WIMAX 802.16 NETWORK – SECURE COMMUNICATIONS

Cătălin-Teodor DOGARU[1], Teodor PETRESCU[2]

"Worldwide Interoperability for Microwave Access" (WiMAX) reprezintă deja una dintre tehnologiile cele mai des utilizate în momentul în care vorbim de asigurarea accesului de bandă largă în cazul conexiunilor fără fir. Dacă, pentru cazul 802.11, problemele de securitate au fost tratate dupa finalizarea standardului, pentru 802.16, aceste probleme au constituit o prioritate. Cum WiMAX-ul reprezintă totuşi o tehnologie nouă, implementările curente nu sunt încă suficiente pentru a evidenţia eventualele vulnerabilităţi, riscuri sau ameninţări ce pot afecta comunicaţia în cazul unui trafic real.

Acesta este şi motivul pentru care vom încerca sa tratăm în această lucrare posibilele probleme de securitate ce pot apărea printr-o analiză atentă a standardului 802.16 (WiMAX).

"Worldwide Interoperability for Microwave Access" (WiMAX) represents one of the most important technologies of the moment when we are talking about providing Broadband Internet using wireless connections. As a wireless protocol, WiMAX has an additional set of security threats not faced in cable systems. Because the DOCSIS protocol was developed for cable modems, not wireless systems, the original 802.16 standard does not provide enough security for the intended purpose. The standard threats for wireless systems still apply to WiMAX systems, in particular all the attacks to the higher levels. We present in this article an overview of the security aspects of this standard.

Keywords: WiMAX, security, wireless, standard 802.16, VPN, authorization, authentication, attack, vulnerabilities, solutions

Abbreviation List:

- ASCII - American Standard Code for Information Interchange
- ATM – Asynchronous Transfer Mode
- CID – Connection Identifier
- DES – Data Encryption Standard
- DOCSIS - Data Over Cable Service Interface Specifications
- EAP – Extensible Authentication Protocol

[1] PhD student, Department of Electronics Engineering and Telecommunications, University POLITEHNICA of Bucharest, Romania, cătălin.dogaru@yahoo.com
[2] Professor, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania

- KEK – Key Encryption Key
- OFDM – Orthogonal Frequency Division Multiplexing
- PDU – Protocol Data Unit
- PHY – Physical Layer
- PKM – Privacy Key Management
- QAM – Quadrature Amplitude Modulation
- RSA - Ron Rivest, Adi Shamir, and Leonard Adleman
- TEK – Traffic Encryption Key
- WiMAX – Worldwide Interoperability for Microwave Access

1. Introduction

Security is an ever moving target that must be continually managed and refined to ensure appropriate confidentiality, integrity, and availability of the services and systems that are critical to your business, as well as the valuable information that is often at the heart of the organizations we defend. And, when the infrastructure for the network is based on a wireless technology, the perception is that the whole communication is more vulnerable.

If we add that the *WiMAX* technology is one of the newer technology to be used for broadband wireless access, we can have a better *picture* of the work that we want to implement – define the security aspects for IEEE 802.16 networks, as we can obtain them based on the carefully reading of the standards and on the revision of the white papers for the different developments from different leading producers in this field.

Our goal for this paper will be to address the security aspects of the IEEE 802.16 standards and to point out the security vulnerabilities, threats and risks associated with this standard. At the end of the paper, we will offer an **example** of security procedures (authentication, authorization) for a most common architecture used nowadays – VPN-kind architecture.

The final goal for the whole research (presented in our Ph.D. Thesis) will be to obtain **a new security plan (and a corresponding architecture)** which can be applied by any operator who wants to develop a new *WiMAX* network.

2. General overview for the WiMAX/802.16 layers

WiMAX/802.16 defines two layers of the protocol stack, physical (PHY) and medium access control (MAC). The MAC layer manages connections and security. The PHY handles signal connectivity and error correction, as well as initial ranging, registration, bandwidth requests, and connection channels for management and data. The PHY layer consists of a sequence of equal length

frames transmitted through the coding and modulation of RF signals. Physical frames, and also MAC frames, do not necessarily begin or end on boundaries of higher layer frames—this is handled by intermediate mapping layers. Intermediate mapping gives 802.16 the flexibility to support a wide variety of traffic types and profiles in the transport layer and above, including IP, Ethernet, and ATM, with a high level of efficiency

3. IEEE 802.16 - Physical Layer

WiMAX uses OFDM technology. Orthogonal frequency-division multiplexing (OFDM) allows assigning sub-carriers to different users. In the IEEE 802.16 standard from 2004, the OFDM signal is divided into 256 carriers, while for the version 802.16e (mobile WiMAX), we will use Scalable OFDMA (Orthogonal Frequency Division Multiple Access). The standard 802.16 supports a wide range of frequencies and the physical layer contain different forms of modulation and multiplexing. The modulation methods used for the uplink (from the subscriber to base-station) and for the downlink (from base station to subscriber) are BPSK (Binary Phase Shift Keying) or 2-QAM (Quadrature Amplitude Modulation), QPSK (quaternary PSK) or 4-QAM, 16-QAM and 64-QAM.The IEEE 802.16 supports two types of transmission duplexing: Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) and support both full and half duplex stations. TDD framing is adaptive and it has a fixed duration. In FDD, while transmissions are still scheduled by DL-MAP and UL-MAP, uplink and downlink communications take place at the same time, but on different frequencies. Frame duration can be set to 0.5, 1 or 2 milliseconds. In TDD, the portion allocated for the downlink and portion allocated to the uplink may vary. The Uplink is time division multiple access (TDMA) where bandwidth is split into time slots. Each time slot is allocated to an individual MS (mobile station) being served by the BS. A downlink sub-frame contains two parts. One part is for control information, which holds preamble for frame synchronization &maps and the other contains data. A Downlink map states the starting position and transmission attributes of the data bursts. An Uplink map states the allocation of the bandwidth to mobile station (MS) for their communication.

One may ask why not use code division multiple access (CDMA) as a signaling format (as we do for the usual Wi-Fi case). CDMA requires a bandwidth that is much larger than the data throughput to maintain a processing gain capable of overcoming interference. Furthermore, OFDM and OFDMA support NLOS performance making maxi-mum use of the available spectrum.

4. IEEE 802.16 – MAC (Medium Access Control) Layer

The transmission scheme for 802.16 MAC is connection oriented. All data communications are defined in the context of a connection.

The MAC Layer of IEEE 802.16 was designed for point to multipoint (PMP) broadband wireless access applications. But, as soon as the mobility standard – IEEE 802.16e-2005 – was approved, the discussions can also be applied to mesh architectures [6].

IEEE 802.16 standard is made up of a protocol stack with properly defined interfaces. There is a Base Station (BS), as the Access Points in 802.11, and several Subscribers Stations (SS). BS is basically wired and it broadcasts to the Subscriber Stations (SS).In contrast to 802.11 CSMA/CA method, 802.16 uses Uplink and Downlink maps to confirm collision free access. SS uses Time Division Multiple Access (TDMA) to share the uplink, while BS uses TDM (Time Division Multiplexing). All these functions are done through UL-MAP and DL-MAP messages.

The standard 802.16-2004 is designed to carry any present or future higher-layer protocol such as IP versions 4 and 6, voice-over-IP (VoIP), Ethernet, ATM and virtual LAN (VLAN) services. 802.16 accomplish this by dividing its MAC layer into separate subLayers that handle different services.

MAC layer consists of three sub layers [5]: Service Specific Convergence SubLayer (MAC CS), the MAC Common Part SubLayer (MAC CPS) and the Privacy SubLayer (see Fig.1).

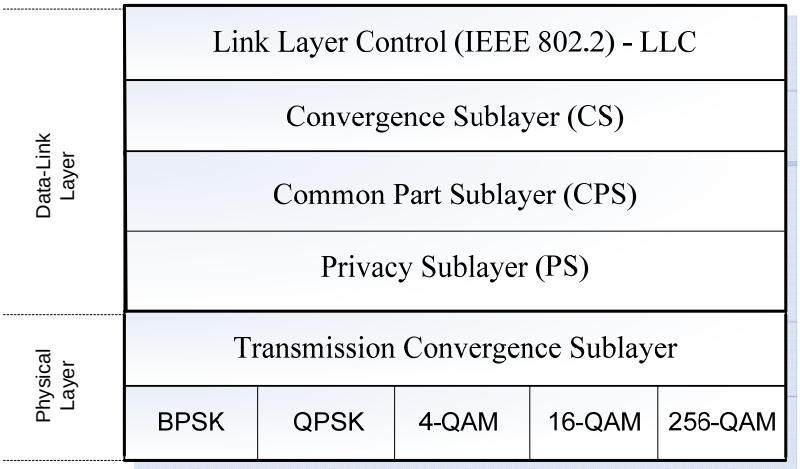

Fig. 1 MAC and PHY Layers and SubLayers for IEEE 802.16

The Privacy Sublayer is accountable for the encryption and decryption of data that is coming and leaving the Physical layer [1].

It carries 56-bit DES encryption for traffic and 3-DES encryption for key exchanges. In IEEE 802.16 network, the Base Station (BS) has 48-bit base station ID, which is not a MAC address and Service Station (SS) has 48-bit 802.3 MAC address [3].

The 16-bit connection identifier (CID), used in MAC PDU (Protocol Data Units), functions as a reference for all connections and is constantly granted bandwidth on demand. There are two types of MAC connection: one is Management connection and the other is Transport connection [2]. MAC layer connections are like TCP connections. For example, the SS can have several connections to a BS for different services, like for network management or for data transport. In MAC, all associations use different parameters for priority, bandwidth and security. BS always assigns CID for SS. As soon as a SS joins a network, three different CIDs are allocated to it. Moreover, each CID has separate QoS requirements.

The basic function of CS Layer is that it receives data from higher layers, classifies data as ATM cell or packet and forwards frames to CPS layer. The core part of the IEEE 802.16 MAC is the MAC CPS, which defines all methods for connection management, bandwidth distribution, request & grant, system access procedure, uplink scheduling, connection control, and automatic repeat request (ARQ). Communication between management connection levels: Primary (authentication and connection setup), Basic (used to transfer brief, time-critical MAC and Radio Link control messages) and Secondary Management connections (transfer standards--based management messages i.e. DHCP, TFTP, and SNMP). Both basic and primary management connections are created when a MS (Mobile station)/SS is joined to a BS network Transport connections can be established on demand. They are used for user traffic flows, unicast or multicast transmission. Additional channels are also reserved by the MAC to send out uplink and downlink schedule. A single CID can carry traffic for many different higher-layer sessions.

We have to mention that 802.16 MAC is connection oriented even for connectionless transmissions such as IP. Connectionless transmission is mapped into a connection, which is used as a pointer to destination and context information.

4.1 Format of MAC messages – MAC PDU

MAC Protocol Data Units (MPDUs) contains exchange messages of BS MAC and SS MAC. It has three parts: a fixed length MAC header, which contains frame control information; a variable-length Payload (frame body) and a frame check sequence (FCS), which holds IEEE 32-bit CRC. We can see a generic representation of the MAC PDU in fig.2.

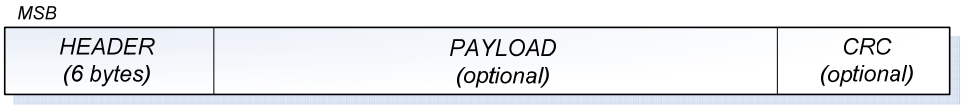

Fig. 2 Format of MAC PDU

Again, MAC header types are: MAC Service Data Unit (MSPU), where payloads are MAC SDUs segments, e.g. data from the upper layer (CS PDUs). Second one is, Generic MAC header (GMH) where the payloads are MAC Management messages or IP packets encapsulated in MAC CS PDUs. Both are transmitted on management connections. The third one is Bandwidth Request Header (BRH) which is sent out without payload.

Except the Bandwidth Request PDUs, MAC PDUs may hold either MAC management messages or convergence SubLayer data - MSDU. For both GMH and MSDU, Header Type (HT) bit is always set to 0 (zero) while Bandwidth Request Header is set to 1. The MAC header contains a flag, which indicates whether the payload of the PDU is encrypted or not.

The header for MAC PDU is presented in the fig. 3. We have to mention that this header is valid for all the PDUs excepting the Bandwidth Request PDU.

The description of the fields is offered in the Table 1.

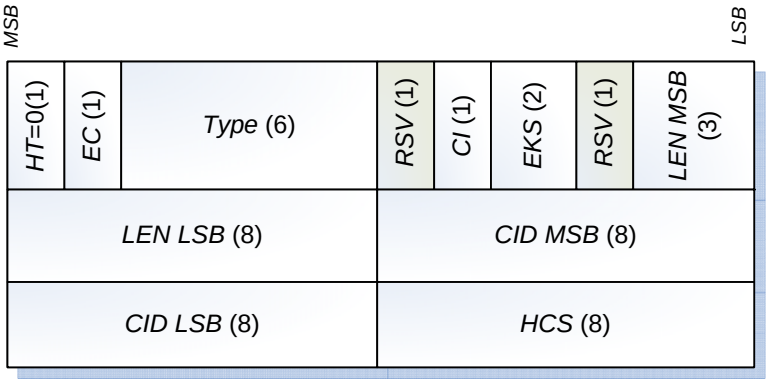

Fig. 3 Presentation of the header for non-bandwidth request PDUs

Table 1

Field description for the header for non-bandwidth request PDUs

Field name	Length (bits)	Description
HT	1	*Header Type*
EC	1	*Encryption Control* 0 – uncrypted ; 1 – encrypted
Type	6	This field indicates the sub-headers and special payload types present in the message payload
Rsv	1	Reserved
CI	1	*CRC Indicator* 0 – no CRC ; 1 – with CRC
EKS	2	*Encryption Key Sequence* – valid only if *EC*=1
LEN (*MSB/LSB*)	3	*Length* – for *MPDU* (including header and *CRC* – if any)
CID	16	*Connection Identifier*
HCS	8	*Header Check Sequence*

According to IEEE Standard 802.16-2001, MAC header and all MAC management messages are not encrypted. This decision was made to "facilitate registration, ranging and normal operation of the MAC SubLayer"[4] as it allows generation of false management messages. Consequently, this leads to vulnerabilities. Otherwise, if encrypted, spoofing was difficult during BS and SS had exchanged encryption keys. In case of vulnerabilities in management messages, authentication will be exposed to eavesdropping, man in the middle attacks, active attacks and replay attacks [1]. In the latest IEEE 802.16e standard, the payload of MAC PDUs is encrypted with DES in the CBC mode or AES in the CCM mode [2]. The amended 802.16e introduces an integrity protection mechanism for data traffic. The EKS (Encryption Key Sequence) field is used to make sure that the BS and SS are synchronized in their use of Traffic Encryption Keys (TEK) and Initialization Vectors (IV). When a SS joins a BS network, it follows a multi-step process [4]. And when the SS detects an active connection it transmits its presence to BS through a Range Request (RNG-REQ) message. The SS and BS continue their conversation via RNG-REQ and RNG-RSP messages using newly assigned basic CID by BS. BS replies with REG-RSP message describing the supported capabilities. SS acknowledges the REG-RSP with REG-ACK message.

4.2 Privacy Sublayer

Two main protocols work in this security SubLayer: one is an encapsulation protocol for encrypting packet data across the fixed BWA, and the other is a Privacy and Key Management Protocol (PKM) providing secure distribution of keying data from BS to SS. It also enables BS to impose conditional access to

network services. The PKM protocol uses RSA[3] public-key algorithm, X.509 digital certificates and strong encryption algorithm to carry out key exchanges between SS and BS. This Privacy protocol is based on the PKM protocol of the DOCSIS[4] BPI+ specification; it has been enhanced to accommodate stronger cryptographic methods such as AES to fit into the IEEE 802.16 MAC. The entire security of IEEE 802.16 is in the privacy SubLayer [2].

