An Overview on WiMAX Security Weaknesses/Potential Solutions

Daniel SIMION, Mihai-Florentin URSULEANU, Adrian GRAUR
Stefan cel Mare University of Suceava
dasimion@eed.usv.ro

***Abstract* — Nowadays anyone from anywhere in the all world can access all types of data with a high level of QoS. The wireless industry continues to change day by day, tending to use the equipment more easily and safely and with a connection speed that tends to be higher and higher. But this mobility has its price. Intruders or illegitimate users can access important data and data is money. For this reason technologies used in data transmission need extra data security. Even if WiMAX technology has complex authentication and authorization methods and very strong encryption techniques is still vulnerable on different attacks or threats like jamming, scrambling or water torture attacks.**

This paperwork is an overview of most threats involved in infrastructure and WiMAX deployment and the security solutions needed to overcome them.

***Index Terms* — attacks, security, threats, WiMAX, wireless.**

I. INTRODUCTION

Security threats are a problem that needs more research in order to find solutions to these threats, fact that will help WiMAX to become a successful and reliable technology.

To exchange data with a higher protection between MAC and PHY layers, WiMAX has define a security sublayer on the ground of the MAC layer, which contains privacy and key management and protects the data communication from hijacking attacks between SS (Subscribe Station) and BS (Base Station). The PKM (Privacy Key Management) protocol represents the main protocol from security sublayer which provides authentication, key management and a better privacy for data traffic. Also, protection keys, like AK (Authorization Key), TEK (Traffic Encryption Key), KEK (Key Encryption Key) or HMAC (Message Authentication Key), which are used in security sublayer, provide a better security for WiMAX technology. But security risks, threats or vulnerabilities are still available for WiMAX technology.

II. WiMAX ARCHITECTURE

The WiMAX protocol architecture is structured into two major layers (see Fig. 1): - the MAC layer and the PHY layer.

MAC layer contains 3 sublayers. Starting from the base, the first sublayer is SS which encrypts and decrypts the data which are entering and leaving in and from PHY layer. This sublayer uses for data traffic 56bit DES (Data Encryption Standard) encryption and for Key Exchanges uses 3DES encryption [1].

The second MAC sublayer is the CS (Service Specific Convergence Sublayer). This sublayer maps higher level data services to MAC layer service flow and connections [2, 3, 4].

The third sublayer is the CPS (Common Part Sublayer). In this sublayer are constructed the MPDUs (MAC Protocol Data Units). The CPS sublayer defines rules and mechanisms for ARQ (Automatic Repeat Request 10), for connection control and for system access bandwidth allocation. It also provides centralization, channel access and duplexing. CS and CAP are communicated by MAC SAP (Service Access Point) [1].

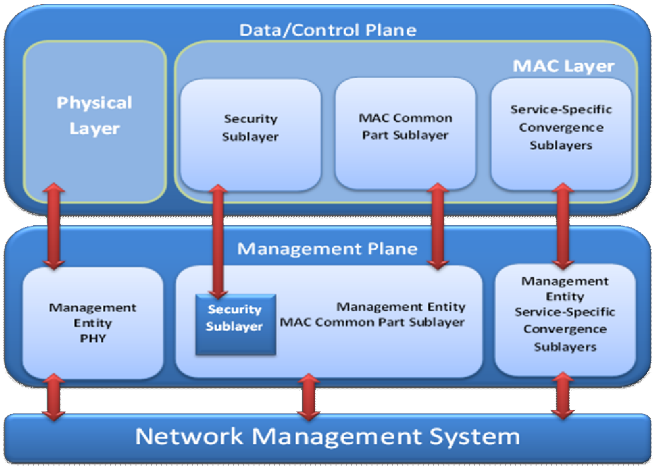

Figure 1. WiMAX Protocol Layers

The PHY layer it's a connection between MPDU and the PHY layer frames with the encoding of the radio frequency signals when sent and received through modulation.

WiMAX technology architecture was created so as to allow its connection with IP networks which provide Internet services.

III. WiMAX SECURITY ELEMENTS

The whole security mechanism of WiMAX technology is defined by SA (Security Association), X.509 certificates, PKM Authorization, Privacy and Key Management and Data Encryption [2].

Security policies are enforced by the BS to the SS, so it can only access authorized SA that respects the characteristic of that type of service. One SS may have one till three different SAs; one for the secondary management channel and one/two for uplink/downlink channels. The downstream being protected by the primary SA, in multicast communication the primary SA can't protect it. For this reason are used static and/or dynamic SAs.

IEEE 802.16 standard supports 2 types of SAs – data and authorization SA. Data SAs protects the data transport connections between BS and SS and authorization SAs

establishes the data SA and authorizes the SS to access the BS.

A *X.509 certificate* is used for identification of SS. The standard doesn't define certificates for BS. A *X.509 certificate* defines an authentication algorithm based on public-key techniques. Every SS has its own X.509 digital certificate which contains the SS's MAC address and the public key. The base station authenticates the subscribe stations when initial authorization exchange and in requesting time of an AK, SSs present to the BS the own digital certificate. After, the BS checks them and used the public key for AK encryptions. Requesting SSs receive back the AK and the BS associates for each SS an authentication identity, on which SSs are authorized to access, with the AK exchange, services like data, video or voice.

So, BS can avoid the cloned SSs attacks (*masquerades attacks*). SSs have RSA public/private key pairs installed at the factory or have an algorithm which generates dynamically RSA key pairs. In the second case, if the SS must generate its RSA key pair, this key pair will be generated before the AK exchanges. For this reason SSs need to support a mechanism which installs the X.509 certificates issued by the manufacturer. Attackers must crack the encryption of the X.509 certificate used and must have an SS from the same manufacturer for succeeding his attacks on the BS, pairing between SSs can only be achieved if they have preinstalled from the factory a RSA private/public key.

In WiMAX, the security of connections access is accomplished by complying with the *Privacy Key Management protocol*. The utility of this protocol is that it provides periodical and normal authorization of SSs; it distributes keying material to them and also provides key refresh and reauthorization. Another task of PKM is to insure that the authentication algorithms and supported encryption are correctly applied to the exchanged MPDUs.

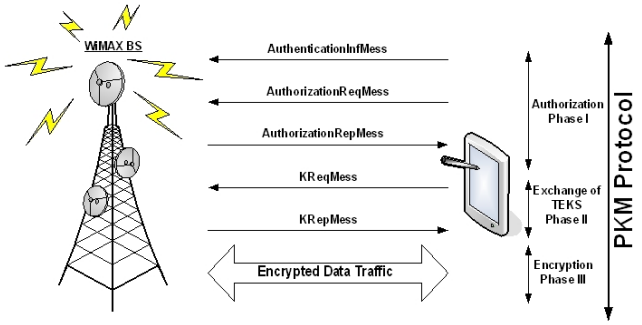

Figure 2. PKM Protocol Phases

In order to securely exchange keys between BS and SS, the PKM protocol uses the symmetric cryptography and X.509 certificates.

As it is shown in Fig. 2, the protocol is based on three phases. The BS plays the role of the server and it manages identification keys to the SS, who plays the role of client. The BS authenticates a SS client using PKM protocol in the initial authorization exchange. SS uses a digital certificate for authentication at the BS. Also, the BS uses a shared secret encrypted key, which can be periodically changed by the SS, to communicate with the SS, key provided by PKM protocol.

SS transmit an authentication message (*AuthenticationInfMess*) which contains the certificate of SS producer. In the same time, SS transmit another message which contains the authorization Request Message (*AuthorizationReqMess*) that request an AK (Authorization Key). The *AuthorizationReqMess* contains the SS's certificate; the cryptographic capabilities which contains a stack of cryptographic layers with a packet of data authentication and encryption algorithms and the SAID (Security Association IDentifier) whose value is the same with the primary 16Bit CID (Connection IDentifier) that the BS transmits to the SS at the initialization and network entry phase. After that, the BS will verify the X.509 digital certificate; will choose the encryption algorithm and then will send the authentication response. Finally, SS receives it's the RSA-public key encrypted AK from the BS.

