Secure Network Entry Process in Wimax

Noudjoud Kahya, Nacira Ghoualmi-Zine, and Marwa Ahmim
Badji Mokhtar University, Department of Computer Science, Laboratory Networks and Systems, Annaba, Algeria
Email: kahya.noudjoud@gmail.com; ghoualmi@lrs-annaba.net; ahmim.marwa@gmail.com

Abstract—WiMAX (Worldwide interoperability for Microwave Access) IEEE 802.16, is a new technology providing wireless and broadband data access to mobile and stationary users with high bandwidth and transmission rates. Security is always important in data networks, but it is particularly critical in wireless networks such as WiMAX. After the launch of this new standard, a number of security issues were reported in several articles. This paper focuses on reviewing the security vulnerabilities in the network entry process and authentication process of the WiMAX. The initial network entry process is the begin step to start communication between Mobil station (MS) and Base station (BS). This process is very important and must be secure. However, many messages send in this process are not encrypted nor authenticated, so several attacks are possible like Denial Of Service, Replay, Reflection, and Man-In-The-Middle. Based on the related background research, we focus on finding a strong mechanism and method of security such use Elliptic Curve key exchanges with Digital Signature to secure initial entry process and using nonce and timestamp together to secure authentication process. According to formal verification tool AVISPA, the results show that our solution prevent denial of service, resist to Men In The Middle, Replay, Reflection attacks, and grants no Repudiation.

Index Terms—Wimax, Network Entry process, Authentication, AVISPA.

I. Introduction

WIMAX (Worldwide Interoperability for Microwave access) or usually acknowledged as IEEE 802.16, new standard provide use a many of security features such as integrity, privacy, access control, authentication with a strong security, and guarantee to us mobility, scalability, quality of service. Wimax is structured in to two layers, MAC layer and PHY layer. MAC layer has three sub-layers Convergence Sub-layer, Common Part Sublayer and the Security Sub-layer [1]. The main purpose of Security Sub layer is to verify the authenticity of user, authorize the legitimate user and provide encryption support for the key transfer and data traffic. In this technology, many methods of authentication and encryption have been implemented, but it still exposes to various attacks.

1- Attacks to the initial network entry in WIMAX. Initial network entry process is one of the important processes, as it is the first phase to establish connection between Mobil Station (MS) and Base Station (BS). Initial network entry process is the major issue, as it directly influences the delay in the network.

2- Attacks to Privacy Key Management (PKM) protocol. PKM is responsible for the normal and periodical authorization of MSs and distribution of key material to them, as well as reauthorization and key refresh.

The contribution of this paper is twofold:

First, we propose a new solution based on key exchange protocol uses Elliptic Curve key exchange with Digital Signature Algorithm to secure Initial network entry process.

Second, we propose a revised authentication protocol (authorization phase and exchange of TEKs phase) to secure PKM against replay, DoS and Man-in-the-middle attacks.

We use the formal method to verified if our proposed solutions resolute the security problems of the network entry process.

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

II. Network entry Basics

WIMAX is a broadband wireless technology that provides an efficient service for fixed, nomadic, portable and mobile subscribers [2]. WiMAX supports wide coverage areas with a coverage radius for the WiMAX cell up to 50km and data rates may go up to 70Mbps. Additionally; IEEE 802.16 standard is designed to operate in Non-Line of Sight (NLOS) mode at operating frequencies equal to 11GHz and in Line-of-Sight (LOS) mode at operating frequencies between 10 to 66GHz [3], [4].

WIMAX, is very complex and many of parameters need to be agreed upon before any successful transmission between a new station and the desire BS. Network entry is the term used in the standard IEEE 802.16 to define a list of process for entering and registering a new station [5].

Network entry is summarized as follows:

1- Downlink Channel Synchronization: To acquire a downlink channel, MS scans for a channel in the defined frequency list to determine whether it is currently in the coverage of base station. First, MS attempts to reacquire

Manuscript received January 10, 2019; revised November 7, 2019.
doi:10.12720/jcm.14.12.1205-1210

this downlink channel. If this fails, it scans the possible channels of the downlink frequency band of operation until it finds a valid downlink signal. The synchronization is complete, as given by a PHY indication, the MAC acquires the channel control parameters for the downlink and then the uplink [6], [7].

2- Initial Ranging: In initial phase, the BS and MS need to adjust timing offset and power parameters.

At first, MS sending a ranging request MAC message (RNG-REQ) on the contention based initial ranging interval using the minimum transmission power. If it does not receive a response, the MS sends the ranging request again in a subsequent frame, using higher transmission power [6], [7].

The BS send a ranging response (RNG-RSP).The response either specifies power and timing corrections that the MS must make or indicates success.

3- Capabilities Negotiation: After initial ranging, MS and BS must negotiate their supported parameters.

The MS sends SBC-REQ (MS Basic Capability Request) to inform the BS of its basic capabilities in terms of bandwidth allocation, duplexing methods, supported modulation levels, coding schemes and rates.

Based on its capabilities, BS responds with an SBC-RSP message with the intersection of the MS and the BS capabilities [7].

4- Authentication: In this phase, the BS authorize and authenticates the MS by providing the keying material to enable the ciphering of data through the privacy and key management protocol (PKM).

First, MS sends the PKM request message (PKM-REQ) along with X.509 certificate of the MS manufacturer. Along with the message, a description of the supported cryptographic algorithms is also send to its BS.

The BS validates the identity of the MS, determines the cipher algorithm and protocol that should be used, and sends an authentication response (PKM-RSP) to the MS. The response contains the key material to be used by the MS. The MS periodically perform the authentication and key exchange procedures to refresh its key material [7].

5- Registration: After successful completion of authentication, the MS registers with the network.

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 includes IP version support, MS managed or non-managed support, ARQ parameters support, classification option support, CRC support, and flow control.

The MS and BS create transport connections using a MAC-create-connection request. A request to create a dynamic transport connection indicates whether MAC-level encryption is required [7].

6- IP Connectivity process: At this step, MS acquires an IP address to establish IP connectivity. The MS and BS need to have the current date and time. The BS and MS maintain the current date and time using the time of the day protocol [7].

7- Transport Connection Creation: After completion of registration and the transfer of operational parameters, transport connections are created.

For pre-provisioned service flows: The BS sends a dynamic service flow aaddition request message to the MS and the MS sends a response to confirm the creation of the connection.

Connection creation for non-pre-provisioned service flows: The MS initiate the process, by sending a dynamic service flow addition request message to the BS. The BS responds with a confirmation [7].

III. The Network Entry Process Vulnerability

Because of unencrypted, not authenticated messages sends in initial ranging and negotiated process, the network entry procedure has security leaks, and pose vulnerability to many attacks that can compromise the system’s consistency. We analyses vulnerabilities contained in The Network Entry Process, and we categorize these weaknesses in the process into:

A- 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 [8]. In 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 [8]. 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 [9]. As a result, the attackers would eavesdrop and tamper all the information transmitted.

B- Denial of Service attacks: is an incident in which an MS deprived of the service, of a resource they would normally expect to have [8]. All-inclusive studies confirm that there are many vulnerabilities exposing network entry to Denial of Service attacks [10]-[14]. 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 [11]. The RNG-REQ is an unencrypted message; hence, this message has been great potential to be utilized as follows [15]:

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 [12].

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.

C - 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 BS to the air interface provided by another BS [16]. 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 [8], [15].

Fast Power Control (FPC) messages, is unauthenticated management messages sent by a BS requesting an MS to regulate its transmission power. An attacker, can forge this message to set the transmission power of an MS too low, Therefore, the MS has to adjust its transmission power recursively to reach the BS again [15].

D- Attacks on PKM protocol: The PKMv2 protocol is secure enough for its practical implementation [17]. However, it still vulnerable to replay, DoS and Man-in-the-middle. There is no mechanism to ensure integrity and non-repudiation in the authorization process. In the Authorization request/reply message, if anyone with a properly positioned radio receiver catches the message, no digest is used to prove that others have not changed the messages, and nothing is used to make sure the sender cannot repudiate the message. An attacker can forge new frames and capture, modify, and retransmit frames from authorized parties.

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.

IV. Our Proposed Secure Network Entry Process

After deep study of network entry process, we found a list of some vulnerability caused of unencrypted and unauthenticated parameters. The 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 Network Entry Process (SNEP) based on:

1- Key exchange protocol uses Elliptic Curve key exchange with Digital Signature to generate a secure key used for encrypted all messages exchanged in network entry process.

2- Secure PKM protocol (authorization phase and exchange of TEKs phase) by using the timestamp attached with the MS message to the BS along with the nonce to prevent denial of service, replay, and Man in the Middle attacks.

A. *Notations*

We use the notations listed in Table I for describing our protocol named Secure Network Entry Process (SNEP).

TABLE I: Notations Used in Proposed Protocol

Symbol	***Definition***
UL-MAC	Up Link Access definition
SRC	Selected Ranging Code
ID$_{BS}$, ID$_{MS}$	The identity of the Base Station, Mobil 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
RNG-REQ	Ranging request MAC message
RNG-REP	Ranging response MAC message
AK	Authorization Key
MCer,BCr	The MS's certificate ,the BS's certificate
Nms, Nbs	MS's Nonce ; BS's Nonce
Tpms,Tpbs	MS's timestamp; BS's timestamp;
prePAK	pre- primary AK

B. The Formal Definition of the SNEP is Shown as Follows

1- Proposition to secure Initial network process

1.1 MS → BS: ***Selected Ranging Code, 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.
- Selects its static private key randomly $t_{MS} \epsilon$ [1, n-1] and calculates the static public key $T_{MS}=H(t_{MS} \| u_{MS})*P$.
- Sends to the BS: **Selected Ranging Code, ID_{MS} and T_{MS}.**

1.2 BS→MS: ***T_{BS},{ID_{MS}, ID_{BS},U_{BS}, S_{BS}}K_{BMS}***

- The BS selects its static private key randomly t_{BS} ϵ [1, n-1] and calculates its static public key $T_{BS}=H(t_{BS} \| u_{BS})*P$
- It calculates:
  - $e=H(T_{BS})$,
  - $K=H\ (t_{BS}||u_{BS})*\ T_{MS,}$
  - $S_{BS}=u_{BS}^{-1}(e+T_{BS}.K) \bmod n$
  - $K_{BMS}= H\ (ID_{MS}||\ ID_{BS}||X_{TMS}||\ X_{TBS}||X_k)$ 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.
- Sends to the MS: **T_{BS},{ID_{MS}, ID_{BS},U_{BS}, S_{BS}}K_{BMS} .**

1.3 MS → BS: ***{RNG-REQ, U_{MS} , S_{MS}}K_{BMS}***

- MS Calculates:

$K=H\ (t_{MS}||u_{MS})*T_{BS}$,

$KB_{MS}= H\ (ID_{MS}||\ ID_{BS}||X_{TMS}||\ X_{TBS}||X_k)$ 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.

- MS decrypts the received encrypted message by K_{BMS}
- MS calculates:
  - $w=S_{BS}^{-1} \bmod n$,
  - $e=H(T_{BS})$,
  - $U_1=(e*w) \bmod n$,
  - $U_2=(K*w) \bmod n$,
  - $X=U_1*P+U_2*T_{BS}*P$
  - $S_{BS}=u_{BS}^{-1}(e+T_{BS}*K) \bmod n$
  - $U_{BS}=e*S_{BS}^{-1}*P+K*S_{BS}^{-1}*T_{BS}*P$.

Then, it verifies:

If (U_{BS}=X) then MS it calculates:
$e=H(T_{BS})$ and $S_{MS}=u_{MS}^{-1}(e+T_{MS}*K) \bmod n$.
else MS terminates the execution.

1.4 BS→MS: {RNG-REP}K_{BMS}

- BS Calculates:
  - $e=H\ (T_{BS})$,
  - $w=S_{MS}^{-1} \bmod n$,
  - $U_1= (e*w) \bmod n$,
  - $U_2= (K*w) \bmod n$,
  - $X= U_1.P+ U_2.T_{MS}.P$
  - $U_{MS}=e*S_{MS}^{-1}*P+k*S_{MS}^{-1}*T_{MS}*P$.

Then, it verifies
if (U_{MS}=X) ***then***
BS sends {RNG-REP}K_{BMS} to the MS
else BS terminates the execution.

All further ranging messages mast be encrypted using the shared key K_{BMS}. This key is not limited to secure the ranging process but it secure also Negotiation Basic Capabilities (SBC) process.

2- Proposition to secure Authorization phase

2.1 MS →BS:***Mancert(MS);***

MS sends a message to BS, which contains an X.509 certificate identifying MS's manufacturer.

2.2 MS→BS***:{{MSCert,Nms1}pk(BS),Capabilities,SAID, Tpms, Nms}sk(MS);***

MS sends a second message without waiting for an answer from the BS. This second message contains the MS certificate (MsCert) and a nonce (Ns1) used for identification, both are encrypted with the public key of the BS pk(Bs), it also contains the timestamp of MS and generated nonce of MS along with SAID and its security capabilities. MS signs the message ensuring the BS that he/she is not an adversary with her private key sk(MS), the time stamp addition could bring an extra layer of security since the BS could identify the message as current one. The time stamp could avoid the intruders who are trying to synchronize time with either BS or MS.

2.3 BS→MS***: {{prePAK}sk(Bs), SAIDlist, Tpms, Tpbs, Nms, Nbs,prePAKSeq,prePAKlifetime,BsCert}pk(MS);***

If BS determines that the MS is authorized it replies with a message. BS sends a generated nonce along with nonce, which was sent by the MS. That could ensure MS that received message is the reply of the request send by 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 secret key of BS sk(Bs), The AK is derived from Pre-AK. Use of Pre-AK gives the opportunity to avoid AK sending in raw format (though encrypted with the public key). The Lifetime of Pre-AK and Sequence number of pre-AK are sent in this message.

2.4 MS→ BS:{***Nmb,Tpms }sk(MS);***

From pre-PAK, the MS generates AK. If AK is used correctly, then MS gains the authorization to access the Wimax. As this message sends the BS certificate, the MS is now sure that the message is not copied by the adversaries.MS sends its Timestamp and the nonce of BS previously received to confirm authorization access. MS signs the message with its private key.

3- Proposition to Exchange of TEKs phase:

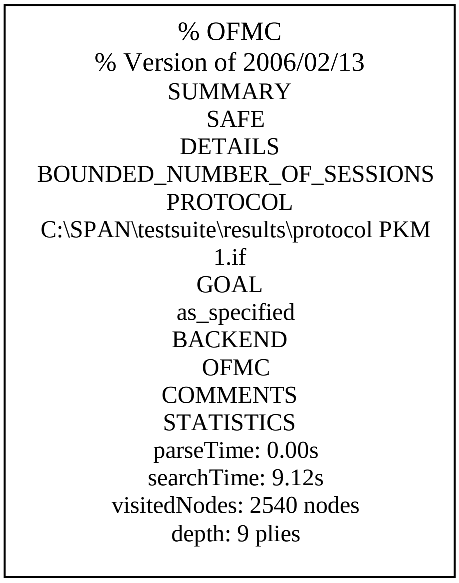
After the authentication procedure has been done, the AK is used to derive three additional keys. For verifying the source and integrity of messages, the standard use message authentication (HMAC) keys. A KEK is also derived from the AK. The KEK is used for key exchange messages to acquire the TEK (Transmission Encryption Keys) used when transmitting data.

The exchange of TEKs is vulnerable to the replay attack. If an attacker replays the first message, the BS will assign and send new keying material using a KRspMess message. The legitimate MS, will think that it is the BS, which requested the rekeying and sent the first optional message. Consequently, this attack causes both the MS and BS to exchange keying material without intending to. To prevent replay attack, we used the timestamp attached with nonce in all messages to exchange the TEK key.

3.1 BS→MS:***Tpbs,Nbs,SeqNo,SAID,HMAC(RkeyMess).***
3.2 MS → BS: ***Tpbs, Tpms, Nbs, Nms, SeqNo, SAID, HMAC(KReqMess)***
3.3 BS → MS: ***Tpms, Nbs,*** $(TEK)_{KEK}$***, TEKSeqNo, TEKlift, HMAC(KRepMess)***

V. Formal Security Verification of (SNEP) Using AVISPA Tool

In this section, we provide a formal security verification of our protocol (SNEP) using Automated Validation of Internet Security Protocols and Applications (AVISPA) [18] and the Security Protocol Animator for AVISPA (SPAN) to prove the resistance of the proposed protocol (SNEP) against the various types of attacks. 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 Fig. 1. The simulation results indicate that our proposition are safe and that no attack has been found.



```
% 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
```

Fig. 1. Results of the formal verification of the proposed scheme using OFMC back-end.

VI. Conclusions

The Network Entry and initialization, 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 and a revised authentication protocol (authorization phase and exchange of TEKs phase) is proposed by using nonce and timestamp together in |. The proposed solution has been implemented with formal verification tool AVISPA and results show that (SNEP) resist to various attacks. SNEP is not limited to secure the ranging process but it secure also all phases of Network Entry.

References

[1] A. Sangwan and V. R. Singh, "A secure authentication scheme for WiMax network and verification using Scyther tool," *International Journal of Applied Engineering Research*, vol. 12, no. 11, pp. 3002-3008, 2017.

[2] 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.

[3] J. Sangeetha, N. Goel, R. P. Rustagi, and K. N. B. Murthy, "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, 2017.

[4] B. A. Alomar, A. R. Ali-Ali, and T. Landolsi, "WiMAX multiple hops architecturein smart grid communications," *Journal of Communications*, vol. 11, no. 9, pp. 805-812, 2016.

[5] H. Labiod, H. Afifi, and H. De Santis, "Wi-FiTM, BluetoothTM, ZigbeeTM and WiMaxTM," *Springer*, 2007, pp. 1-311.

[6] S. Ahson and M. Ilyas, "WiMAX standards and security," CRC Press Taylor & Francis Group Francis Group, LLC. 2008, pp. 1-251.

[7] S. Y. Tang, P. Muller, and H. R. Sharif, *WiMAX Security and Quality of Service an End-To-End Perspective*, John Wiley & Sons Ltd, 2010, pp. 1-425.

[8] A. Akhunzada, S. Murtaza, A. R. Cheema, and A. Wahla, "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, 2009.

[9] S. Hasan and M. Qadeer, "Security concerns in WiMAX," in *Proc. First Asian Himalayas international Conference on Internet*, 2009, pp. 1-5.

[10] P. K. Gandhewar and P. P. Lokulwar, "Improving security in initial network entry process of IEEE 802.16," *International Journal on Computer Science and Engineering*, vol. 3, no. 9. pp. 3327-3331, 2011.

[11] S. Naseer, M. Younus, and A. Ahmed, "Vulnerabilities exposing IEEE 802.16e networks to DoS attacks: A survey," in *Proc. ACIS International Conference on*

Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing Ninth, 2008, pp. 344-349.

[12] J. Han, M. Y. Alias, and G. Min, "Potential denial of service attacks in IEEE802.16e-2005 networks," *Communications and Information Technology*, 2009, pp. 1207–1212.

[13] B. Sridevi, M. Brindha, R. Umamaheswari, and S. Rajaram, "Implementation of secure & cost effective authentication process in IEEE 802.16e WiMAX," *International Journal of Distributed & Parallel Systems*, vol. 3, no. 2, pp. 215–229, 2012.

[14] S. Maru and T. X. Brown, "Denial of service vulnerabilities in the 802.16 protocol," in *Proc. 4th Annual International Conference on Wireless Internet*, Maui, HI, USA, 2008, pp. 1–9.

[15] A. Akhunzada, S. Murtaza, A. Raza Cheema, and A. Wahla, **"**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, 2009.

[16] S. Pahal, B. Singh, and A. Arora, "Cross layer trigger-based handover scheme for mobile WiMAX network," *International Journal Ad Hoc and Ubiquitous Computing*, vol. 19, no. 3-4, pp. 133–142, 2015.

[17] M. Gilanian-Sadeghi, B. M. Ali, and J. A. Manan, "Key management in mobile WiMAX," Chapter 6 form Selected Topics in WiMAX Networks, Intech, 2013, pp. 130-148.

[18] AVISPA Project. (2006). AVISPA Protocol Library. [Online]. Available: http://www.avispa-project.org/

Noudjoud Kahya was born in Algeria. She is currently pursuing the Ph.D degree with the Department of Computer Science at Badji Mokhtar University, Annaba, Algeria. She is researcher and member of the Laboratory Networks and Systems. Her research interests include wireless networks, WIMAX, security in protocol, and cryptography.

Nacira Ghoualmi-Zine is a Professor in Computer Sciences and has been a Lecturer in the Department of Computer Science at Badji Mokhtar University, Annaba, Algeria since 1985. She is the Head of the Master and Doctoral option entitled Network and Computer Security, and Head of a Laboratory of Computer Networks and Systems. Her research includes cryptography, computer security, intrusion detection system, wireless networks, distributed multimedia applications, quality of service, and security in the protocol.

Marwa Ahmim is a PhD in Computer Sciences and has been a Lecturer in the Department of Computer Science at Badji Mokhtar University, Annaba. She is a member of the Laboratory of Computer Networks and Systems. Her research interests include computer security, security metric, cryptography, and security analysis.