The function of this SubLayer is to provide access control and confidentiality of the data link. Security Associations (SA) is identified by SAID, which contains, Cryptographic suite (e.g. encryption algorithm) and Security Info (e.g. key, IV).The basic and primary management connections do not have SAs. The secondary management connection can have an optional SA. Transport connections always have SAs [6].

4.3 Data SAs (Security Associations)

Data SA has a 16-bit SA identifier, a Cipher (DES in CBC mode) to protect the data during transmission over the channel and two Traffic encryption keys (TEKs) to encrypt data: one is the current operational key and the other is TEK. When the current key expires, TEK, a 2-bit key identifiers is used. A 64-bit initialization vector (IV) is used for each TEK. The lifetime of TEK is between 30 minutes to 7 days. There are three types of data SA: Primary SA is used during link initialization, static SAs are configured on the BS and dynamic SAs are used for transport connections when needed. The primary SA is shared between an MS and its BS. Static SAs and dynamic SAs can be shared among several MSs (Mobile stations) during multicast. During the connection process, SA first starts a data SA using a connection request function. A SS generally has two or three SAs - one is the secondary management connection and one is for both uplink and downlink connections; it may use separate SAs for uplink and down-link channels. BS ensure that each SS has access only to SA it is authorized to.

4.4 Authorization SAs (Security Associations)

The authorization SA has a 60-bit authorization key (AK) and a 4-bit key to identify the AK. To identify SS, it uses an X.509 certificate. The lifetime of AK ranges is from 1 to 70 days, default is 7 days. Key encryption key (KEK) has a 112- bit 3DES key for distributing TEKs (Temporal encryption key) and a list of authorized data SAs. It uses a downlink & uplink HMAC (Hash function based message authentication code) key providing data authenticity of key distribution messages from the BS to SS and vice versa. An authorization SA state is shared between a particular BS & SS. Base stations use authorization SAs to configure

[3] Ron Rivest, Adi Shamir, and Leonard Adleman
[4] Data Over Cable Service Interface Specifications (DOCSIS) Baseline Privacy Interface Plus (BPI=)

data SAs on the SS. SS authentication uses X.509 certificate (Privacy Key Management (PKM) authorization protocol and encryption) to negotiate security capabilities between BS and SS. This certificate establishes security association (SAID) through Authentication Key (AK) exchange. AK serves as authorization token and it is encrypted using public key (RSA) cryptography. Authentication is done when both SS and BS possess AK.

4.5 Data key exchange

Data encryption requires data key called Transport Encryption key (TEK), which uses AK from authentication process to derive Key Encryption Key (KEK) and Message Authentication Key (MAC key). TEK is generated by BS randomly. TEK is encrypted with 3DES (use 112 bits KEK), SA (use SS's public key) and AES (use 128 bits KEK). Key Exchange message is authenticated by MAC-SHA1, which provides Message Integrity and AK confirmation.

Based on the previous description of MAC PDU and the SA used in the radio communication between BS and SS, we can provide at this point a class diagram of the SA structure (see Fig.4).

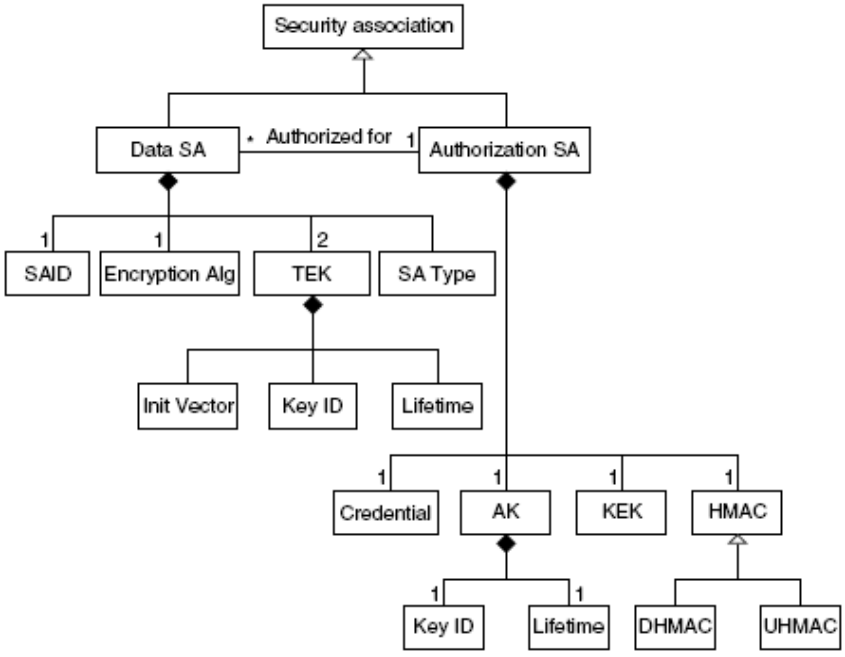

Fig.4 Class diagram of SA structure. *DHMAC* and *UHMAC* are *Downlink*/*Uplink HMAC*.

5. Network security risks

The 802.16 MAC protocol specifies (as we have shown) security procedures used to authenticate new nodes and to exchange an maintain private and encryption keys. The private encryption keys are used to encrypt traffic to first-hop neighbors or to the base station.

We have reviewed the security associations, the authentication process and other details related to a 802.16 network security. Since, nowadays, one of the most important way to access the Internet is through a VPN (Virtual Private Network), we propose, at the end of our paper, in order to see a small applications of the theoretical things described above, an end-to-end security scheme (see fig. 5).

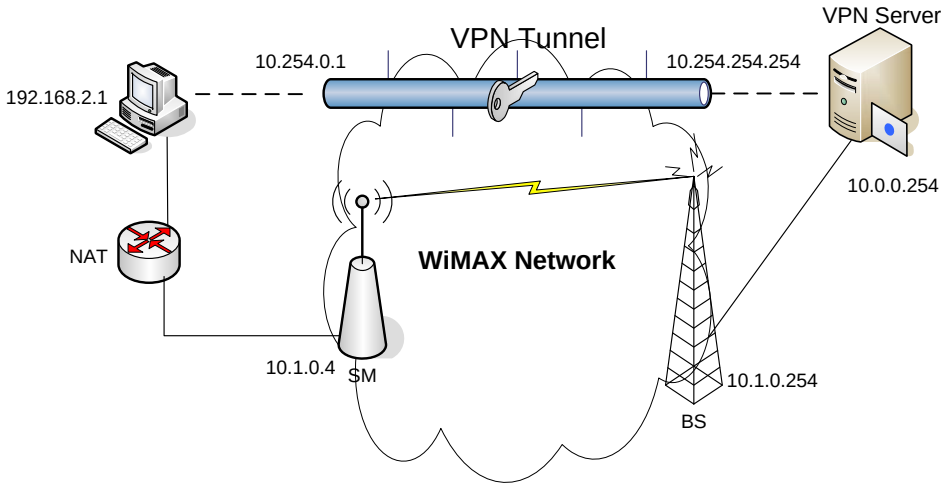

Fig.5 End-to-end VPN tunneling

IEEE 802.16 provides a mechanism to encrypt traffic traversing data connections at each hop. However, manufacturing mesh routers that can perform encryption at high speeds, available at the physical layer, may be costly. In the scheme that we propose, the encryption is taken out of the mesh backbone.

Actually, the encryption is handled at the edge of the network. The user terminal establishes a VPN tunnel with a VPN server outside the mesh backbone, so no encryption is required by mesh routers. We add a VPN server before the traffic goes on the Internet.

The server is on a special unprotected subnet 10.0.0.0/16. The user terminal negotiate IPSec tunnels with the VPN server and, after the VPN tunnel is established, the user terminal gets an IP address on the protected subnet 10.254.0.0/16.The VPN tunnel may be in any mode – e.g. encryption of the payload or both IP headers and the payload. This means that both the user

terminal and the authentication server should support IPSec NAT traversal (NAT-T), which allows the use of IPSec over NAT. This is not a problem since NAT-T is part of modern operating systems [6].

Although this end-to-end encryption scheme protects user traffic, it doesn't protect the 802.16 management traffic. This means that 802.16 nodes should still use the primary security association encryption (which we described in 4.3) to communicate with the base station. However, since this presents a small amount of traffic, implementing it in practice may not be hard.

6. Conclusions

In wireless networks, confidentiality is a primary concern for secure transmission. Resistance to interception and eavesdropping are common threats. Message authentication is for integrity of the message and sender authentication. Availability guarantees that the services are not prevented from access by DoS attack [1]. Anti-replay technique identifier and disrepute any message that is a repeat of a past message. There are some typical attacks on authentication protocols. One common attack is Message replay attack on authentication and authenticated key formation protocols [4]. The WiMAX Forum group declared that "If the messages are exchanged in an authentication protocol that do not carry proper freshness identifiers, then an opponent can easily get himself authenticated by replaying messages copied from a legitimate authentication session" [2].

Man-in-the-middle attack is usually associated in a communication protocol where common is the missing of the mutual authentication. Other known attacks that are likely to occur include parallel session attack, reflection attacks, interleaving attacks, attacks due to type flaw, attacks due to name omission, and attacks due to lack of cryptographic services [3].

IEEE 802.16 design failed to explicitly define the authorization SA - for instance, state of the SA never differentiates one authorization SA instance from another, which is vulnerable to replay attacks. This will become a significant issue when deployment of IEEE 802.16e networks will facilitate mobility and roaming. Also, SS cannot identify reused data SAs. Thus the encryption scheme is vulnerable to attack via encryption key reuse. In addition, the authorization SA does not contain the BS identity; hence the SS cannot differentiate authorized from unauthorized BSs. Here we can assume that, hiding it from SS is protecting the SS from forgery and replay attacks [3].

One solution against the replay vulnerability is to include a random value generator from the BS and SS to the authorization SA. In the latest IEEE 802.16e standard, this modification was added. The protocols presume that no parties with different public or private key pairs are certified to employ same MAC address;

condition must be explicitly defined that all certified MAC address is unique to avoid MAC masquerading problem.

The new IEEE 802.16e standard has changed several security mechanisms - like generating each per-frame IV (Initialization Vector) randomly or replaying protection using Packet Number (PN). It is using AES (Advanced Encryption Standard) as a main encryption method and introduces a flexible authentication method based on the Extensible Authentication Protocol e.g. EAP-TLS[5], EAP-TTLS[6], PEAP, EAP-SIM[7], which extends the authentication to AAA server. The standard replaces, also, Triple-DES key wrapping in the PKM protocol with the AES-ECB mode and facilitates low cost re-authentication during roaming. Still, further research is required to find out security threats and vulnerabilities in the IEEE 802.16e standard. Security mechanism is an expensive process; it requires extensive level of research, performance evaluation and implementation outcomes. The IEEE 802.16e opens the door for wireless mobility, but for vulnerability as well, because there are no constraints for an attacker.

Even so, IEEE 802.16 (WiMAX) has the capability to attain success in wireless communication arena. Though, wireless vendors have already marketed their WiMAX (fixed and mobile) product, this technology is still under development and need more academic research and time to achieve a maturity level. Therefore, business organization, service provider and IT professionals should take great care before deployment of this new technology.

R E F E R E N C E S

[1] *D.D Boom*, Denial of Service Vulnerabilities in IEEE 802.16 Wireless, Naval Postgraduate School[2], Ph.D. Thesis, 2004

[2] *M.Barbeau*, WiMax/802.16 Threat Analysis, School of Computer Science, Carleton University, 2006

[3] *H. Chou*, 802.16 & 802.11 Security Overview, Australian Information Security Conference, 2006

[4] *S.Xu*, *M. Matthews* & *C.Huang*, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16" , Department of Science, University of South Carolina, 2006

[5] *Frank Ohrman*, WiMax Handbook:Building 802.16 Wireless Networks, McGraw-Hill, NewYork, USA, 2005

[6] *S.Wattanachai*, Security Architecture of the IEEE802.16 Standard for Mesh Networks, Royal Institute of Technology, Stockholm University, 2006

[5]EAP-Transport Layer Security

[6] EAP-Tunneled Transport Layer Security

[7] EAP for GSM Subscriber Identity