This process of authentication and key exchange between SS and BS, the first step of the PKM, is presented in the Fig. 3.

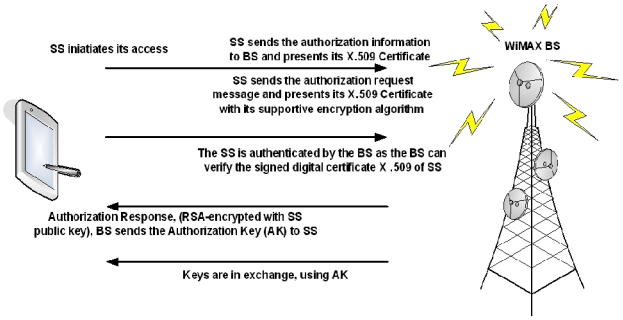

Figure 3. Authentication and Authorization Key allocation by the BS

Next, a data SA is established by the PKM protocol through the exchange of TEKs (see Fig. 4).

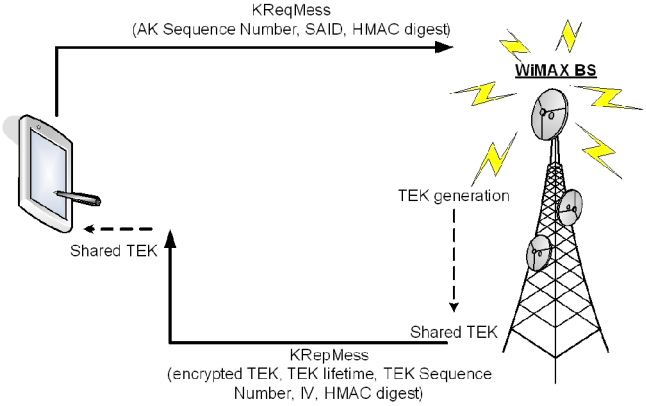

Figure 4. TEKs Exchange

The BS is prompted by the SS at regular intervals with a renewal of TEK using Key Request Message (KReqMess). The BS verifies the authenticity of the KReqMess and compares the SAID from the SA with the SS and if they match the HMAC digest it will respond to the message. In that message a Reply Message (KRepMess) key is also added, key used by the TEK state machine. In the KRepMess message there are data that contains TEK-Parameters and the BS can extract two active keys per SAID, that he stores.

The KRepMess message is composed of an AK sequence number, the SAID, the parameters linked to the old TEK, and the new TEK and an HMAC digest - in order to ensure the SS that the message is being sent by the BS without

being tampered with. It is known that the validity durations of the two TEKs overlap. The new TEK is being activated before the old TEK expires, and the old TEK is destroyed after ensuring that the new TEK was activated. In order to estimate when the BS will invalidate a previous TEK or request a new TEK, the SS uses the lifetime of a TEK. The BS will reply with a Key Reject Message which contains the AK sequence number, the SAID and an error code with an indication regarding the reason of rejection and a HMAC digest. The SS could thus resend a different KReqMess message to obtain a new TEK if the SAID in the KReqMess message is invalid. The third phase of Privacy Key Management Protocol is *Data Encryption* phase. The transmitted data between the SS and BS begins to be encrypted using the TEK only after achieving the SA authorization and the TEK trade [5].

Each SA has 2 TEKs created by the BS. If one expires it makes a new one. The downlink traffic is encrypted with the old key. The other key can be used to decrypt the uplink traffic.

Fig. 5 illustrates a SS request to the BS for TEK0 and TEK1 encryption keys. The BS changes its key every time is expiring.

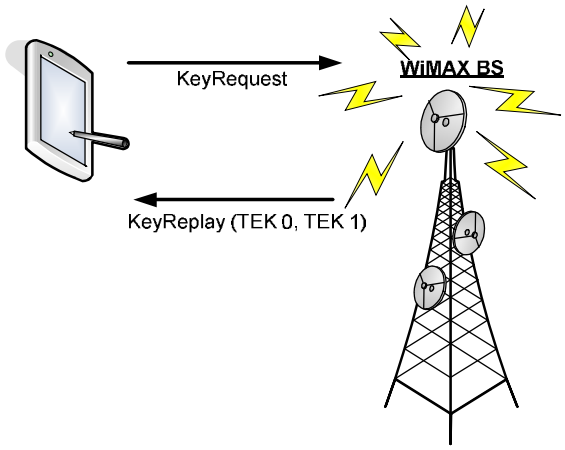

Figure 5. SS sends a request to the BS for TEK0 and TEK1 encryption keys

The SS uses the newer of the two keys for encrypting the uplink traffic. On the other hand, for the downlink traffic, can be used either of the two keys - depending upon which key is used by the BS at that moment.

It is known that the TEKs have a limited lifetime and have to refresh regularly. The BS can use the newer TEK for encryption when the older TEK expires. It is the duty of the SS to bring up to date its keys periodically. A KEK is used by the BS in order to encrypt the TEK in the Key Reply (PKM-RSP) MAC management message.

The TEK can be encrypted using one of the following algorithms, using the KEK: 3-DES, RSA or AES (Advanced Encryption Standard). The TEK encryption algorithm is specified by the TEK encryption algorithm identifier in the cryptographic suite of the SA.

IV. WiMAX SECURITY THREATS

Security algorithm of WiMAX technology is implemented in the security sub layer, at the bottom of MAX layer and above to the PHY layer. Thus, the PHY layer it's an open door for the hackers. IEEE 802.16 is vulnerable at the attacks like jamming, scrambling or water torture attack, most of all that supports mobility.

Thus, the PHY layer it's an open door for the hackers. IEEE 802.16 is vulnerable at the attacks like jamming, scrambling or water torture attack, most of all that supports mobility.

Like Michel Barbeau says in [6], a jamming attack is an attack *achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel*.

A jamming attack can be easily launched, deliberately or undeliberately, with some equipments (radio spectrum monitor, for example), which are easy to obtain. In [7] are describe, step by step, techniques for this kind of attack. This type of attacks is a dangerous one and very difficult to be detected.

A scrambling attack is presented in Fig. 6.

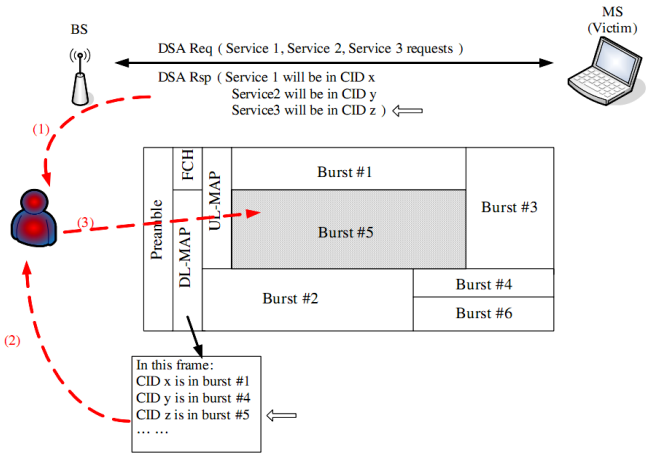

Figure 6. Scrambling attack procedure [7]

In this scenario attackers wish to scramble the service 3. First of all, he must sniff the DSA (Digital Signature Algorithm) message and then the MAP information. With this information, the attackers know from the frame the target data region and can send interference signals.

Another threat in WiMAX wireless networks is when the attacker sends a series of frames to consume the receiver's battery; this kind of attack is called Water Torture (see Fig. 7).

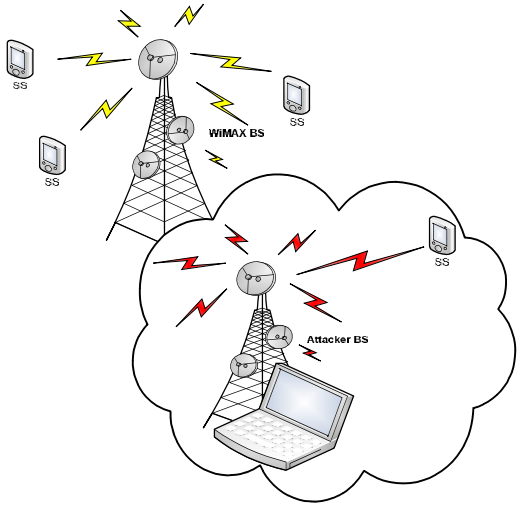

Figure 7. Attacker BS uses Water Torture to create DoS attack

Like most wireless networks, the signal may be high jacked using a RF receiver so a measure to prevent this type

of behavior is required (maybe a cryptographic security mechanism which can be maintained while a mobile Subscribed Station (SS) changes between WiMAX BS). Data authenticity technology is required in order to prevent an attacker with a RF sniffer to capture, change and retransmit data frames to the WiMAX BS. When the transmission range is longer, a detection mechanism for relayed frames is needed to prevent attackers to forward data frames, from authorized stations that can't communicate directly.

Other threats in IEEE 802.16 standard are - forgery attacks – using the wright radio technology an attacker can write to a wireless channel [8] and replay attacks – an attacker resend legitimate frames that he was intercepted its in the relaying process (or middle of forwarding).

A considerable threat comes from the WiMAX authentication scheme, where masquerading attacks and attacks on the authentication protocol are the most harmful. The masquerading problem consists of assuming, by a system, identity of another one. A masquerade attack possible can be made by means of sniffing and spoofing.

A masquerade attack can be done in two ways:

- identity theft – is the case an attacker changes the address of a device with another's assuming its identity. The address can be cloned through transmissions that contain management data;

- rogue Base Station attack – in this case a false BS imitates a valid one, case in which all the SSs of that BS are compromised. The SSs think that they are connected to the legitimate BS, when in reality they are connected to the rogue BS and all of the data can be intercepted. Because of the lack of mutual authentication, a MITM attack (Man-in-the-Middle-Attack) can be performed with a fake BS by sniffing messages related to authentication from the SS. If the WiMAX connection supports PKMv2 mutual authentication this attack can't be easily implemented.

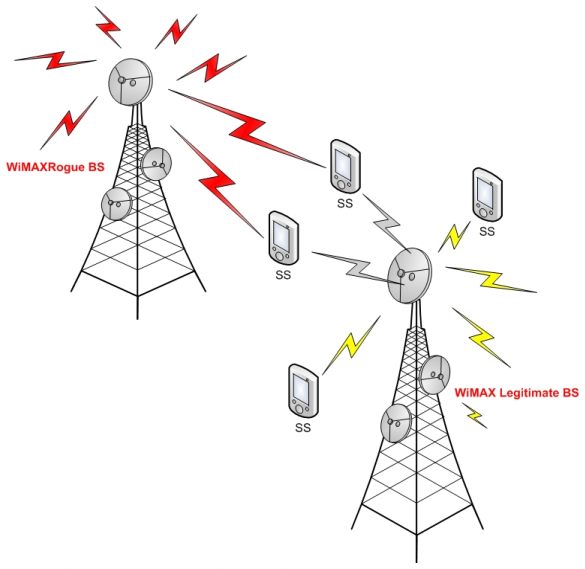

Figure 8. WiMAX Masquerade Attack

PKMv2 fixes a lot of the issues of PKMv1, but it has its own flaws, mostly a weak spot for MITM and other new types of attacks [8].

Vulnerabilities in the MAC layers of the IEEE 802.16 are speculated by attackers. The most important and critical attacks can be the DoS and MITM attacks. With the use of PKMv2 WiMAX can prevent MITM attacks.

A possible solution for this kind of attack is described in [9], where Tao Han (and the others) proposed SINEP (Secure Initial Network Entry Protocol). The SINEP solution is based on DH (Diffie-Hellman) key exchange protocol and enhances the security level throughout network initial. Approximately the same solution is offered in paper [10].

Denial of Service (DoS) attack is one of the most powerful on a wireless communication network.

Some of the most significant DoS attacks are:

- ✓ DoS attacks based on RNG-REG/RNG-RSP (Ranging Request/Response) messages;
- ✓ DoS attacks based on MOB_NBR_ADV (Mobile Neighbor Advertisement) message;
- ✓ DoS attacks based on FPC (Fast Power Control) message;
- ✓ DoS attacks based on Auth-Invalid (Authorization-invalid) message;
- ✓ DoS attacks based on RES-CMD (Reset-Command) message.

The vulnerabilities in the initial network entry should be fixed in order to prevent DoS attacks and solution is that the authentication methods should be extended to as many as management frames as possible. For even a greater security, digital signatures can be used as an authentication method.

V. SOLUTION FOR SECURITY PROBLEMS IN WiMAX NETWORKS

WiMAX standard has two types of certificates, one for SS and one for the manufacturer, and not for BS. This becomes a problem. Subscriber certificate identifies a subscriber by its MAC address. SS certificates are normally created and signed by the manufacturer using public key, this enables the BS to validate a SS certificate and so identify a certain device as genuine. This type of drawback is called *mutual authentication* problem.

Creating a scheme for mutual authentication is the only way that attackers can't forger or replay attack on a BS, for example with X.509 certificate you can verify EAP (Extensible Authentication Protocol) encryption. A defense shield for the *man-in-the middle attacks* or the *forgery attacks* is made by PKM-MSH protocol, which ensures the mutual authentication.

A possible solution for the *jamming attack* was described in [11]. Increasing the power or the bandwidth of signals using techniques like FHSS (Frequency-Hopping Spread Spectrum) or DSSS (Direct-Sequence Spread Spectrum) it can avoid the jamming attacks. Also, with a radio monitoring equipment jamming attacks could be detected and compromised.

The attacks on the DES-CBC encryption algorithm can be avoided by using a randomly generated initialization vector (IV) placed in the payload, instead of the current one that is predictable and the attackers are able to get it. In this way, data won't be decrypted and the attackers won't predict the initialization vector.

To prevent a *water torture attack*, is essential a sophisticated mechanism to reject the false frames. To prevent *forgery and replay attacks* presented above it must

be used mutual authentication.

Also, for the most powerful attacks, *scrambling attacks*, a possible solution, called DCJS (Dynamic CID Jumping Scheme) based on a key-dependent one way function and the DH (Diffie-Hellman) protocol is presented in [12], by Po-Wen Chi.

An essential improvement on WiMAX security mechanism is to add the CertificateChainRequest and CertificateChainReply messages for enabling a node which will verify the AuthorizationsNodeCertificate where the messages complete the RSA authentication within the PKM-MSH.

The IEEE 802.16 standard has improved mutual authentication between BS and SS where random numbers are included to stop replay attacks. In order for the handshake identification to be successfully fallowed the RSA based authentication has incorporated its own certificate.

The handshake identification is done following the next steps [13]:

1) RSA-Request (SS → BS): MS_Random, MS_Certificate, SAID, SigSS.

2) RSA-Reply (SS → BS): MS_Random, BS_Random, Encrypted pre-PAK, Key Lifetime, Key Sequence Number, Bs_Certificate, SigBS.

3) RSA-Acknowledgement (SS → BS): BS_Random, Auth Result Code, Error-Code, Display-String, SigSS.

Regarding cryptographic problems, the 224bit ECC (Elliptic Curve Cryptography) offers 2048bit RSA security instead of 160bits ECC which offers 1024bit RSA. So, 224bit ECC will bring a speedier computational efficiency with the same level of security, memory, and bandwidth and energy savings.

Within PKM-MSH messaging, replay attacks are avoided using random numbers. If a message is hacked and the attackers resend the random generated number in the message it can be detected by the receiver. In doing so, the receiver ignores the message because the random number sequence doesn't match. If the random number is found, the attacker still has to verify the signature. The verification can't be completed because the attacker can not provide the private key.

VI. CONCLUSION

This paper wants to be an overview of most threats involved in infrastructure and IEEE 802.16 (WiMAX Technology) deployment and the security solutions needed to overcome them. The contributions of this research overview helps researchers to better understand the security in WiMAX.

Even if WiMAX technology has complex authentication and authorization methods and very strong encryption techniques is still vulnerable on different attacks or threats. Being still a new technology, a special attention for security improvements is required in IEEE 802.16 standard. We hope that in the future they will become fewer and resolvable.

In conclusion we can say that there are and there will be ways to study security challenges for new wireless technologies until this communications will be 100% safe.

VII. FUTURE WORK

This paper is a part of larger research project about data transmission over wireless network medium.

Future papers will include case studies about contributions to the optimization of data streaming in heterogeneous environments.

Future research work will be done to conceive a scientific paper that includes a survey about simulation medium in IEEE 802.16 with a goal of improving security elements in wireless traffic.

ACKNOWLEDGMENTS

This paper was supported by the project "Knowledge provocation and development through doctoral research PRO-DOCT - Contract no. POSDRU/88/1.5/S/52946", project co-funded from European Social Fund through Sectoral Operational Program Human Resources 2007-2013.

REFERENCES

[1] Rysavy Research and 3G Americas, "EDGE, HSPA & LTE. The Mobile Broadband Advantage", September 2008 (whitepaper).

[2] Raj Jain and Trung Nguyen, "A survey of WiMAX security threats", Project report, 2009.

[3] Abdelrahman Elleithy, Alaa Abuzaghleh, Abdelshakour Abuzneid, "A new mechanism to solve IEEE 802.16 authentication vulnerabilities", Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT.

[4] Mohsen Gerami, "A survey on WiMAX", IJCSIS– International Journal of Computer Science and Information Security, vol. 8, No. 2, 2010, ISSN 1947-5500, pp. 352-357.

[5] Slim Rekhis and Noureddine Boudriga, "WiMAX Security Defined in 802.16 Standards", Ed. John Wiley & Sons, Ltd, 2010.

[6] Michel Barbeau, "WiMAX/802.16 Threat Analysis", Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks - Q2SWinet '05, New York, USA, ACM, October 13, 2005, ISBN: 1-59593-241-0, pp. 8-15

[7] Richard A Poisel, "Modern Communications Jamming Principles and Techniques", Artech House Inc. Publisher, USA, ISBN 1-58053-743-x, 2004

[8] David Johnston and Jesse Walker, "Overview of IEEE 802.16 Security", Journal of IEEE Security and Privacy, IEEE Educational Activities Department Piscataway, NJ, USA, vol. 2, issue 3, May, 2004, ISSN: 1540-7993, pp. 40-48.

[9] Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang and Yuan'an Liu, "Analysis of mobile WiMAX security: Vulnerabilities and solutions", 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems - MASS 2008, Atlanta, October 2008, ISBN: 978-1-4244-2574-7, pp. 828-833.

[10] Taeshik Shon and Wook Choi, "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", Proceedings of the First International Conference on Network-Based Information Systems, Springer-Verlag LNCS No.4658, September 2007, p.88.

[11] Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara and Toshiaki Tanaka, "Security Vulnerabilities and Solutions in Mobile WiMAX", IEEE, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007, pp. 7-15.

[12] Po-Wen Chi and Chin-Laung Lei, "A prevention approach to scrambling attacks in WiMAX networks", WoWMoM'09, IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops, 15-19 June, ISBN: 978-1-4244-4440-3, 2009, pp. 1-8.

[13] Md. Rezaul Karim Siddiqui and Sayed Mohammad Atiqur Rahman, "Security analysis of the WiMAX Technology in Wireless Mesh networks", Master thesis, Blekinge Institute of Technology, Karlskrona, Sweden, 2009, pp. 45.