theft: attacker embarks on coding the device again with the hardware address of the other device. This address can be stolen by the intruding management messages. [8]

Rogue BS Attack: SS can be endangered with a counterfeit BS which simulates an actual BS. The counterfeit BS carries out an activity so that SS imagines that they have established with an actual BS. So, this activity can lead to the penetration in whole SS data. [8]

In IEEE 802.16 with using PKMv1, lack of mutual authentication will prevent from approval of BS authentication and gives the possibility of personal attack among (MITM) in faked BS. Although actualizing this type of attack completely in WiMAX, which takes advantage of mutual authentication through using PKMv2, is difficult, with using new version of PKM, WiMAX has removed many of these deficiencies such as vulnerability against MITM due to the lack of mutual authentication. However, PKMv2 has vulnerabilities against new attacks.

IV. Analysis of Attacks to Authentication Protocols (PKMv1) and Its Subsequent Version (PKMv2)

Various threats are caused by WiMAX Authentication Protocol, in which, attacks and deformations in PKM Authentication Protocol are of the most important threats.

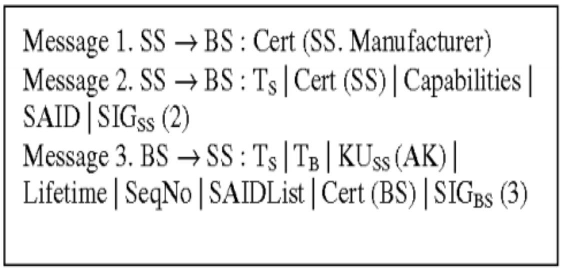
A. Types of Attack to PKMv1

BS faces with reply attack of enemy SS side which saves message sent by an actual SS and penetrates into it. [7]

The name of this attack is "Simple Reply Attack". This attack has been named simply for this reason that this reply attack carries out distortions merely in message. [7]

As it was mentioned in [9], when we were studying Kerberos Protocol, the author was claiming that designers usually pay less attention to this type of attack and do not focus on it. They refer to it as "vulnerability", not as a serious defect. However, this has the same conditions of PKM protocols in IEEE 802.16. Its main reason is this that if BS sets a number for termination of time, legal request from victimized SS will be ignored as well. So, the service, which will be occurred in victimized SS, will be ignored, otherwise, if request is accepted by BS, it will force to make a new AK for AK which usually includes nonce information. This activity can weaken BS capabilities. To avoid these reply attacks, it is proposed that timestamps should be added along with signs of SS in message 2. [7]

Similarly, message three (3) puts SS at risk against reply attacks. Even, enemy BS can make its Auth-REQ message with its AK. This attack is a type of MITM attack which requires mutual authentication. Namely, SS requires authenticating the BS. This activity can be fulfilled with adding BS certificate in message three (3). The modified protocol is shown in Fig.7. [7]



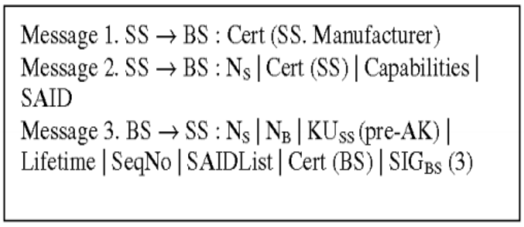
Message 1. SS → BS : Cert (SS. Manufacturer)
Message 2. SS → BS : T_S | Cert (SS) | Capabilities | SAID | SIG_{SS} (2)
Message 3. BS → SS : T_S | T_B | KU_{SS}(AK) | Lifetime | SeqNo | SAIDList | Cert (BS) | SIG_{BS} (3)

Figure 7. Modified Authentication Protocol [7]

In Fig.7, TS and TB are the timestamps as created by SS and BS. SIGss is SS signature in message two (2) while SIGBS is the signature of BS in message three (3).

B. Attack to PKM, Intel Nonce Version

Nonce is a suitable choice for timestamp of authentication protocol. In [10], authors have used nonce instead of timestamp. This protocol has been shown in Fig. 8.



Message 1. SS → BS : Cert (SS. Manufacturer)
Message 2. SS → BS : N_S | Cert (SS) | Capabilities | SAID
Message 3. BS → SS : N_S | N_B | KU_{SS} (pre-AK) | Lifetime | SeqNo | SAIDList | Cert (BS) | SIG_{BS} (3)

Figure 8. Authentication Protocol with Nonce [10]

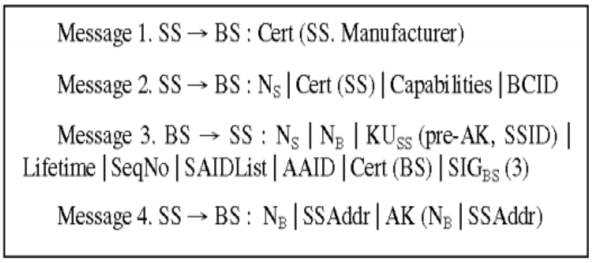
However, using nonce(s) merely ensures SS that message three (3) is its request reply. Also, BS may be at the risk of reply attack, because BS cannot tell whether message 2 has been sent newly and/or is merely the message of reply.

Personal attack is one the most important security defects in determining unilateral identity which identifies SS in BS merely. But, SS has no way of knowing this issue. This defect in plan can prepare protocol to be prone to the counterfeiting attacks, in which, licensed BS can establish relationship with SS. Bilateral identification can remove this vulnerability, i.e. SS should identify BS as well. This affair can be realized by adding certified BS in message three (3). [5]

C. PKMv2 Protocol

IEEE 802.16e proposes PKMv2, in which, an additional message has been added at the end of original protocol. This protocol is shown in Fig.9 [7].

SSID is identifier of SS from cert (SS) and AAID is also identifier of Authorized Association (AA) while SSAddr is the address of MAC related to SS.



Message 1. SS → BS : Cert (SS. Manufacturer)

Message 2. SS → BS : N_S | Cert (SS) | Capabilities | BCID

Message 3. BS → SS : N_S | N_B | KU_{SS} (pre-AK, SSID) | Lifetime | SeqNo | SAIDList | AAID | Cert (BS) | SIG_{BS} (3)

Message 4. SS → BS : N_B | SSAddr | AK (N_B | SSAddr)

Figure 9. Authentication Protocol for PKMv2

In fact, three are three selective protocols for X.509 certificate. (1. Unilateral Authentication, 2- Bilateral Authentication and 3- Tripartite Authentication)

Although IEEE 802.16 original authentication protocol has two messages, it is yet considered as unilateral authentication, because, it provides only SS certificate for BS. The modified version and Intel Nonce version are considered as bilateral authentications. PKMv2 is regarded as tripartite authentications which has a confirmed message from SS to BS. [7]

Both timestamp and nonce are used in X.509 certificate. For this reason, timestamp is not used as a type of nonce in X.509; rather, it is used as lifetime that includes start time (optional) and end time in order to avoid sending with delay. So, one nonce, which is a sole lifetime, is used to prevent from reply attack. In [7], it was mentioned that timestamp is vital for unilateral and bilateral protocols. SS signature is necessary to avoid distorting and replying provided that timestamp has been inserted in X.509 and also in modified 902.16 authentication protocol.

In tripartite authentication, nonce NB is included at the last message from SS to BS. It seems that checking timestamp is not necessary, because, nonce of each two parts is sent for other. So, each two parts checks nonce of mutual side to prevent from reply attack. This method is usually used when there is not clock synchronization.

For the abovementioned reasons, it is claimed that BS does not require checking TS timestamp[11]. However, several defects have been found by researchers, for example, in [7], it has been shown that troublemaker can respond request message to BS and misuse from the SS. Therefore, if the protocol is not designed properly, it can be at the risk of attack as well.

D. Decision-Making Keys to Re-Identify in PKMv2

When applicant MS, which is defined by IEEE 802.162 standard, starts getting access to network and when AK survival time was expired, it can execute re-identification path. Then, AK lifetime is a key factor in order to set the date for starting re-identification path. According to the different identification methods in PKMv2, there are five (5) different ways to produce AK which is led to the complexity of AK lifetime: [12]

1) AK Lifetime

According to the definition of AK lifetime in IEEE 802.16e standard, we can see that: MIN=AK (PKM lifetime, PAK lifetime)

That is to say that AK lifetime equals to the least amount between two PAK lifetime (if existed) and PMK lifetime (if existed).PAK is always produced with RSA method while PKM is always produced with EAP method. The AK production method will be divided into five (5) groups through different identification methods as follows: [12]

a) Single PKMv2 RSA Identification Method

AK <=Dot16kdf(PAK,SSMAC Address|BSID|PAK|"AK",160)

Wherein, AK is produced only for identification of RSA. Under such circumstances, MIN is equal to AK (MIN=AK) (PAK lifetime), namely, when PAK is expired, identification will be executed again.

b) Single EAP PKMv2-Based Identification Method

AK <=Dot16kdf(PMK,SSMAC Address|BSID|"AK",160)

Wherein, AK is produced only for EAP-based identification. Under such circumstances, MIN is equal to AK (PMK lifetime). Namely, when PMK is expired, identification is executed again.

c) Method of EAP + EAP Identification (Identified)

AK<=Dot16kdf(PMK+PMK2,SSMAC ddress|BSID|"AK",160)

Under such circumstances, AK is produced merely because of PMK and PMK2.

At the first turn, PMK is produced through EAP-based identification method while PMK2 is a key which is produced through EAP-based identification method in the second turn. Although two PMKs are produced in two turns, AK lifetime is merely because of PMK. The lifetime equals as follows: MIN=AK (PMK lifetime), namely, when PMK is expired, re=identification will be executed.

d) EAP+RSA Identification Method (Identified)

AK<=Dot16kdf(PAK+PMK,SSMACAddress|BSID|PAK|"AK",160)

In this method, implementing common identification of PKMv2 RSA is done at the first step which leads to PAK. Then, identified EAP is executed as common identification of user in order to produce PKM. AK is determined jointly by PAK and PMK. Then, lifetime is equal to MIN=AK (PAK lifetime, PMK lifetime). Namely, updating AK is as a result of the first key information of initiator. When AK is expired, re-identification will be observed.

e) EAP- and RSA-Based Identification Method

According to 8-bit binary value in the field of “Supporting Policy of Identification), which is observed in SBC-REQ/SBC-RSP messages, this integrated method (comprised of EAP+RSA-based identification method) will never execute in initial entry identification method.

According to the explanation extant in IEEE 802.16e standard, during MS period:

AK <=Dot16kdf(PAK,SSMAC Address|BSID|”AK”,160)

Before MS departure, AK is produced by RSA method. The lifetime is equal to MIN=AK (PAK lifetime). If MS leaves its place and moves towards another BS field, reentrance will be able to execute EAP-based authentication. Then,

AK <=Dot16kdf(PMK,SSMAC Address|BSID|”AK”,160)

This situation is very similar to the single EAP-based method and lifetime is equal to MIN=AK (PMK lifetime).

In fact, we can observe EAP+RSA-based method as two single RSA-based and EAP-based methods with this difference that EAP-based method can be occurred merely at MS reentry in the field of one another BS.

In security terms, IEEE 802.16e, related to AK, contains one 32-bit HMAC/CMAC_PN_U and one 32-bit HMAC/CMAC+PN_D which sets scheduled re-identification date. We show them with H/CMAC_PN*, in which, HMAC_PN_U is counter of relevant number for communication from ground station to satellite. In the same direction, HMAC_PN_D is used for communicating from satellite to the ground station.

In telecommunication links (ground to air and air to ground), when SS and BS send a package, the value of CMAC_PN_U/D will be increased to one value.

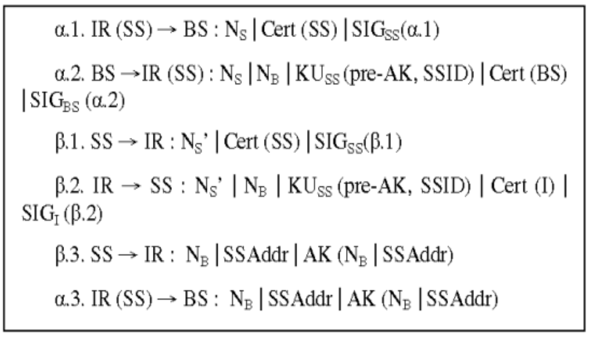
This counter is useful for resisting against replay attack. If the counter value is beyond the upper range, identification will be performed again. But this upper range is so great that re-identification is always executed for other reasons. [10]

E. Types of Attack to PKMv2

First Attack: Forging, faking, or changing request message is very simple without SS signature. This is similar to the same thing named “simple reply attack”.

Second Attack: There is the possibility of attack even with signature of SS which is saved as authentication message. This attack is similar to the attack which was proposed in [13]. A new attack was found on original X.509 tripartite authentication protocol. [7] It means that when a factor is wrong about frequency of meetings, this attack can be eradicated through adding BS identity. From the above discussion, we can conclude that initial PKM has many defects. For example, it almost does not provide any guarantee about the AK to SS. PKMv2 adds another message to the end of protocol in order to ensure BS on the novelty of the first message. However, this attack fails and tangled attack is used as well. Then, it can be concluded that signature of SS and BS certificate are important and necessary for all authentication protocol versions.

Here, we describe them for PKMv2. We assume that request message is signed by SS. In fact, signature will not help nonce versions. Moreover, we delete message one from original protocol and non-critical part in those messages for more summary. Fig.10 shows scenario of this attack: [7]



α.1. IR (SS) → BS : N_S | Cert (SS) | SIG_{SS}(α.1)

α.2. BS →IR (SS) : N_S | N_B | KU_{SS} (pre-AK, SSID) | Cert (BS) | SIG_{BS} (α.2)

β.1. SS → IR : N_S’ | Cert (SS) | SIG_{SS}(β.1)

β.2. IR → SS : N_S’ | N_B | KU_{SS} (pre-AK, SSID) | Cert (I) | SIG_I (β.2)

β.3. SS → IR : N_B | SSAddr | AK (N_B | SSAddr)

α.3. IR (SS) → BS : N_B | SSAddr | AK (N_B | SSAddr)

Figure 10. Inter Leaving Attack to PKMv2

In Fig.10 [7], α means message 1 in the protocol sample, will execute α. IR (SS) shows IR intruder which replace α instead of SS. In execution of α, IR shows itself instead of SS and send message 1 to BS. In fact, message is a response which SS has sent it previously. When IR receives α2 from BS, it requires answering with α3 in order to be successful in authentication.

But now, there is not IR, because, it cannot restore the message to its original state which has been encoded by SS general key. However, IR can misuse SS.

In addition, IR can force SS to execute another β protocol sample and also can reply SS with nonce message which has been sent by BS. SS returns β3 for IR, in which, IR can send it to BS and also can terminate α.

If IR wants to become victorious in this attack, two problems will remain.

Firstly, AK in PKMv2 has been derived from previous AK with SSAddr and BSAddr. Since AKs in α and β are very similar to each other, IR should forge BSAddr as well. It is very easy in wireless networks. Secondly, PKMv2 uses AA to bond security meetings. It can also be forged or replied by SS or IR. Similarly, this attack can be stopped with adding BS identifier in message 3 which has been encoded by AK. According to this comment, this attack can be considered as “Due or Name Omission” attack as well. Moreover, SSAddr is not necessarily encoded.

If message 3 is not changed, it means that it has been encoded with the AK as derived from SSAddr. Also, BS should be derived from the same AK in order to encode it. So, it can be assured that SSAddr has not changed; otherwise, IR should forge its AK which has been derived from SSAddr. So, encoding SSAddr does not cause any other security. Designer can ask SSAddr to act like Salt. BSID can do this work if added. Also, SSID is not necessary in message 2 and encoding with SS general key has guaranteed that the message belongs to SS ONLY.

A type of new attack has been found in tripartite X. 509 authentication protocol by the source [7] even with checking timestamp. The author has named this attack as “Multiple Attack”, in which, one factor commits mistake on the multiplicity of the meeting. This attack can be overcome by adding BS ID. Consequently, it can be said that BS certificate and SS signature are necessary for all versions of this authentication protocol.

In the same direction, timestamp is also necessary for base PKM and Intl version but it can be omitted in PKMv2only after PKMv2 is changed. However, simple reply attack is also possible for PKMv2. So, message can be so brief. The above modified version includes two messages. As compared with three messages in PKMv2, a small number of exchanged messages are always necessary for the authentication protocol. Moreover, there is no problem to use timestamp here because of nature of IEEE 802.16, because SS and BS have been synchronized during the initial ranging. Moreover, the changed protocol is resistant against simple reply attack. [7]

V. A Comparative Analysis of Security in PKM Protocol

A. *Repeated Attacks*

TEK exchange in PKMv1 is vulnerable to the repeated attacks. In the same direction, SA-TEK-Challenge includes a random number which is generated by transmitter and SA-TEK-Response reply message and SA-TEK-Request contains random numbers which have been generated by the transceiver (transmitter and receiver) respectively. The random number of the subsequent message should be equal to the related random number existing in the previous message, for example, BS_random in SA-TEK-Challenge and SA-TEK-Request which should be the same.

If attacker uses eavesdropped message for fulfilling repeated attacks, receiver can identify the message by its random number to know whether it is exactly answer of the previous message or is a repeated message merely. So, with doing this correction, tripartite SA-TEK handshaking in PKMv2 can resist against repeated attacks. [14]

B. Forgery and Juggle Attacks

In comparison with PKMv1, each message carries C/HMAC message identification code. The C/HMAC value uses encoding C/HMAC_Key_U/D key while derivation uses AK. If an attacker eavesdrops each message and manipulates it, attacker can calculate value of C/HMAC without AK. Such manipulation is studied in practice and approving H/CMAC value at the terminal of receiver will lead to the rejection of TEK exchange. Therefore, we can say that tripartite PKMv2 can resist against tangled and forgery attacks. [14]

C. Man In The Middle Attacks

Regarding analysis of TEK exchange in PKMv1, we know that if attacker manipulated the value of encoding set in the middle of the road, SS would probably be led to a direction in order not to use identification strategy and/or use weak encoding algorithm. To solve this problem, SS should send its security facilities and capability in SA-TEK-Request message. Despite an attacker who manipulates this message in SA-TEK-Response, BS can contain received security capabilities, so that SS can announce actuality of this problem whether value of encoding set transmitted by itself has been entangled or nor? [14]If the value of encoding sets is changed, then, MIM attacks will be found.

VI. CONCLUSION

In this article, we discussed on the security solutions existing in WiMAX and possible attacks to authentication protocol and also its various weak points in WiMAX network. Some of these problems have been solved in the security terms and solutions (IEEE 802.16), but some of them have been remained unchanged which require more investigation and precision. We studied different vulnerability in authentication protocol of mobile WiMAX network and described the said solutions for improving them. Although WiMAX provides more security solutions than other wireless technologies like Bluetooth or WiFi, WiMAX is yet developing and requires conducting more researches with relation to its security vulnerabilities. WiMAX will be developed completely in the very near future and this can be a good opportunity for WiMAX in order to turn into top wireless communications technology.

References

[1] A. K. M. N. Sakib and M. S. Kowsar, "Shared Key Vulnerability in IEEE 802 . 16e : Analysis & Solution," presented at the 13th International Conference on computer and Information TechnologyEngineering and Technology, bangladesh, 2010.

[2] R. K. Jha and U. D. Dalal, "A Journey on WiMAX and its Security Issues," Journal of Computer Science and Information Technologies, vol. 1, pp. 256-263, 2010.

[3] M. Bogdanoski, P. Latkoski, A. Risteski, and B. Popovski, "IEEE 802 . 16 Security Issues : A Survey," presented at the 16th Telecommunications Forum (TELFOR 2008) Belgrade, Serbia,2008.

[4] P. Rengaraju, L. Chung-Horng, Q. Yi, and A. Srinivasan, "Analysis on mobile WiMAX security," in Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference, 2009, pp. 439-444.

[5] R. Srivastava and D. K. Mehto, "Prevention of Security Threats in IEEE 802.16 Standards," International Journal of Soft Computing and Engineering (IJSCE), vol. 1, pp. 103-108, Sep 2011.

[6] M. Barbeau, "WiMax/802.16 threat analysis," presented at the Proceedings of the 1st ACM international workshop on Quality of service \&amp; security in wireless and mobile networks, Montreal, Quebec, Canada, 2005.

[7] X. Sen and H. Chin-Tser, "Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions," in Wireless Communication Systems, 2006. ISWCS '06. 3rd International Symposium on, 2006, pp. 185-189.

[8] M. Barbeau and C. C.-c. N. Local, "WiMax / 802 . 16 Threat Analysis," Security, 2005.

[9] R. N. M. Abadi, "Prudent Engineering Practice for Cryptographic Protocols," IEEE Trans. Softw. Eng., vol. 22, pp. 6-15, 1996.

[10] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," IEEE Security and Privacy, vol. 2, pp. 40-48, 2004.

[11] C. I'Anson and C. Mitchell, "Security defects in CCITT recommendation X.509: the directory authentication framework," SIGCOMM Comput. Commun. Rev., vol. 20, pp. 30-34, 1990.

[12] Y. Fan and C. Yi, "Re-Authentication Design for PKMv2 of IEEE 802.16e Standard," in Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on, 2010, pp. 1-4.

[13] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., vol. 8, pp. 18-36, 1990.

[14] Y. Fan, "Comparative Analysis on TEK Exchange between PKMv1 and PKMV2 for WiMAX," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, 2011, pp. 1-4.