RIST

Information Processing at the Digital Age

VOL22. N.2(2018) 39-60

Secured Initial Ranging Process in Wimax

Noudjoud Kahya*, Nacira Ghoualmi-Zine, Marwa Ahmim

Laboratory Networks and Systems,
Department of Computer Science,
Badji Mokhtar-Annaba University 23000, Algeria

Submitted 08/02/2019 , accepted 20/03/2019

Abstract

In Wimax, when a Mobil Station (MS) wants to be a part of the network and get the service from the selected Base Station (BS) it must take a set of methods called Initial Network Entry Process. The initial ranging process is the first steps to begin communication between a MS and a BS, and one of the most important process. After, we have studied the initial ranging process, we find that this process still exposed to various kinds of attacks. This is due to the unencrypted, unauthenticated MAC messages send in this process.

The weakness of this process has attracted a number of researchers. For our part, we propose a strong mechanism based on elliptic curve key exchanges with digital signature to secure initial ranging process. The proposed solution has been implemented with AVISPA tool and results show that our solution resist to Men In The Middle, Denial of Service, Replay, and Repudiation attacks.

Keywords: IEEE 802.16, Security, Initial Network Entry, SINECDS, Formal Verification, AVISPA;

1. Introdution

WIMAX (Worldwide Interoperability for Microwave access) or usually acknowledged as IEEE 802.16, is a telecommunications protocol that provides fixed and mobile internet access. WIMAX can offer high broadband speed, large coverage area, multiple bands and support for multimedia whit giving use numerous of security highlights such as integrity, privacy, access control, authentication, strong security, QoS guaranteed service (Chiang et al, 2013). WIMAX operates on two layers: physical layer (PHY) and MAC layer (MAC), when security is embedded at the security sub layer of the MAC layer.

The fundamental reason of security sub layer are to verify the authenticity of user, authorize the legitimate user and offer encryption support for the key transfer and data traffic.

In this technology, numerous strategies of authentication and encryption have been implemented, but it still uncovered to different attacks. One of these, it exists attacks of the initial network entry. Initial network entry is one of the important processes, as it is the first phase to establish connection between Mobil Station (MS) and Base Station (BS), is the major issue, as it straightforwardly influences the delay in the network (Pero et al., 2009).

The contribution to this paper is twofold: first, we explain existing protocols and methods proposed in literature on the existing vulnerabilities at the initial network entry procedure. Second, we propose a new solution based on key exchanges protocol uses Elliptic Curve key exchange with Digital Signature, and we use the formal method to verify our proposed protocol.

The paper is structured as follows: Section 2 presents the fundamentals concepts of WIMAX and the basics about the initial network entry process. In section 3, we summarize the vulnerabilities that are possible to the initial network entry process and we presents the existing methods and solutions proposed in literature. In Section 4, we outline our proposed protocol SINECDS. In Section 5, we describe the security analysis and formal verification with AVISPA tools of the SINECDS. In section 6, we make comparative study between the related works and SINECDS. Finally, we conclude in Section **7.**

2. Basic concepts

2.1. Wimax architecture

Worldwide Interoperability for Microwave Access (WiMAX) is a broadband wireless technology that provides an efficient service to mobile stations (MS) (Sangeetha et al, 2017). The protocol stack of IEEE 802.16 standard consists of two main layers: Physical (PHY) layer and Medium Access Control (MAC) layer, this new technology has features to support different MAC and physical layer parameters. (IEEE Std 802.16, 2009), (Bandhu and Vishwakarma, 2016).

First, the PHY layer consists of a sequence of equal length MAC frames transmitted through the coding and modulation of radio frequency signals. It supports Frequency Division Duplexing (FDD) and Time Division Multiplexing (TDM) (Ahson and Ilyas, 2008).

Second, the MAC layer is subdivided into three sub-layer that are Convergence Sub-layer (CS), Common Part Sub-layer (CPS) and Security Sub-layer (SS).

- The Service Specific Convergence Sub-layer (CS), it receives packets from higher layers and then do a set of functions (Gilanian-Sadeghi et al., 2013):
    - Packet classification and header suppression.
    - The capsulation of these packets into the MAC Service Data Unit (MAC SDU) format.
    - The distribution of the MAC SDUs to common part sub-layer.
    - At present, there are two types of service specific convergence sub-layer (Kuran and Tugcu, 2007).
        - The ATM convergence sub-layer used for ATM networks.
        - The packet convergence sub-layer used for packet services like Ethernet, IPv4 and IPv6, Point-to-Point (PPP) protocol.

- The Common Part Sub-layer (CPS). Is responsible for system access, connection management, bandwidth

request and grant, bandwidth allocation, scheduling and connection control (Tang et al., 2010).

- The security sub-layer provide authentication, authorization, establishment, and exchange of secured key (AK). It is also used for encryption and decryption of data exchanged from the MAC layer to PHY layer and vice versa (IEEE Std 802.16e, 2006). Two main protocols of security sub-layer are: *the PKM protocol*, used for secure key exchange between BS and MS, and *Encapsulation Protocol*, used for ciphering operations on data in the networks (Priya and Kumar, 2014) .

2.2. Initial network entry basics

In IEEE 802.16, when MS wants to be a part of the network and get the services for the selected BS, it must take after a set of method. The network entry process consist the following phases (Prasad and Velez, 2010).

1. Downlink channel synchronization.
2. Obtain Uplink Parameters.
3. Perform Ranging.
4. Capability's negotiation.
5. Authentication message exchange.
6. Registration.
7. IP connectivity stages.
8. Transport Connection Creation.

The following subsections describe each of these phases in more detail (Nair et al., 2004).

2.2.1 Downlink Channel Synchronization

In to begin with, MS scans for a channel in the frequency list to decide if it is presently within the coverage of the selected BS. Each MS stores a list of all operational parameters, like the downlink (DL) frequency utilized during the past operational instance. Hence, MS attempts to reacquire this downlink channel. In case this fails, the MS checks other frequencies of the downlink channel band of the operation tray it finds a valid downlink signal, when the DL frame preamble is detected, the MS can synchronize itself with regard to the DL transmission of the BS (Nair et al., 2004).

2.2.2 Obtain Uplink Parameters

When MS gets DL synchronization, it listens to the different control messages, such as: Frame Control Header (FCH), Downlink Channel Descriptor (DCD), Uplink Channel Descriptor (UCD), DL-MAP, and UL-MAP; that take after the preamble to get the different PHY and MAC related parameters corresponding to the DL and UL transmissions. (Jeffrey et al, 2007). Based on these UL parameters, MS chooses whether the channel is appropriate for its purpose or not. In case the channel is not appropriate, the MS return to past stage and scan new channels until it finds one that is. In case the channel evaluated usable, the MS listens to the UL-MAP message to collect data around the ranging opportunities (Gandhewar and Lokulwar, 2011) and (Jeffrey et al., 2007).

2.2.3 Perform Ranging

Once uplink parameters is gotten, BS and MS need to performing initial ranging in order to determine power

and timing offset requirements (Boone et al, 2008).

To begin with, MS sends a ranging request MAC message (RNG-REQ) on the contention based initial ranging interval utilizing the minimum transmission control. When MS does not get a response, it sends the ranging request once more in a consequent frame, utilizing higher transmission control.

Then, BS sends a ranging response MAC message (RNG-RSP) indicates power and timing corrections that the MS must make or indicates success.

In the end, in case the response indicates adjustments, the MS makes these adjustments and sends another ranging request (RNG-REQ). In the event that the response indicates success, the MS is ready to send data on the UL.

During this process, MS is allocated its Basic and Primary Management Connection Identifiers (CID) (Prasad and Velez, 2010).

2.2.4 Capabilities Negotiation

In this step, the MS and BS must negotiate capabilities of each one. MS sends a capability request message (SBC-REQ) to the BS describing its basic capabilities set; this request indicates physique and bandwidth parameters, as in terms of: the supported modulation levels, coding schemes, rates, and duplexing methods.

The BS responds with an SBC-RSP message with the intersection of the MS and the BS capabilities (Jeffrey et al, 2007) and (Prasad and Velez, 2010).

2.2.5 Authentication

After negotiating the basic capabilities. The BS must authorize MS by utilizing the privacy and key management protocol (PKM). First, MS sends the PKM request message (PKM-REQ) along with X.509 certificate of the MS producer. Along with the message, a depiction of the supported cryptographic algorithms is too send to its BS. At that point, the BS approves the identity of the MS, decides the encryption algorithm, and sends an authentication response (PKM-RSP) to the MS. The response contains the key material to enable the ciphering of data (Gilanian-Sadeghi et al., 2013).

2.2.6 Registration

With the completion of this step, the MS registers with the network. During the process, the MS sends a registration request (REG-REQ) message to the BS, and the BS sends a registration response (REG-RSP) to the MS. The registration exchange incorporates IP version support; Automatic Repeat Request (ARQ) parameters support, Classification Option support, Cyclic Redundancy Check (CRC) support, and Flow control. After the registration, MS gets the secondary management CID and hence a completely secured connection is established (Tang et al, 2010).

2.2.7 IP Connectivity Stages

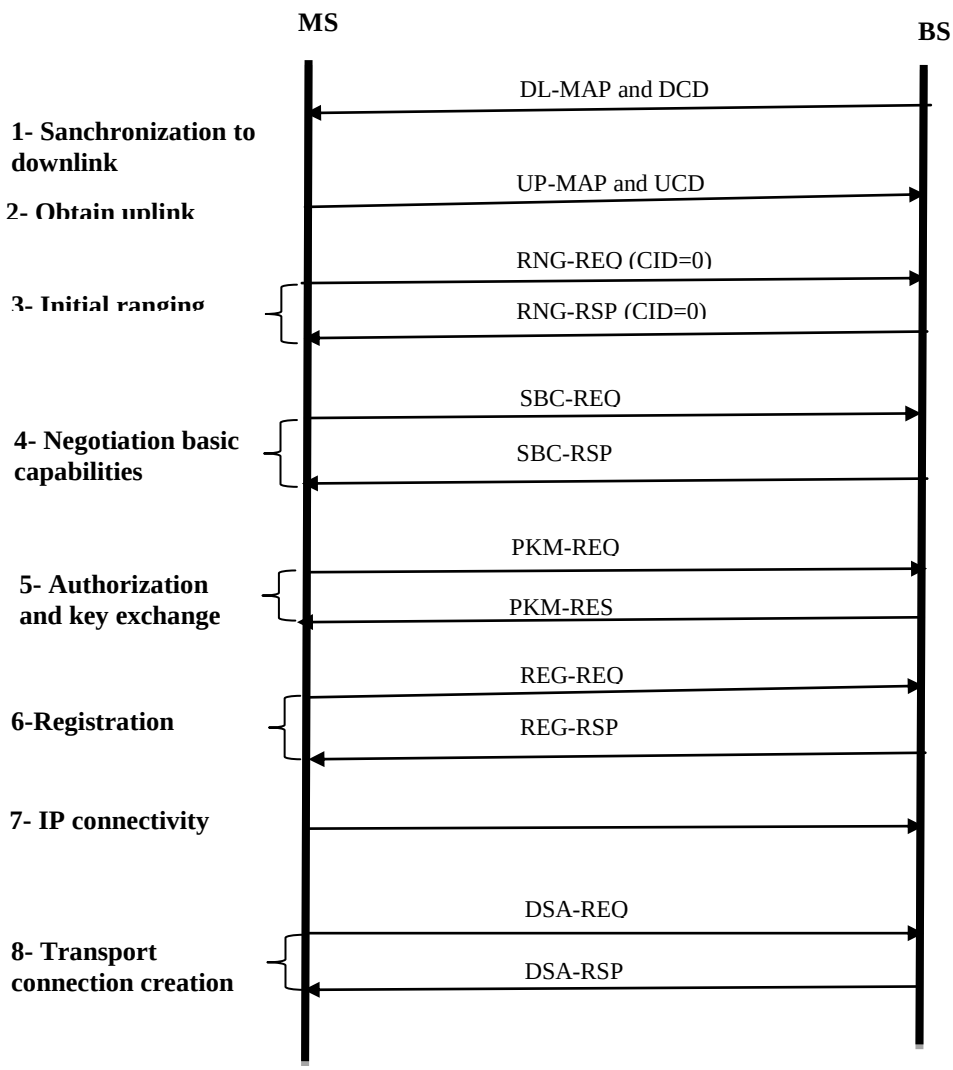
As soon as this step has been carried out, MS uses DHCP to acquire an IP addresses (Nair et al., 2004).

2.2.8 Transport Connection Creation

In this step, a transport association is created. To start the creation of a service flow, the BS confirms whether

the MS is authorized for such service and whether the requested level of QOS can be supported. In case the MS is authorized for this service, BS makes a new SFID (Benefit Stream ID) and sends a Dynamic Service Activate message DSA-REQ with the conceded QoS set and the CID to be used. On receipt of this message, the MS sends a DSA-RSP message indicating its acknowledgment. At that point BS accomplishes this process by sending a DSA-ACK message. At end, MS and the BS are prepared to trade data and management messages over the indicated CID (Tang et al., 2010). We summarize phases and messages exchanged in the network entry in figure1.

Figure 1 The network entry process (Prasad and Velez, 2010)



3. Review of literature

3.1 The Initial Network Entry Process Vulnerability

Because of unencrypted, not authenticated parameters in initial ranging and negotiated process, the initial network entry procedure has security leaks, and pose vulnerability to many attacks that can compromise the system's consistency. We analyse vulnerabilities contained in The Initial Network Entry Process, and we categorize these weaknesses in the process into two categories: Man-In-The-Middle and Denial of Service attacks.

Man-in-the-middle attacks: During the communication between MS and BS, the attacker intercepts messages communicate and then retransmits them, tempering the information contained in the message, so that MS and BS still appear to be communicating with each other (Han et al., 2008). In initial network entry, only the key transfer messages are encrypted; a most of the management message remains unencrypted. Therefore, there exist the possibilities that an attacker intercepts and capture message in this entry procedure. The Man-in-the-middle can be generated in capabilities negotiation process, when an attacker camouflages himself as the legitimate MS and sends tamped SBC-RSP message to serving BS (Han et al., 2008). The spoofed message may contain the false message about the security capabilities of the legitimate MS. For instance; the attacker sends messages to inform the BS that the MS only supports low security capabilities or has no security capabilities. In this situation, if the BS supports this kind of MS, the communication between the MS with the serving BS will not be encrypted (Hasan and Qadeer, 2009). As a result, the attackers would eavesdrop and tamper all the information transmitted.

Denial of Service attacks: is an incident in which an MS deprived of the service, of a resource they would normally expect to have (Han et al., 2008). All-inclusive studies confirm that there are many vulnerabilities exposing initial network entry to Denial of Service attacks such as unprotected network entry, unencrypted management communication, unprotected management frame (Gandhewar and Lokulwar, 2011); (Naseer et al., 2008); (Han et al., 2009); (Sridevi et al., 2012) and (Maru and Brown, 2008). An attacker can falsify these messages to generate DOS attack:

1- ***Ranging Request (RNG-REQ) message***: The Ranging Request (RNG-REQ) message is the very first message sent by an MS seeking to join a network and request for transmission timing, power, frequency, and burst profile information. This message is send periodically to allow for adjustments on the part of the MS and to inform the BS of its preferred downlink bust profile (Naseer et al., 2008). The RNG-REQ is an unencrypted message; hence, this message has been great potential to be utilized as follows (Akhunzada et al., 2009):

- Attacker can captured this message and alter the reported most preferred burst profiles of the authentic MS to the least effective one, consequently downgrading the service.
- Attacker can change the MSs downlink channel to diverse frequency range and has different facets.
- An adversary can shift only uplink channel to interrupt the communication between MS and BS.

2- ***Ranging Response (RNG-RSP) message:*** when it gets, the RNG-REQ, the BS responds with a RNG-RSP message. The BS uses this message to alter up- and downlink channel of the MS, and modify the settings of transmission link, transmission power level to improve the quality and efficiency of its services. The (RNG-RSP) message is unauthenticated, unencrypted, so an attacker can forge this message to generate several attacks.

- The attacker can forge a (RNG-RSP) message to modify the power level of the MS to transmit at least power. The impact of this setting is that the MS transmit at a power so low; it can barely reach the real BS and triggers the initial ranging procedure repeatedly (Han et al., 2009).
- The attacker forged (RNG-RSP) message to tell the legitimate MS to increase its power levels, to the maximum, effectively and quickly drain its battery life.

- The attacker intercepts the message (RNG-RSP) and changes the value of the response to Abort. The consequences of this attack, MS must re-initiates the transmission process.

3- Another unauthenticated management messages are:

- The Mobile neighbor advertisement (MOB_NBR-ADV) message unauthenticated. for maintaining the service continuity during migration of mobile user from air interface provided by one Base Station (BS) to the air interface provided by another BS (Pahal et al, 2015). The BS sent (MOB_NBR-ADV) to state the characteristics of the neighbor BS. An attacker can falsify such a message to state the accessibility of a rogue BS, thus preventing the MS from performing an efficient handover or denying such an operation to it (Tang et al., 2010) (Akhunzada et al., 2009).
- Fast Power Control (FPC) messages, is unauthenticated management messages sent by a BS requesting an MS to regulate its transmission power. An attacker, to set the transmission power of an MS too low, can forge this message. Therefore, the MS has to adjust its transmission power recursively to reach the BS again (Akhunzada et al., 2009).
- Downlink Burst Profile Change Request/Response (DBPC-REQ/RSP) are messages sends between BS and MS for changing the burst profile in order to adjust with the variations of distance between them and/or communication characteristics of the medium. An attacker can falsify (DBPC-REQ/ DBPC-RSP) to modify the burst profile deliberately and interrupt the communication between the BS and MS (Tang et al., 2010).

The Auth-invalid message (Auth-Invalid) is sent from the BS to the MS if the AK shared between them expires, or they have lost AK synchronization. The Auth-invalid message is sent as plaintext messages, this message has a value that indications to MS rejection of synchronization, and does not use the PKM serial number, and an attacker to deny accessed to a legitimate MS might use this value.

We will conclude this section by showing in Table 1 a list of unencrypted, unauthenticated management messages, with are susceptible to different attacks (Akhunzada et al., 2009).

Table 1 List of unencrypted, unauthenticated management messages in initial network process (Akhunzada et al., 2009)

Message Name	**Sent By**	**Connection**
Uplink Channel Descriptor (UCD)	BS	Broadcast
Downlink Channel Descriptor (DCD)	BS	Broadcast
Downlink Access Definition (DL-MAP)	BS	Broadcast
Uplink Access Definition (UL-MAP)	BS	Broadcast
Ranging Request (RNG-REQ)	MS	Initial Ranging or Basic
Ranging Response (RNG-RSP)	BS	Initial Ranging or Basic
Basic Capability Request (SBC-REQ)	MS	Basic
Basic Capability Response (SBC-RSP)	BS	Basic
Mobile neighbor advertisement (MOB_NBRADV)	BS	Broadcast, primary management
Fast Power Control (FPC)	BS	Broadcast
Auth-invalid message (Auth-Invalid)	BS	Primary management
Downlink burst profile change request (DBPC-REQ)	BS	Basic
Downlink burst profile change response (DBPC-RSP)	MS	Basic

3.2 Proposed solutions

The Initial Network Entry Process, is the main phase for any MS willing to communicate within the network, this process must be secured. If not, the entire network will be exposed to many attacks. After study of this process, we find that is not effectively secured that makes Man-In-The-Middle and DOS attacks possible. The weakness of this process has attracted a number of researchers.

In (Maru and Brown, 2008), Maru and Brown presented the detailed study for DoS attacks and its effects during the initial network process. To secure the process against DoS attacks, the authors recommend changing the security protocol by encrypting initial ranging messages and MAC management messages and utilizing the hash functions to authenticate all management messages. The proposition can be successful in preventing DoS attacks; however, the authors, they have not indicated the mechanism or technique utilized to secure initial and management messages.

Additionally, Han et al. (Han et al., 2008), proposed a new Secure Initial Network Entry Protocol (SINEP) that resists to DoS and MITM attacks. The protocol was based on the DH key exchange protocol. To mitigate the MITM attack presented in the implementation of the basic version of the DH key exchange protocol; the authors have introduced a mutual entity authentication algorithm using hash functions.
The DH has been modified and enhanced as follows: MS generates a TSSI from its international MS identity. A hash function is used to generate the hash value H(TSSI), which is used as an input parameter of the hash authentication function. This proposition gives a successful solution to DoS and MITM attacks. However, the authors have not use any verification method or tool to verify the protocol.

Next, a new solution is suggested in Rahman and Kowsar (Rahman and Kowsar; 2009), which is inspired from Han et al. (Han et al., 2008). The authors proposed the usage of a modified version of the basic DH key exchange protocol; where they used an entity authentication based on cryptographic sealing functions and International Subscriber Station Identifiers (ISSIs) for every MS to fit in the Mobile WiMAX environment.

Afterward, a novel mobile WiMAX security model called ROSMEX proposed in Shon et al. (Shon et al., 2010). In this protocol, a hash based authentication scheme between the MS and the BS are utilized. One of the periodically broadcast ranging codes sanded by BS to an MS is used to generate one of the global variables necessary in the implementation of the DH protocol. The other global variable has generated by MS. The BS sends its public key after verification of the two prime numbers and the MS's private/public key pair. By sharing the global variables and the respective station's public keys, a shared encryption key called pre-TEK is produced and utilized to ensure all the management messages.

