Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 423281, 28 pages
doi:10.1155/2010/423281

Review Article

WiFi and WiMAX Secure Deployments

Panagiotis Trimintzios[1] and George Georgiou[2]

[1] *Technical Competence Department, European Network and Information Security Agency (ENISA), P.O. Box 1309, GR-71001 Heraklion Crete, Greece*
[2] *Thermal Construction and Engineering Department, Public Power Corporation (PLC), