# Formal Analysis of Key Management in mobile Wimax

Noudjoud Kahya[(1)], Nacira Ghoualmi[(2)], Pascal Lafourcade[(3)], Roumaissa khelf [(4)]
[(1), (2) (4)] Networks and Systems Laboratory (LRS)
Badji Mokhtar University, Annaba, Algeria
(3) LIMOS Laboratory
Blaise Pascal University, Aubière, France.

***Abstract*—The Mobile WiMAX IEEE 802.16e is a new technology supporting broadband wireless *communication with fixed and mobile access. The* standard offers high throughput broadband connections, supporting handover and roaming capabilities, and provides a security sub layer, which is responsible for secrecy, authentication and secure key exchange. In the area of security aspects, Mobile WiMAX exhibits vulnerabilities while adopting improved security architecture. Several versions of 802.16 networks were released. While the first versions have shown some security weaknesses that were later corrected by the recently released versions, the security mechanisms of 802.16 still remain vulnerable and the limited deployment of such technology is insufficient to satisfy the demands of security. This paper focuses on reducing the security vulnerabilities in the authorization protocol PKM and the generation of traffic encryption keys (TEKs). We propose the usage of 1. A formal analysis of the PKM protocol (authorization phase and exchange of TEKs phase) and 2.Device certificate for key exchange process to provide secure authentication and 3. Give a formal analysis of our new PKM protocol (authorization phase and exchange of TEKs phase). The formal analysis has been conducted using a specialized model checker Scyther, which provides formal proofs of the security protocol. The revised authentication protocol is expected to provide better secure platform for all process of PKM.**

***Keywords –mobile Wimax, PKM, TEK, attack, analyze formal.***

## 1. INTRODUCTION

IEEE 802.16, commonly known as Worldwide Interoperability for Microwave Access (WiMAX), is a recent wireless broadband standard that has promised high bandwidth over long-range transmission. In the past few years, the IEEE 802.16 working group has developed a number of standards for WiMAX. First published in 2001, the IEEE 802.16 standard specified a frequency range of 10–66 GHz with a theoretical maximum bandwidth of 120 Mb/s and maximum transmission range of 50 km. However, the initial standard only supports line-of-sight (LOS) transmission and thus does not seem to favor deployment in urban areas. A variant of the standard, IEEE 802.16a-2003, approved in April 2003, can support non-LOS (NLOS) transmission and adopts OFDM at the PHY layer. It also adds support for the 2–11GHz range. These two standards were further revised in 2004 (IEEE 802.16-2004). Recently, IEEE 802.16e has also been approved as the official standard for mobile applications.

In the IEEE 802.16 technology, security has been considered as the main issue during the design of the protocol. However, several design and security vulnerabilities were found in this technology. These vulnerabilities are the main cause to introduce unauthenticated messages which are susceptible to forgery, the unencrypted management communication which reveals important management information and it does not have perfect mechanism for mutual authentication;

Previous works have addressed the necessity of mutual authentication as well as mechanisms to counter attacks on 802.16. However, there are still some flaws in their protocols. Our paper analyzes those possible attacks to both BS (base station) and MS (mobile station), and proposes revised authentication protocol to solve those problems.

## 2. WIMAX OVERVIEW

In order to understand Wimax security issues, we first need to understand his architecture and how securities specifications are addressed in this technology.

### *A. Wimax Architecture*

IEEE 802.16 standard protocol stack consist of two layers: MAC (Medium Access Control) layer and PHY (Physical) layer. The MAC layer is subdivided into three sub-layer that is Convergence Sub-layer (CS), Common Part Sub-layer (CPS) and Security Sub-layer (SS) [1].

Security Sub-layer lies between MAC CPS and Philae. This sub-layer is responsible for encryption and decryption of data traveling to and from the PHY layer, and it is also used for authentication and secure key exchange [2].

### *B. Security Scheme*

In WIMAX, security has been included in the design of systems at the very start. To provide secure distribution of sensitive data from the BS to the MS and protect network services from attacks, Wimax applies strong support for authentication, key

management, encryption and decryption, control and management of plain text protection and security protocol optimization.

This sub layer performs three functions:

***1-*** *Authentication:*Authentication is achieved using a public key interchange protocol that ensures not only authentication but also the establishment of encryption keys. Wimax defines Privacy Key Management (PKM) protocol in security sub-layer, which allows three types of authentication:

*The first type is RSA based authentication:* RSA based authentication applies X.509 digital certificates together with RSA encryption. In this authentication mode, a BS authenticates the MS through its unique X.509 digital certificate that has been issued by the MS manufacturer. The X.509 certificate contains the MS's Public Key (PK) and its MAC address. When requesting an Authorization Key (AK), the MS sends its digital certificate to the BS, and then BS validates the certificate, uses the verified Public Key (PK) to encrypt an AK and sends back to the MS. All MSs that use RSA authentication have factory installed private/public key pairs together with factory installed X.509 certificates [3].

*The second type is EAP (Extensible Authentication Protocol) based authentication:* In the case of EAP based authentication, the MS is authenticated either by an X.509 certificate or by a unique operator-issued credential such as a SIM or by user-name/password. There are three types of EAP: the first type is EAP-AKA (Authentication and Key Agreement) for SIM based authentication; the second type is EAP-TLS (Transport Layer Security) for X.509 based authentication; the third type is EAP-TTLS (Tunneled Transport Layer Security) for SS-CHAPv2 (Microsoft-Challenge Handshake Authentication Protocol) [3].

*The third type is RSA based authentication followed by EAP authentication*.

***2-*** *Authorization:* This process follows the authentication process. MS requests for an AK and a SAID (Security Association ID) from BS by sending an Authorization Request message. This message includes the MS X.509 certificate, encryption algorithms and cryptographic ID. In response, the BS interacts with an AAA (Authentication, Authorization and Accounting) server to validate the request from the MS, and sends back an Authorization Reply which includes the AK encrypted with the MS's public key and a lifetime key and an SAID [3] [4].

*3- Encryption:* The previous authentication and authorization process results in the assignment of and Authorization Key (AK), which is 160 bits long. The Key Encryption Key (KEK) derived directly from the AK and it is 128 bits long. The KEK are not used for encrypting traffic data; so MS 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.

Many attacks are identified on authentication protocols PKM during mutual authentication. The potential attacks that can be carried out are man-in-the-middle, replay, interleaving and DoS attacks.

## 3. LITERATURE REVIEW

Few of relevant papers tackle the security issues of WIMAX network. T.Han and all [5], M.Rahman and M.Kowsar [6], M.Barbeau [7], M.Nasreldin and all [8], they give the most complete analysis of WIMAX security; they focused on the problem of IEEE 802.16.The purpose of this literature review is to study the literature of WiMAX/802.16. The review is of security mechanisms for this technology and his security threats, which are described in certain papers by different authors.

Table 1 contains the tabular format of a summarized review of the literature. What are the challenges to the WiMAX? And what are the solutions for these challenges. Every author has its own view.

| Author | Summary | Problems/Challenges | Solution |
|---|---|---|---|
| Michel Barbeau 2005[7] | An analysis of the security attacks on the wimax and architecture has been conducted. Focus is on the threats analysis of physical and Mac layer. | - Jamming, - Screambling, - DDOS, - Rouge BS, -X.509 digital certificate compromised. | Communication keys should be secure mutual authentication needed. |
| M. Nasreldin, H. Aslan, M. El-Hennawy, A. El-Hennawy. 2008 [8] | An analysis of threats according to the level of risk to IEEE 802.16. These threats were classified. | - Eavesdropping of management message. - Rouge BS. – DOS, - Jamming attack. | Strong authentication technique for SS and mutual authentication for BS. Spread spectrum scheme. Intrusion Prevention System. |
| Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, Yuan'an Liu2009 [5] | The paper is an overview of security architecture of mobile WiMAX network. He investigates man-in-the-middle attacks and Denial of Service (DoS) attacks toward 802.16e-based | - Man-in-the-middle attacks. - RNG-RSP DoS attack. - DoS attacks. | Propose Secure Initial Nenvork Entry Protocol (SINEP) based on DiffieHellman (DB) key exchange protocol to enhance the security level |

| | | | |
|---|---|---|---|
| | Mobile WiMAX network. | | during network initial. |
| Muhammad Sakibur Rahman, Mir Md. Saki Kowsar 2009 [6] | This article shows security vulnerabilities found in WiMAX (man-in-the-middle attack) and gives possible solutions to eliminate them. | - Man-in-the-middle attacks.- Description of some unauthenticated and unencrypted management messages | Propose modify DH protocol to fit mobile WiMAX to eliminate man-in-the-middle attack by using cryptographic sealing function. |
| John Hong Kok Han, Mohamad Yosoff Aias and Goi Bok Min. 2009 [9] | This paper presents one of the possible attacks namely the denial of service attacks on the IEEE 802.16e-2005 mobile wimax networks. | - DoS attacks on IEEE 802.16e. | The authors Simulation of DoS attacks and they show that a DoS attack exploiting the design of RNG-RSP messages is devastating the overall service levels of the wimax network. |
| Fang-Yie Leu, Yi-Fung Huang, Chao-Hong Chiu 2010 [10] | The authors propose an authentication key management approach, called Diffie-Hellman-PKDS-based authentication method (DiHam) to improve current security level of facility authentication between IEEE802.16e's BS and SS by using a secret door asymmetric one-way function, PKDS. | Dos/DDoS attack and a man-in-the-middle attack launched by a fake BS or SS during the network authentication phase. | In this article, the authors focus on the lift of the security level of the WiMax authentication, and develop an authentication mechanism to improve WiMax facility authentication by employing an integrated system that integrates the DH-PKDS and the DiHam, and in which a two-way authentication instead of the unidirectional authentication of PKMv1 is used. |
| Ramanpreet Singh, Sukhwinder Singh 2011 [11] | Ramanpreet Singh and Sukhwinder Singh have thought of the problem of detecting rogue base station in WiMAX/802.16 networks. A rogue base station duplicates a legitimate base station and so it is considered as attacker station. The rogue base station puzzles a collection of subscribers who attempt to get service that they believe to be a legitimate base station and it may lead to disturbance in service. The strategy of attack depends on the kind of network. | Attack of The rogue base station. | Their approach was based on the received signal strength (RSS) reports received by mobile stations and inconsistencies in sensitivity can be seen if a rogue Base Station (BS) is present in a network. These reports are assessed by the legitimate base stations, for example, when a mobile station undertakes a handover towards another BS. A new algorithm for detecting a rogue base station was described in this paper [10]. |
| Shahid Hussain, Muhammad Naeem Khan, Muhammad Ibrahim 2012 [12] | They have projected a new and distinctive security model and Encryption technique on the idea of existing model to secure WiMAX from Rogue Base station Attack and reply attack. | Rogue Base station Attack and reply attack. | They used two way authentications between base station and therefore the subscriber station to eliminate the Rogue base station Attack. Another improvement done on this paper was the use of nonce and time stamp that eliminate reply and DOS attack. For security, they projected some improvement in their model to enhance the capabilities and encryption Time. The comparison of ECC and RSA has done that shows that ECC is better than RSA due to smaller key size |
| Adnan Shahid Khan, Halikul lenando, Johari Abdullah, Norsheila Fisal 2015 [13] | Mobile Multihop Relay (MMR) network is one of the emerging technologies, especially LTE-Advanced, WiMAX and the Smart grid communications. Ensuring security is one of the most imperative and challenging issues in MMR networks. Privacy Key Management protocol is proposed to ensure the security measures in MMR networks. However, the protocol still faces several security threats, specifically Denial of Service (DoS), replay attacks, Man in the Middle (MitM) attacks and the interleaving attacks, which is termed as Medium Access Control (MAC) layer attacks. | Denial of Service (DoS), replay attacks, Man in the Middle (MitM) attacks and the interleaving attacks | This paper proposed a modified version PKM protocol for both unilateral and mutual authentication, which is termed as Self-organized Efficient Authentication and Key Management Scheme (SEAKS) authentication protocol. This protocol ensures secure end-to-end data transmission using distributed hop-by-hop authentication and localized key management schemes with a very simple and efficient way. |

## 4. PKM PROTOCOL

Security of connections access in WiMAX is done with respect to the Privacy Key Management (PKM) protocol. The protocol is responsible for the normal and periodical authorization of SSs and distribution of key material to them, as well as reauthorization and key refresh. It also manages the application of the supported encryption and authentication algorithms to the exchanged MAC Protocol Data Units (MPDUs).

The version of the PKM protocol, which will be described below, is that defined for use in the IEEE 802.16-2004 standard. This version was later extended to cope with mobility in the IEEE 802.16e standard.

PKM is a three-phase based protocol. The remaining part of this section describes each of these phases [14] [15].

### *A- PKM Authorization [14][15]*

The first phase of the PKM is the process of authorizing the MS by the BS.

To connect with the BS, the MS sends an authentication message (AuthenticationInfMess) containing the certificate of MS vendor. Immediately after that, the MS sends an authorization Request Message (AuthorizationReqMess) to the attached BS, requesting an Authorization Key (AK).

This information will be used as a shared secret. The message contains the following information:

• The MS certificate.• A description of the cryptographic capabilities supported by the MS. • The security association identifier (SAID) of the MS's primary SA. This value is equal to the primary 16-bit Connection Identifier (CID) that the MS receives from the BS during the network entry and the initialization phase.

The MS will be authorized based on the verification of its certificate. The public key contained in the certificate will be used for constructing the third message. The BS verifies also whether it supports one or more of the cryptographic capabilities of the MS. The response of the BS to the MS is described by message 3 (AuthorizationRepMess). It contains:

• The Authorization Key (AK) generated by the BS and encrypted using the MS public key contained in its certificate. A proper use of this AK shows an authorization regarding the access of the WiMAX channel. • A 4-bit AK sequence number to differentiate between the consecutive Authorization Keys.• The AK life time value.• The SAIDs descriptor(s) as the identity and properties of the primary SA and zero or more existing static SAs for which the MS may be authorized to get the keying information.

*Last message is from BS in reply to MS containing the Authorization Key (AK) encrypted with MS's public key along with sequence number, life time of AK and Security Association Identity List (SAID list).*

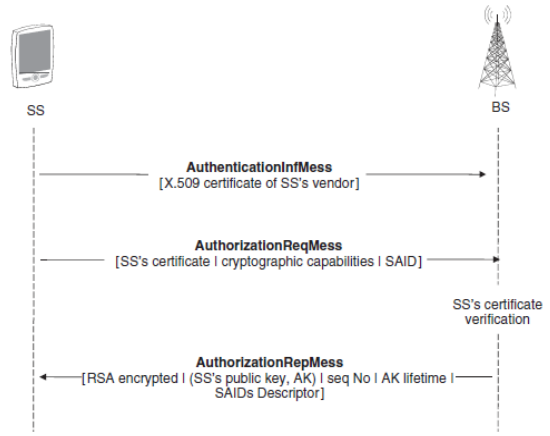



Fig 1 : PKM Authorization [14]

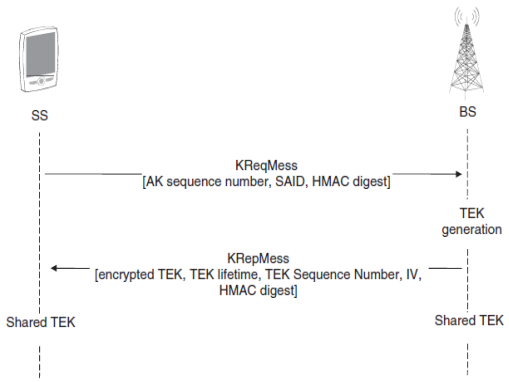



Fig 2 : Privacy and Key Management phase [14]

### *B- Exchange of TEKs [14][15]*

The aim of the second phase of the PKM protocol is to initiate the exchange of TEKs, and establish a data SA. The TEKs will be later used for encryption. As stated previously, the authorizationRepMess message contains, in addition to the SAID and properties of the SA, from zero to several static SAs for which the MS is authorized to obtain the key material. Therefore, the MS starts, in this phase, a separate state machine for each of the SAID identified in the authorizationRepMess message.

Every state machine is responsible for managing the keying material associated with the related SAIDs.

Every MS sends periodically a Key Request Message (KReqMess) to the BS, asking it for the renewal of the TEK. This message is composed of:

• the AK sequence number which allows the BS to determine the Uplink HMAC Key used by the SS to generate the HMAC digest of this message;• the SAID related to the SA whose keying material is requested. This SAID is related to the started TEK state machine; • the HMAC digest produced by the

application of the HMAC function on the message payload using the Uplink HMAC Key.

After making sure that the received SAID matches the SA at the MS and verifying the authenticity and the integrity of the KReqMess message by checking the HMAC digest, the BS responds to that message. It sends a key Reply Message (KRepMess) containing the new key material needed by the TEK state machine. At any time, the BS maintains two active key materials per SAID, which are denoted by TEK-Parameters in the KRepMess. A keying material includes:

• TEK encrypted with the KEKs using either the 3DES in EDE mode with 128 bits, RSA PKCS#1, or AES in ECB mode with 128 bits;• the remaining lifetime of the TEK;• the TEK sequence number;• a 64-bit initialization vector.

The KRepMess message contains an AK sequence number, the SAID, the parameters related to the old TEK and the new TEK and an HMAC digest to ensure the MS that the message is sent by the BS without being tampered with. Note that the validity durations of the two TEKs overlap. In fact, the new TEK is being activated before the old TEK expires and the old TEK is destroyed after the activation of the new TEK. The lifetime of a TEK is also used by the MS to estimate when the BS will invalidate a previous TEK or request a new TEK.

*C- Data Encryption [14][15]*

After achieving the SA authorization and the TEK exchange, transmitted data between the MS and BS starts to be encrypted using the TEK. An encryption algorithm is used to encipher the MAC PDU. Note that, neither the CRC nor the MAC header is involved in encryption in order to guarantee the forwarding of the MAC PDU and support diverse services. In the MAC header, an Encryption Control (EC) field is set to 1 as an indication regarding the availability of an encrypted MPDS. In addition, the 2-bits Encryption Key Sequence (EKS) field indicates the used TEK. Encryption can be done by means of the Data Encryption Standard (DES) using Cipher Block Chaining (CBC) mode with 56 bits.

## 5. FORMAL ANALYSIS OF PKM USING SCYTHER TOOL

There are numerous robust tools available for formal security protocol analysis such as OFMC [16], Scyther [17], and ProVerif [18].

Scyther is a formal protocol analysis tool, for the symbolic automatic analysis of the security properties of cryptographic protocols (typically confidentiality or variants of authenticity). It assumes perfect cryptography, meaning that an attacker gains no information from an encrypted message unless she knows the decryption key. Scyther takes as input a role-based description of a protocol in which the intended security properties are specified using claims. Claims are of the form claim (Principal, Claim, Parameter), where Principal is the user's name, Claim is a security property (such as 'secret'), and Parameter is the term for which the security property is checked.

This section describes the main security weakness related the PKM standard, showing potential attacks in authorization phase and exchange of TEKs phase.

Similar to the approach taken by our analysis of PKM v1/v2 [19] [20], we contains the retrace and we formally verify our analysis on different phases of PKM protocols using scyther. In the end of this section we describe the proposed protocol and we discuss the obtained results.

*D- Properties Specifications*

Authenticity, confidentiality, access control, secrecy and uniqueness of the keys and freshly of message are selected for formal verification.

*1) Authenticity:* The principals (MS/BS) verify the authenticity of received messages (by verifying signatures or MACs). In order to fulfill authenticity the MAC address of the Meshach identifies it must remain secret. The MAC address is included in the MS's certificate (SsCert).

The formal definition of authenticity is given below [20] [21].

***Property 1:*** $claim(SS, Secret, SSCert)$

*2) Confidentiality:* Expresses that certain information is not revealed to an intruder. The security satisfied if the MS has the guarantee that all exchanged user data to BS is secret. The formalization of information confidentiality is given below [20] [21].

***Property 2:*** $\forall \propto \in Msg(claim(SS, Secret, \propto))$

*3) Access control*: This claim is fulfilled if the BS has the guarantee that, neither an unauthenticated user should gain access to the services provided, nor should an unauthenticated user be able to impersonate another user. A service should always be bound to an authenticated user.

Its formal definition is given as follows [20] [21]:

***Property 3:*** $\forall \propto \in Msg(claim(BS, Secret, \propto))$

*4) Secrecy and uniqueness of the session keys:* This claim is fulfilled if the BS and the MS have the guarantee that all exchanged keys (AK and TEK) are secret and unique.

***Property 4:*** $\forall key(claim(BS|SS, Secret, key))$

*5) Freshly of messages:* An important part of security protocols is the generation of fresh values which are used for challenge-response mechanisms (often called nonce's), or as session keys. This claim is fulfilled if the BS and MS have the guarantee that the session key is fresh [20] [21].

***Property 5:*** $(claim(BS|SS, Fresh, key))$

### *A. Formal Verification*

Pseudonymity, information confidentiality, no theft of service and secrecy and uniqueness of the session keys are selected for formal verification, we apply Scyther tool to verify if this properties are proved or not in PKM protocol.

Our analysis reveals that the phases of Key Management Protocol PKM are vulnerable into many attacks; these attacks fall into the following categories: replay, DoS, Man-in-the middle attacks.

1. *Property 1:* Scyther detected a possible attack, as an intruder eavesdrops the second message and obtains the MS's certificate (MsCert).
*2. Property 2:* Scyther detected a possible Authenticity attack. Message2 is sent in plaintext so an intruder eavesdrop this message and obtains the SS's certificate (MsCert). BS may face a replay attack from a malicious SS who intercepts and saves or modified the authentication messages sent by a legal MS previously.
*3. Property 3:* It is proved that unauthenticated user cannot access the services provided, and cannot impersonate another user. The BS uses the certificate of the MS to determine if the MS is authorized, then sends the AK encrypted with the public key of the MS. This guarantees that only the specific MS can decrypt the AK.
*4. Property 4 and 5:* It is proved that an adversary cannot obtain the unique AK as it is encrypted with the public key of the MS. AK is proved to be unique using synchronization claim and the fact that AK is a constant in one of the roles appearing only in one send event.

After the MS authentication procedure has been done, the AK is used to derive KEK and HMACkey. TEK is then generated by BS randomly. The TEK is the key actually used to encrypt data traffic exchanged between the BS and MS. A key exchange message is authenticated by HMAC-SHA1 to provide message integrity and AK confirmation. It is proved that an adversary cannot obtain the unique TEK.

Similar to the authorization protocol, the exchange of TEKs phase of the PKM is vulnerable to the replay attack. If an attacker replays the first message, the BS will assign and send new keying material using a KRepMess message. The legitimate MS, which is not aware of the attack, will think that it is the BS which requested the rekeying and sent the first optional message. As a consequence, this attack causes both the MS and BS to exchange keying material without intending to.

As seen in the formal analysis, the secrecy and uniqueness of the keying material distributed and the no theft of service possible claims are valid in both phases of PKM. However, pseudonymity and information confidentiality are broken.

## **6.** THE PROPOSED REVISED AUTHENTICATIONPROTOCOL

As discussed in the previous section, the existing protocol does not fulfill the claims pseudonymity and information confidentiality because it still vulnerable to replay, DoS and Man-in-the-middle. Some solutions are introduced to solve those problems in our new revised protocol. To prevent replay and man-in-the-middle attacks we add timestamp. The problem with timestamp is that it requires time synchronization between MS and BS. In the wireless scenario, time synchronization is considered to be difficult (particularly under mobility). But In IEEE 802.16(e), it is assumed that time synchronization is done between MS and BS.

Nonce is a possible alternative to timestamps for use in the authentication protocols. Nonce shows that the request queued were not used before. Timestamp identifies which request are the newer one and also the time sent by the MS and BS. Nonce will not give any information about the time that was sent. Nonce is also not sufficient to tell the BS that it is the current message received from the MS. There are two problems with the protocol that has timestamps only. An adversary can easily capture the timestamp of MS by listening to message 2. The time adjustment can be done by the adversary accordingly. Hence the scope of man in middle attack is persists with timestamp added protocol. To prevent security threats like replay attacks, DoS attack and Man-in the- middle attack, both nonce and time stamp are needed. So the revised protocol has the timestamp attached with the MS message to the BS along with the nonce.

The protocol is shown as follows:

- SS/MS and BS send a message to find an X.509 certificate and it own public key information onto the server CA.
- *SS*/MS and BS exchange their certificates through the certification center CA in order to decide if etch particular is a trusted device or not.
- SS/MS sends a message contains the SS/MS certificate (SsCert) and a nonce's (Ns) used for registration and exchange certificates, it also contains the timestamp of SS/MS along with SAID and its security capabilities. Authorization request message is encrypted with the public key of the BS pk (Bs); the timestamp addition could bring an extra layer of security since the BS could identify the message as current one. The timestamp could avoid the intruders who are trying to synchronize time with either BS or SS/MS.
- If BS determines that the MS/SS is authorized it replies with a message authorization reply message. BS sends nonce (Ns) which was sent by the MS. That could ensure SS/MS that message send by

BS is the reply of the request send by SS/MS itself. BS Nonce ensures the MS about the authentication of BS. This mutual authentication gives extra layer of security. BS sends a pre- AK encrypted with the private key of BS sk (BS). From pre-PAK, the MS generates AK. After generation of AK correctly, the MS is authorized to access theWIMAX channel. The message contained also Lifetime of Pre-AK a Sequence number of pre-AK. BS sends his Timestamp (Tb) to grant that is not copied by adversaries, the timestamp and the nonce of BS previously received to confirm authorization access. BS encrypted the message with his public key.

- The last message ensures that the message is from the actual BS. Two layers of assurance are provided in this message: the nonce (Nb) and timestamp sent by BS (Tb). MS use it signature to ensure that message is from an actual MS and to assure the information integrity.
- Similar to the authorization phase, we used the timestamp attached with the MS message to the BS along with the nonce in all messages of Exchange of TEKs phase

The formal definition of the revised PKM is shown as follows:

1- Authorization phase :

*MS→CA: MS*
*CA→MS:{MS,{CertMS,pk(MS)}sk(CA)}sk(CA)*
*MS→BS:{{CertMS,Ns}pk(CA)}sk(MS)*
*BS→CA: BS*
*CA→BS:{BS, {CertBS, pk(BS)}sk(CA)}sk(CA)*
*BS→CA: {{{CerMS, Ns }pk(CA)}sk(MS), CertBS,Nb}sk(BS)*
*CA→BS:{{CerMS, Ns, Nb }pk(BS), {CerBS, Ns, Nb }pk(MS)}sk(CA))*
*BS→MS:{{CerBS, Ns, Nb }pk(MS)}sk(CA)*
*MS→BS:{{Ts, Nb,cap,SAID}pk(BS));*
*BS→MS:{{prePAK(BS)}sk(BS),SAIDlist,Ts,Tb, Ns, preSeq,prePAKlifetime}pk(MS)*
*MS→BS:{Tb, Nb }sk(MS)*

2- Exchange of TEKs phase:

*BS →MS: Tb' ,Nb',SeqNo ,SAID, HMAC(Tb' ,Nb'|,SeqNo ,SAID).*
*MS→ BS: Tb' , Ts', Nb', Ns', SeqNo, SAID, HMAC(Tb' , Ts', Nb', Ns', SeqNo, SAID)*
*BS →MS: Ts', Nb', SeqNo, SAID, OldTEK, NewTEK, HMAC(Ts', Nb', SeqNo, SAID, OldTEK, NewTEK,)*

*Formal analysis of the revised authentication protocol*

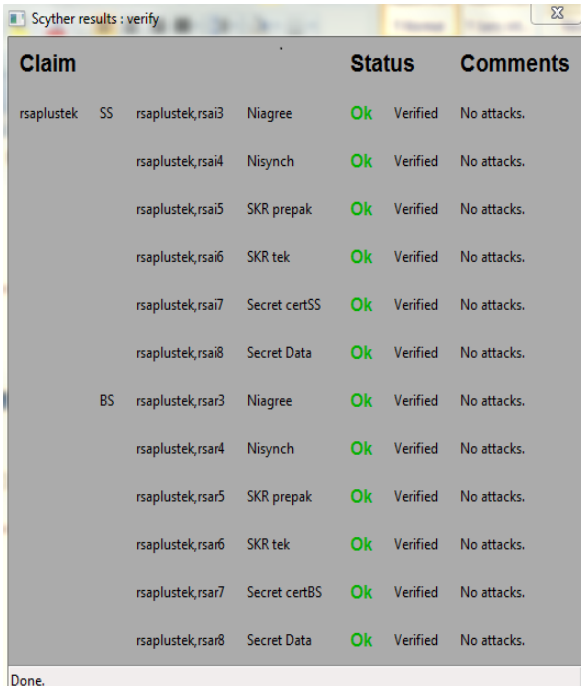
In this section, we formally verify our analysis on all phases of PKM protocols, and the correctness of our reversion. The revised authentication protocol is going to be challenged with the following requirements using the Scyther tool.

1. *Property 1:* In the formal analysis, it is proved that an intruder cannot obtain the MS certificate (MsCert).
*2. Property 2:* In the formal analysis it is proved that the authorization key exchanged in the authentication protocol is secret and not broken.
*3. Property 3:* It is proved that unauthenticated user cannot access the services provided, and cannot impersonate another user. Also, it is not possible to modify the data by an unauthorized individual.
4. *Property 4 and 5:* It is proved that an adversary cannot obtain the unique pre-PAK and the TEK is secured Timestamp and nonce are used in the revised protocol to prevent replay and man-in-the-middle attack. The MS appends the time stamp and nonce. This helps the BS to identify the request as a newer one. The nonce will wipe out the possibility of replay attack.

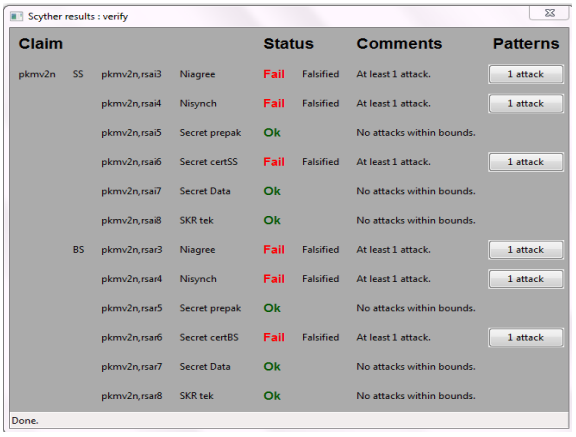
The nonce helps the BS to identify successive requests and it enhances the BS capacity to reject those requests which was sent by the intruders or adversaries. BS, thus, can identify the latest requests and it is able to filter out samples of replay attacks. In stapes authorization reply message, the BS sends the time stamp and nonce of MS. That helps in preventing an adversary from forging a BS. This protocol also provides mutual authentication. The nonce value sent by the BS helps in preventing the man-in-the middle attack.

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. The addition of nonce from the BS helps the MS to identify whether the message which he received with pre AK is a newer one or not. It is better to add more buffers to carry the used nonce values in the previous sessions. This gives more security to the BS and user MS.

Similar to the authorization phase, the nonce and timestamp helps the MS and BS to prevent replay attacks in the exchange of TEKs phase.




A- Analyses formal of New PKM




B- Analyses formal of PKMv2

## 7. CONCLUSION

In the IEEE 802.16 technology, security has been considered as the main issue during the design of the protocol.

However, several design and security vulnerabilities were found in this technology. In this paper we focused on the PKM protocol which is directly associated with the key management procedures of IEEE 802.16. Concentrating on PKMv2, several aspects of PKM functionality were examined including initial authorization /authentication between a BS and MS, key derivation. As discussed in this paper, PKM protocol vulnerable to replay, DoS and Man-in-the- middle attacks. Some solutions are introduced to solve those problems in our new protocol by using nonce and timestamp together. The revised authentication protocol ensures secure end-to-end data transmissions for all process of PKM.

## REFERENCES


[1] IEEE std 802.16e, 2006, 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 and Amendment and Corrigendum to IEEE Std 802.16-2004, IEEE Press.

[2] Perularaja Rengaraju, Chung-Horng Lung, Yi Qu,Anand Srinivasan, Analysis on Mobile WiMAX Security, IEEETIC-STH, Information Assurance in Security and Privacy. 2009,

[3] Sen Xu, Chin-Tser. "Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions" 200 IEEE Huang Computer Science and Engineering Department University of South Carolina Columbia, SC 29208, USA

[4] Ayesha Altaf, M.Younus Javed, Attiq Ahmed. "Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005" College of Signals, NUST. Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, IEEE 2008.

[5] T. Han, N. Zhang, K. Liu, B.Tang, Y.Liu "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions". 5th

IEEE International Conference on Mobile Ad Hoc and Sensor Networks, 2008. Atlanta, USA

[6] M.Sakibur Rahman, M.Saki Kowsar "WiMAX Security Analysis and Enhancement". 12th International Conference on Computer and Information Technology (ICCIT 2009).

[7] M.Barbeau. "Wimax /802.16 Threat analysis". ACM in workshop on quality of service and security in wireless and mobil networks, 2005.

[8] M.Nasreldin, H.Aslam and M.El-Hennawy. "Wimax Security". 22h international conference on advanced information networking and application, IEEE 2008.

[9] J. Han , M.Yusoff Alias and G. Min. "Potential Denial of Service Attacks in IEEE802.16e-2005 Networks". ISCIT 2009. Published by IEEE 2009.

[10] Fang-Yie Leu, Yi-Fung Huang, Chao-Hong Chiu « Improving security levels of IEEE802.16e authentication by Involving Diffie-Hellman PKDS»,2010 International Conference on Complex, Intelligent and Software Intensive Systems

[11] Ramanpreet Singh, Sukhwinder Singh, "Detection of Rogue Base Station Using MATLAB", International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Volume-1, Issue-5, November 2011.

[12] Shahid Hussain, Muhammad Naeem Khan, Muhammad Ibrahim, "A Security Architecture for Wimax Networks", International Journal of Computer Applications, Volume 50 – No.9, July 2012

[13] Adnan Shahid Khan*, Halikul lenando, Johari Abdullah, Norsheila Fisal "Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks" Jurnal Teknologi (Sciences & Engineering) 73:1 (2015) 75–81

[14] Seok-Yee Tang, Peter Muller, Hamid R. Sharif "WiMAX SECURITY AND QUALITY OF SERVICE AN END-TO-END PERSPECTIVE"ISBN 978-0-470-72197-1 (H/B) .A John Wiley and Sons, Ltd., Publication, 2010.

[15] Ramjee Prasad l Fernando J. Velez "WiMAX Networks, Techno-Economic Vision and Challenges" ISBN 978-90-481-8751-5 e-ISBN 978-90-481-8752-2 DOI 10.1007/978-90-481-8752-2 Springer Dordrecht Heidelberg London New York, 2010.

[16]D. B. Sebastian M¨odersheim Luca Vigano. Ofmc: A symbolic modelchecker for security protocols. International Journal of Information Security, 4(3):181–208, June 2005. Published online December 2004.

[17]C. Cremers. The Scyther Tool: Verification, falsification, and analysis ofsecurity protocols. In Proc. CAV, volume 5123 of LNCS, pages 414–418.Springer, 2008.

[18] B. Blanchet. An efficient cryptographic protocol verifier based on Prologrules. In Proc. 14th IEEE Computer Security Foundations Workshop(CSFW), pages 82–96. IEEE, 2001.

[19] N.Kahya, N. Ghoualmi, P.Lafourcade « Secure key management protocol in wimax. »International journal of network security and its application volume 4, number6, November 2012. ISSN 0974-9330

[20] N.Kahya, N. Ghoualmi, P.Lafourcade « Key management protocol in wimax revisited » Advances in computer science, engineering and application, Springer 2012, ISSN1867-5662.

[21]Ahmed M. Taha1, Amr T. Abdel-Hamid, and Sofiène Tahar Formal Verification of IEEE 802.16 Security Sublayer Using Scyther Tool 2009 ESR Groups France