To prevent attacks in initial network, Mehto and Srivastava (Mehto and Srivastava, 2011) have proposed a simple authentication for key exchange and a secure initial network entry. The proposed solution is summarized as follows:

1. To start authentication, An MS sends a request authentication to a BS.
2. The BS gets the request and calculates a random number called the nonce BS and sends a response that contains the nonce BS and BS certificate in the Uplink Map message (UL-MAP) message.
3. The MS verifies the BS certificate and calculates random numbers, a pre-shared key (psk) and MS identity (TSSI). At that point, MS uses psk and TSSI to generate two keys, pair authentication key (Pak) and pair encryption key (Pek). MS sends these keys encrypted with public key of BS.
4. When BS receives the message, it verifies the freshness of Nonce BS and obtains psk, TSSI, Nonce BS by using the BS private key to decrypt the message. By utilizing the obtained values, the BS derives Pak and Pek. BS then calculates a response RNG-RSP message that contains MAC for simple authentication.

The proposed solution gives a secured initial network entry and guarantees key freshness and session key consistency. However, evaluation of this protocol require to be conducted to perform its viability (Alezabi et

al., 2016).

A further analysis was conducted by Gandhewar and Lokulwar (Gandhewar and Lokulwar, 2011). Where, they have proposed new solution called Elliptic Curve Diffie Hellman (ECDH), is a mechanism to exchanging keys between two parties in a confidential manner. This protocol is summarized through the following steps (Alezabi et al., 2016).:

1. MS scans for an appropriate downlink channel and selects an initial ranging code from the initial ranging codes sent by BS.
2. MS uses ECDH algorithm to generate domain parameters G (the generator) and p (prime number).
3. MS generates its public key by using domain parameters p and G.
4. MS sends the RNG-REQ message, initial ranging code, domain parameters, and its public key to BS.
5. BS generates the public key after verifying parameter p.
6. BS sends the RNG-RSP message and its public key to MS.
7. BS and MS generate the pre-TEK and perform the ranging process by using this secret key.

Although this method provides a secure initial network entry, considerable evaluation is required to prove its effectiveness (Alezabi et al., 2016).

Sakib et al. (Sakib et al., 2011) proposed a new protocol that resists to DoS attack. Where, they have proposed the following solutions:

- BS and MS send a specific number to each other.

Each party applies a math function f to calculate the value of the received number; the legitimate parties only know this function.

- The result X is then sent to the other party.
- MS then sends an identity number with the result.
- After receiving the result, each party matches the values. If a match occurs, then the communication process will continue; else, the process is stopped.

In (Sridevi et al., 2012) Sridevi et al. have pointed out that the vulnerabilities during the initial network are due to the unauthenticated messages such as MS Basic Capability SBC-REQ, SBC- RSP, PKM-REQ, and PKM-RSP. To solve the problem, the authors have modified the DH key exchange algorithm, and they proposed an authentication method based on hash function. Their solution includes hashing and verifying the ranging codes RCn in MS and BS. If the codes are verified, then the MS is authorized, and a shared key pre-TEK is generated. After the generation of this shared key (pre-TEK) all the management messages are protected by this key during the initial network entry process. The proposed solution provides a good security performance against MITM, jamming, and scrambling attacks.

To enable an authenticated key agreement between the MS and the BS in the initial network entry, handover and sleep mode. Kalantari and Shojaei (Kalantari and Shojaei, 2013); developed a Diffie Hellman (DH) key exchange integrated into a digital signature scheme (DSS). In this kind of DH-DSS protocols, ephemeral public keys are first signed using a DSS for authentication purposes and then used in a DH key agreement to derive a fresh session key. The proposed solution can prevent DoS attack but need to be conducted to show its success.

4. Our proposed Secure Initial Network Entry Process

After deep study of initial network entry process, we found a list of some vulnerability caused of unencrypted and unauthenticated parameters. The initial network entry procedure has security leaks, and pose vulnerability that an adversary can generate serious attacks, using these weaknesses can compromise the system's consistency

Our work aims to building a Secure Initial Network based on Elliptic Curve key exchange using Digital Signature (SINECDS) with a low computation load to improve security of WIMAX. Unlike related works, the proposed protocol (SINECDS) can resist to various attacks types such as Modification, Reflection, Replay, DoS and Man-In-The-Middle with perfect security.

The SINECDS based on ECDSA (Elliptic Curve Digital Signature Algorithm) (Mansour, 2013) and the authentication key agreement elliptic curve proposed in Zeyad et al. (2011). This protocol with modifications that guarantee the security properties.

4.1 Notations

We use the notations listed in Table 2 for describing our protocol named Secure Initial Network based on Elliptic Curve key exchange using Digital Signature (SINECDS).

Table 2 **Notations used in proposed protocol**

Symbol	***Definition***
UL-MAC	Up Link Access definition
SRC	Selected Ranging Code
ID_{MS}	The identity of the Mobil Station
ID_{BS}	The identity of the Base Station
P	The generating point of ECC large prime order in E (F_q)
t_{MS}, t_{BS}	Static private keys of MS and BS
T_{MS}, T_{BS}	Static public keys of MS and BS
u_{MS}, u_{BS}	Private keys of MS and BS
U_{MS}, U_{BS}	Public keys of MS and BS, where: $U_{MS} = u_{MS} * P$, $U_{BS} = u_{BS} * P$.
H	Hash fonctions
K	The computed ephemeral session key by two-party
K_{BMS}	The derived session key by MS and BS
$EK_{BMS}\{\ \}$	Encryption using a symmetric cryptosystem with key K_{BMS}
RNG-REQ	Ranging request MAC message
RNG-REP	Ranging response MAC message
→	Send

4.2 Protocol description (SINECDS)

The proposed Secure Initial Network based on Elliptic Curve key exchange using Digital Signature (SINECDS), is presented as follows: we have two entities of the key exchange protocol, MS and BS, where MS is the protocol initiator who starts the Initial Network Entry Process and BS is the responder of the process.

Let t_{MS}, t_{BS} static private keys of MS and BS.

The MS's Static public key is $T_{MS} = t_{MS} * P$
The BS's Static public key is: $T_{BS} = t_{BS} * P$

As depicted in Figure 2, our proposed protocol is composed of four exchange messages.

Message 1 : $MS \rightarrow BS: SRC, ID_{MS}\ ,\ T_{MS}$

Once uplink parameters is obtained, BS and MS need to adjust timing offset and power parameters in the initialization phase, so when receiving Initial Ranging Codes from Base Station, Mobile Station performs the following operations:

- Selects one of the Ranging Codes (SRC).
- Selects its static private key randomly $t_{MS} \in [1, n-1[$ and calculates the static public key:

  $T_{MS} = H(t_{MS}|u_{MS}) * P$
- MS Sends to the BS: : $SRC, ID_{MS}\ ,\ T_{MS}$

Message 2: $BS \rightarrow MS: T_{BS}, \{ID_{MS}\ ,\ ID_{BS}\ ,\ U_{BS}\ ,\ S_{BS}\ ,\ \}K_{BMS}$

Upon receiving the MS message, the BS performs the following operations:

- The BS selects its static private key randomly $t_{BS} \in [1, n-1[$ and calculates its static public key : $T_{BS} = H(t_{BS}|u_{BS}) * P$
- It calculates: $e = H(T_{BS})$; $K = H(t_{BS}|u_{BS}) * T_{BS}$

  $S_{BS} = u_{BS}^{-1}(e + T_{BS} * K) mod\ n$; $K_{BMS} = H\langle ID_{MS}|ID_{BS}|X_{TMS}\ \ |X_{TBS}|X_K\rangle$

  Where X_{TMS} the x-coordinate of T_{MS}, X_{TBS} the x-coordinate of T_{BS} and X_K denotes the x-coordinate of K.
- BS Sends to the MS: $T_{BS}, \{ID_{MS}\ ,\ ID_{BS}\ ,\ U_{BS}\ ,\ S_{BS}\ ,\ \}K_{BMS}$

Message 3 : $MS \rightarrow BS: \{RNG\_REQ, U_{MS}\ ,\ S_{MS}\ ,\ \}K_{BMS}$

Upon receiving the BS message, the MS performs the following operations:

- Calculates: $K = H(t_{BS}|u_{BS}) * T_{BS}$; $K_{BMS} = H\langle ID_{MS}|ID_{BS}|X_{TMS}\ \ |X_{TBS}|X_K\rangle$

  Where X_{TMS} the x-coordinate of T_{MS}, X_{TBS} the x-coordinate of T_{BS} and $X_{K,}$ Denotes the x-coordinate of K.

- It decrypts the received encrypted message by K_{BMS}

- It calculates: $w = S_{BS}^{-1} mod\ n$; $e = \mathrm{H}(\mathrm{T_{BS}})$; $U_1 = (e * w) mod\ n$
  $U_2 = (K * w) mod\ n$; $X = U_1 * P + U_2 * T_{BS} * P$;

  $S_{BS} = u_{BS}^{-1}(e + T_{BS} * K) mod\ n$; $U_{BS} = e * S_{BS}^{-1} * P + K * S_{BS}^{-1} * T_{BS} * P$

- Then, it verifies whether: $\boldsymbol{U_{BS} = X}$ (1)
- If the verification fails, the MS terminates the execution; otherwise, it calculates:

  $e = H(T_{MS})$; $S_{MS} = u_{MS}^{-1}(e + T_{MS} * K) mod\ n$

- MS sends to BS: $\{RNG\_REQ, U_{MS}, S_{MS}, \}K_{BMS}$

Message 4 : $BS \rightarrow MS$: $\{RNG\_REP\}K_{BMS}$

Upon receiving the MS's message, the BS performs the following operations:

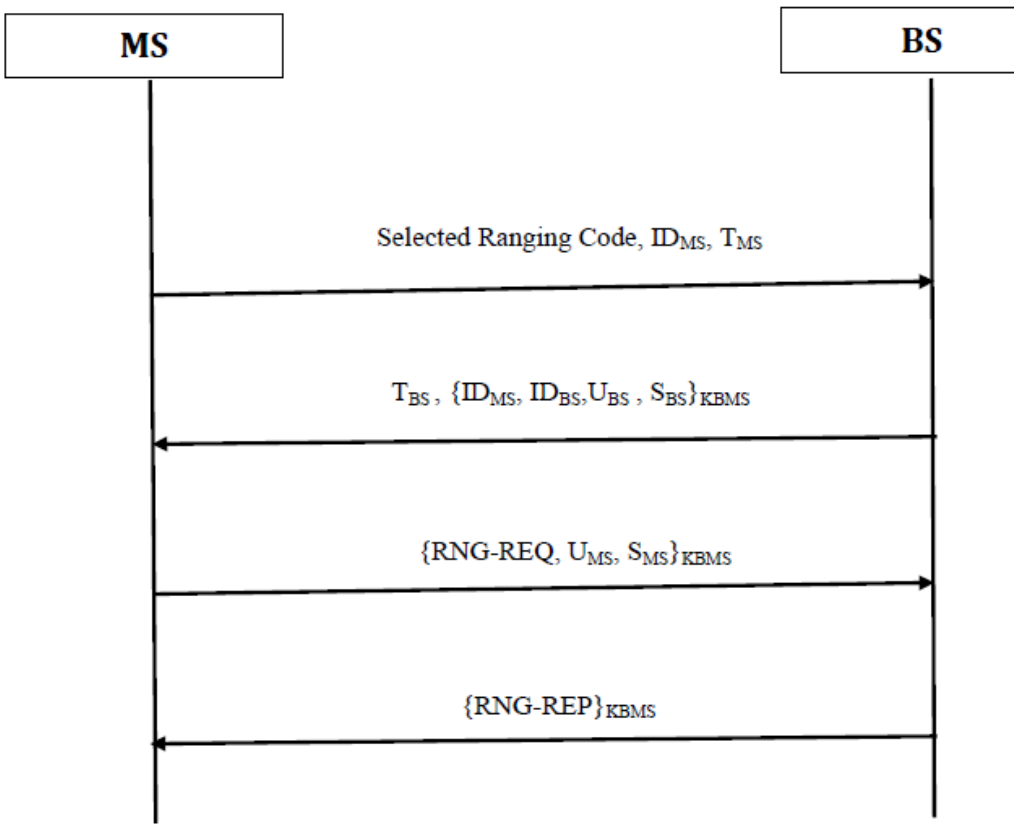
- It calculates: $e = H(T_{MS})$; $w = S_{MS}^{-1} mod\ n$; $U_1 = (e * w) mod\ n$
  $U_2 = (K * w) mod\ n$; $X = U_1 * P + U_2 * T_{MS} * P$;
  $U_{MS} = e * S_{MS}^{-1} * P + K * S_{MS}^{-1} * T_{MS} * P$

- Then, it verifies whether: $\boldsymbol{U_{MS} = X}$ (2)

- If the verification fails, the BS terminates the execution; otherwise, it sends $\{RNG\_REP\}K_{BMS}$ to the MS.

All further ranging messages could be encrypted using the shared key KBMS. We conclude that (SINECDS) is not limited to secure the ranging process but it secure also all phases of Network Entry show in figure1. Particularly Negotiation basic capabilities (SBC) and Authorization and key exchange (PKM) using the same shared key KBMS.

Figure 2 Secured initial ranging process



5. Security evaluation of (SINECDS)

In this section, we present security analysis and formal verification for proposed protocol (SINECDS), which show that our protocol can overcome the weaknesses mentioned in Section 3.

5.1 Security analysis

The proposed protocol (SINECDS) has the following properties:

- **Perfect forward secrecy**: the compromise of the long-term keys should not lead to the compromise of session keys from the earlier sessions (Ahmim et al, 2015). If the adversary possesses the private key u_{MS} of MS at later step, he cannot recover the previously sent messages because he has to get the compromised K_{BMS} and the retrieving the value K_{BMS} is difficult because all private keys t_{MS}, t_{BS}, u_{MS}, u_{BS} are randomly selected. The perfect forward secrecy of our proposed protocol is preserved.
- **Reflection attack***:* it is a method of attacking a challenge-response authentication system, that a single principal does not play the roles of both MS and BS simultaneously. In our protocol, the MS is able to check the identity of the BS in the second message. In a similar way, the BS can verify the MS identity in the third message.
- **Replay attack**: our protocol can resist to the replay attack. Suppose that the adversary 'I' eavesdrops the conversation between the MS and the responder BS, when the interchange is over between them. The intruder 'I' connects to BS, and he sends to BS the T_{MS} read from the last session. Then the BS sends T_{BS}, S_{BS} to the adversary. However, in the third message, the adversary is caught because it cannot produce the S_{MS} corresponding to T_{BS}, and he cannot calculate the same-shared key K_{BMS}.
- **Non- repudiation***:* If the station MS denies that she has sent the RNG-REQ to BS, then any trusted station can compute the verification $U_{MS} = X$ using the key shared K_{BMS} between MS and BS. However if the condition satisfies, that ensures that the message come from MS.
  If BS denies that he has sent the RNG-RSP to MS, the trusted party can also compute the verification $U_{BS} = X$, if the condition satisfies, that confirms that the response come from BS. Our proposed protocol provide the non-repudiation of sent end receive.
- **DoS defense** : In message 3 (RNG-REQ), the MS send this message seeking BS to join a network and request for transmission timing, power, frequency and burst profile information. In previous versions of Initial Network Entry Process, an attacker can intercept this message and change the reported most preferred burst profiles of the legitimate MS to the least effective one, hence downgrading the service. Moreover, he can shift only uplink channel to interrupt the communication between MS and BS (Naseer et al, 2008). To protect the process against DoS attacks in message (3), a shared encryption key K_{BMS} is used to encrypt the Ranging Request (RNG-REQ).
  In message 4 (RNG-RSP): The BS uses this message to change up- and downlink channel of the MS, and modify the settings of transmission link, transmission power level to improve the quality and efficiency of its services. In previous versions, the (RNG-RSP) message is unauthenticated, unencrypted, so an attacker can falsify this message to generate DOS attacks. An adversary can alter the power level of the legitimate MS to transmit at minimum power. The effect of this attack is that the MS transmit at a power so low, it can barely reach the actual BS and triggers the initial ranging procedure repeatedly. The attacker can also forged (RNG-RSP) message to tell the legitimate MS to

increase its power levels, to maximum, effectively and quickly drain its battery life. On the other hand, he can changes the value of the response to Abort. The consequences of this attack, MS must re-initiates the transmission process. Our proposition (SINECDS) can protect the process for all this DOS attacks, we use the shared encryption key K_{BMS} to encrypt the Ranging Response (RNG-RSP).

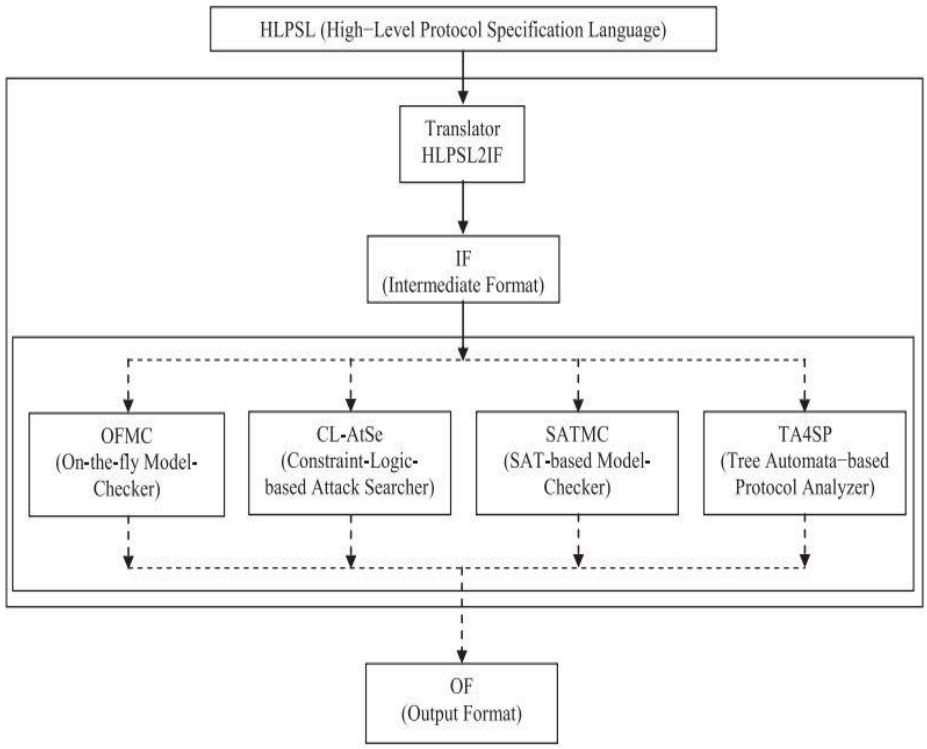
- **Efficiency**: (SINECDS) possesses the properties of ECC such as a small key size, less space for key storage and low computation load. In addition, hash function, multiplication, the addition, the symmetric key, all of these operations used in our protocol, are simple and could be made quickly.
- **Control key**: with our protocol, no single party is able to force the shared key to a pre-selected value.
- **Man-in-the-middle attack**: During the communication between MS and BS, the attacker intercepts messages communicate and then retransmits them, tempering the information contained in the message, so that MS and BS still appear to be communicating with each other. (SINECDS) can resist to MITM attack: Suppose that an adversary I eavesdrops the communication channel between MS and responder BS, he can replace the authentication request U_{BS} with UI. However, the MITM attack cannot be successful because of the verification of U_{BS} = X by the MS in the message 2 and the verification of U_{MS} = X by the BS in the message 3.

5.2 Formal security verification of (SINECDS) using AVISPA Tool

In this section, we provide a formal security verification of our protocol (SINECDS) using Automated Validation of Internet Security Protocols and Applications (AVISPA) and the Security Protocol Animator for AVISPA (SPAN) to prove the resistance of the proposed protocol (SINECDS) against the various types of attacks.

AVISPA composes of four back-ends (AVISPA, 2006): SAT-based Model-Checker (SATMC), Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP), On-the-fly Model-Checker (OFMC) and Constraint Logic based Attack Searcher (CL-AtSe). The AVISPA uses the standard Dolev-Yao mechanism (Dolev et al., 81). In this model, an intruder (passive or active) controls the communication channel in the networks; i.e., it can modify, replay, and suppress message. Figure 3, depicts the framework of AVISPA tool.

Figure 3 The architecture of the AVISPA tool (AVISPAv1.1, 2006; Glouche et al., 2006)



In order to evaluate our proposed scheme with AVISPA, we have to perform the following steps:

Step 1: In this step, we have coded the basic roles in the HLPSL (High Level Protocol Specification Language) that used in AVISPA for specifying protocols and their security properties (Basu et al, 2012); our scheme composed of two basic roles 'Alice' and 'Bob', which represent respectively Mobile Station (MS) and Based Station (BS). Figure 4 shows the role for the BS in the HLPSL language.

Step 2: In this step, we define the roles for the session, environment and goal in the HLPSL language. In the session role, the basic roles such as 'Alice' and 'Bob' are instanced with concrete arguments. The environment role contains the initial knowledge of intruder, global constants and composition of one or more sessions. The goal role serves to specify the security dimensions.

Step 3: We have checked the proposed scheme using SPAN, the results of the formal verification using the OFMC and CL-AtSe back-ends are presented in the figures 5, 6.

Figure 4 Role specification of Based Station (Bob).

```
role bob(B,A:agent,G: text,H: hash_func, SND_A, RCV_A: channel (dy))
played_by B
def=
local State: nat,
        F1,F3,F4,F5,Add,Mul: function,
        Ttss, Ttbs, Uuss, Uubs,KBSS: text,
        ……….
        Z,W,U1,U2,X: text
        const  m1: text,
            sec_b_KBSS : protocol_id
 init State := 1
 transition
1. State = 1  /\ RCV_A(Ulmac') =|>
   State':= 3    /\ Uuss':= new()/\ Uss':= F1(Uuss',P)
                 /\ Ttss':=new()/\ S1':=H(Ttss.Uuss) /\ Tss':=
F1(S1',P)
                 /\ Selecrang':= new() /\ IDss':= new()
                 /\ SND_A (Selecrang'.IDss'.Tss')
2. State=3 /\ RCV_A (Tbs'.{IDss.IDbs'.Ubs'.Sbs'}_KBSS') =|>
State':=5
               /\ K':= F1(S1,Tss')
               ……..
                 /\ Eess':= H(Tss)
                 /\ S2':= exp(Uuss',m1)/\ S3':= F1(Tss,K)
                 /\ S4':= Add(S2',S3')/\ Sss':= Mul(S2',S4')
                 /\ Rngq':=new()
                 /\ SND_A ({Rngq'.Sss'.Uss}_KBSS)
                 /\secret(KBSS,sec_b_KBSS,{A,B})
                 /\  request (A,B,kbss2,KBSS)
end role
```

Figure 5 Results of the formal verification of the proposed scheme using OFMC back-e*nd*.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\SPAN\testsuite\results\protocol PKM
1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 9.12s
  visitedNodes: 2540 nodes
  depth: 9 plies
```

Figure 6 Results of the formal verification of the proposed scheme using CL-AtSe back-end.

```
SUMMARY
  SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  C:\SPAN\testsuite\results\protocol
PKM 1.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS

  Analysed   : 15 states
  Reachable  : 15 states
  Translation: 0.06 seconds
  Computation: 0.00 seconds
```

After the specification of (SINECDS) protocol and their security properties. The HLPLS code runs our protocol in OFMC and CL-AtSe back-end model checkers and the simulation results indicate that (SINECDS) are safe and that no attack has been found.

6. Comparison with other solution's

The Table 3 shows the comparative study between our proposition (SINECDS) with other propositions to secure initial entry network process of Wimax.

Based on security: Most of the studied papers focus on the resistance to DoS and Man-In-The-Middle attacks, but they disregard the other type of attacks as Replay, Reflection and Repudiation. These last ones cause the loss of security dimension like the authentication, integrity and confidentiality. Therefore, the information security will be damaged. However, SINECDS prevents MITM, Replay, Reflection attacks, resistance to Denial of Service and grants no repudiation the transition and reception of messages exchange between MS and BS.

Based on computational operations: hash function, exponential, addition, division, secret key en/decryption, public key en/ decryption. (SINECDS) uses the bases and fastest operations such as addition division to generate secure key. (SINECDS) does not use any exponential operation compared with (Han et al, 2008) (Sridevi et al, 2012) (Kalantari and Shojaei, 2013) they use 2/2, 2/2, 8/8 respectably. Compared with (Han et al, 2008) (Sridevi et al, 2012), we increase number of secret key en/decryption but (SINECDS) assure more security than there propositions.

Based on performance: our proposition can improve performance greatly because of the reduction in the number of messages exchange between MS and BS. (SINECDS) uses four messages for a safe ranging process by using secure key KBSM. Using our proposition not only solves the ranging process but also secure SBC negotiation and authentication and key exchange process by using the same key KBMS. These operations cause a great performance impact that can be offset by the decreased number of messages. To evaluate our solution, (SINECDS) has been implemented in AVISPA, a famous formal verification tool and simulation results show that (SINECDS) can resist to various attack. However, the evaluation of previous propositions needs to be conducted to show its effectiveness.

7. conclusion

The Initial Network Entry Process, is the main phase for any MS willing to communicate within the network, this process must be secured. If not, the entire network will be exposed to many attacks. However, many messages send in this process are not encrypted nor authenticated, so several attacks are possible like DOS, Replay, and Man-In-The-Middle. This process need a strong mechanism and method of security. In this paper, we propose a new solution based on key exchange protocol uses Elliptic Curve key exchange with Digital Signature. We have showed through formal verification that (SINECDS) is save against many attacks: Reflection, Replay, Repudiation, DOS, MITM attacks. In additional the proposed solution use four messages for secure ranging process. SINECDS, is more efficient in terms of computational complexity, hash function, division, the addition, the symmetric key, all of these operations used, are simple and could be made quickly. The proposed solution has been implemented with formal verification tool AVISPA and results show that

(SINECDS) resist to various attacks. SINECDS is not limited to secure the ranging process but it secure also all phases of Network Entry. Particularly Negotiation basic capabilities and Authorization and key exchange using the same shared key K_{BMS}.

Table 3. Comparison of different solutions

Reference		(Han et al., 2008)	(Sridevi et al., 2012)	(Kalantari and Shojaei, 2013)	(SINECDS)
Security	MITM	✓	✓	×	✓
	DOS	✓	×	✓	✓
	Replay	×	×	×	✓
	Reflection	×	×	×	✓
	Repudiation	×	×	×	✓
Complexity	Hash function (MS/BS)	4/4	1/1	3/3	4/4
	Exponential (MS/BS)	2/2	2/2	8/8	-/-
	Addition (MS/BS)	-/-	-/-	2/2	3/3
	Division (MS/BS)	-/-	-/-	4/4	2/2
	Secret key E/Decryption (MS/BS)	2/2	2/2	3/3	3/3
	Public key E/Decryption; (MS/BS)	-/-	-/-	-/-	-/-
Performance	Number of messages transmits	5	6	5	4
	Evaluation	None	MATELAB MYSQL	None	AVISPA
	Formal Verification	None	None	None	AVISPA

8. References

"IEEE Std 802.16, IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems and Revision of IEEE Std 802.16-2004," ed: IEEE Press, 2009.

"IEEE Std 802.16e, 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," ed: IEEE Press, 2006.

Ahmim, M., Babes, M. and Ghoualmi, N. (2015) 'Formal analysis of efficiency and safety in IPSec based on internet key exchange protocol', Int. J. Communication Networks and Distributed Systems, Vol. 14, No. 2, 2015, pp.202–218.

Ahson, S,. Ilyas, M. (2008), 'WiMAX Standards and Security', CRC Press Taylor & Francis Group Francis Group, LLC. pp 1-251.

Akhunzada, A,. Murtaza, S,. Raza Cheema, A,. Wahla, A. (2009**), '**Suggestion of New Core Point of Attacks on IEEE 802.16e Networks: A Survey ', International Journal of Computer and Network Security, Vol. 1, No. 3.pp 1-6.

Alezabi. K.A, Hashim. F, Hashim. S.J, Ali. B. M, Jamalipour. A, (2016), 'Authentication process enhancements in WiMAX networks', Security and Communication Networks, John Wiley & Sons, Ltd, 2016, pp 4703-4725.

AVISPA Project, (2006). AVISPA protocol library, http://ww w.avispa-project.org/.

Bandhu, K.C, Vishwakarma, R.G. (2016), 'Performance evaluation of TCP Vegas in WiMAX network asymmetry', Int. J. Wireless and Mobile Computing, Vol. 10, No. 2, pp.97–103.

Basu, A., Sengupta, I. and Kanta-Sing, J. (2012), 'Formal security verification of secured ECC based signcryption scheme', Proceedings of the Second International Conference on Computer Science, Engineering & Applications, pp.713–725.

Boone. P, Barbeau. M, Kranakis. E, (2008), 'Strategies for fast scanning, ranging and handovers in WiMAX/802.16', Int. J. of Communication Networks and Distributed Systems, Vol.1, No.4/5/6, pp.414 – 432.

Chiang. M.L., Wang. S.S; Wang. S.C; Yan. K.Q., Liang. H.H, (2013), 'Performance enhancement of WiMAX by three layers topology', Int. J. of Mobile Communications, Vol.11, No.1, pp.89 – 106.

Choi. D, Kim. H, Kang. J, Jun. M; (2013); 'ECC-based Mobile WIMAX Initial Network Entry with Improved Security'; International Journal of Advancements in Computing Technology(IJACT); Volume5, Number13, September 2013, pp 505-517.

Dolev, D., Yao, A.C-C: On the security of public key protocols. In: FOCS, pp. 350-357. IEEE 1981.

Gandhewar, PK,. Lokulwar, PP, (2011). 'Improving security in initial network entry process of IEEE 802.16'. International Journal on Computer Science and Engineering (IJCSE), Volume 3, Issue 9. pp 3327-3331.

Gilanian-Sadeghi, M., Mohd Ali, B. and Ab Manan, J. (2013) 'Key Management in Mobile WiMAX', Chapter 6 form Selected Topics in WiMAX Networks, Intech, pp.130-148.

Glouche, Y., Genet, T., Heen, O. and Courtay, O. (2006) 'A Security Protocol Animator Tool for AVISPA**',** *In ARTIST2 Workshop on Security Specification and Verification of Embedded Systems, Pisa.*

Hafizul, SK. And Biswas, I. G.P. (2014) 'A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings', King Saud University-Computer and Information Sciences,Vol. 26, No 1, pp. 55-67

Han T, Zhang N, Liu K, Tang B, Liu Y. (2008), 'Analysis of mobile WiMAX security: vulnerabilities and solutions'. 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Atlanta, GA, USA; pp 828–833.

Han, J., Yusoff Alias, M., Min, G. (2009), 'Potential Denial of Service Attacks in IEEE802.16e-2005 Networks'. ISCIT 2009. Published by IEEE 2009, pp 1207 – 1212.

Hasan, S. Qadeer, M. (2009), "Security Concerns in WiMAX", First Asian Himalayas international Conference on Internet, pp 1-5.

Jeffrey G. A, Arunabha. G, Rias, M., (2007), 'Fundamentals of WiMAX: Understanding Broadband Wireless Networking', Prentice Hall Communications Engineering and Emerging Technologies Series. Forword by theodure S. Rappaport series Editor. ISBN 0-13-222552-2. pp 1-478.

Kalantari. Z; Shojaei. M; (2013); 'A DH-DSS Based Approach to Improve Mobile WiMAX Security against DoS Attack'; International Journal of Computer Science Engineering (IJCSE); Vol. 2 No.05; pp 271-275.

Kuran, M.S. and Tugcu, T. (2007) 'Survey on Emerging Broadband Wireless Access Technologies' Int. J. Computer Networks. Vol. 51, No. 11, 2007, pp 3013–3046.

Mansour, I. (2013) ―Contribution à la sécurité des communications des réseaux de capteurs sans fil‖, université BLAISE PASCAL CLERMONT II, [online] https://tel.archives-ouvertes.fr/tel-00877033/document [accessed January 2014].

Maru S, Brown TX. (2008), 'Denial of service vulnerabilities in the 802.16 protocol'. Proceedings of the 4th Annual International Conference on Wireless Internet, Maui, HI, USA, pp 1–9.

Mehto DK, Srivastava R. (2011) 'An enhanced authentication mechanism for IEEE 802.16 (e) mobile WiMAX'. International Journal of Soft Computing and Engineering; Volume **1**, Issue 4,. pp 98–102.

Nair,G,. Chou, J,. Madejski, T,. Perycz, K,. Putzolu, D,. Sydir, J, (2004). 'IEEE 802.16 Medium Access Control and Service Provisioning', Intel Technology Journal, Volume 8, Issue 3, 2004. pp 213-228.

Naseer, S., Younus, M,. Ahmed, A. (2008), 'Vulnerabilities Exposing IEEE 802.16e Networks To DoS Attacks: A Survey'. ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing Ninth. IEEE 2008, pp 344-349.

Pahal, S., Singh, B. and Arora, A. (2015), 'Cross layer trigger-based handover scheme for mobile WiMAX networks', Int. J. Ad Hoc and Ubiquitous Computing, Vol. 19, Nos. 3/4, pp.133–142.

Prasad, P. l J. Velez, F. (2010), 'WiMAX Networks Techno-Economic Vision and Challenges'. Springer Dordrecht Heidelberg London New York, ISBN 978-90-481-8751-5 e-ISBN 978-90-481-8752-2, pp 1- 508.

Priya. D., Kumar. P, (2014), 'A countermeasure for flooding attack in mobile WiMAX networks', International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.5, pp 99- 112.

Rahman M.S,. Kowsar, Md. S., (2009), 'WiMAX Security Analysis and Enhancement', International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, pp. 679-684.

Sakib AN, Mahmud T, Mountain Munim S, Mountain Munim MMR. (2011) 'Secure authentication & key exchange technique for IEEE 802.16 e by using cryptographic properties'. International Journal of

Engineering Research and Applications; Volume 1, Issue 3, pp 490–496.

Sangeetha .J; Goel.N; Rustagi.R.P; Balasubramanya Murthy. K.N, (2017), ' Location area planning problem in WiMAX networks using nature inspired techniques: performance study', International Journal of Information and Communication Technology (IJICT), Vol. 11, No. 2, pp. 222–242.

Selvarani, R., Ravi T. N., (2015), 'Security for Mobile WiMAX through Secured Initial Ranging Process', International Journal of Computer Science and Information Technologies, Volume 6, Issue (4) , pp 3380-3384.

Shon, T., Koo, B., Park, J. H,. Chang, H.,(2010), 'Novel Approaches to Enhance Mobile WiMAX Security', EURASIP journal on Wireless Communications and Networking, vol. 2010, pp 1-11.

Sridevi B, Brindha M, Umamaheswari R, Rajaram S. (2012), 'Implementation of secure & cost effective authentication process in IEEE 802.16e WiMAX'. International Journal of Distributed & Parallel Systems 2012; Volume **3**, Issue 2. pp 215–229.

Tang. S.Y, Muller. P, Sharif. H.R,. (2010), ' WiMAX Security And Quality Of Service an End-To-End Perspective', John Wiley & Sons Ltd., ISBN 978-0-470-72197-1, pp 1- 425.

Zeyad, M., Chien-Lung, H., Yaw-Chung, C. and Chi-Chun, L. (2011) 'An efficient and secure three-pass authenticate key agreement elliptic curve based protocol', International Journal of Innovative Computing, Information and Control, Vol. 7, No. 3, pp.1273–1284.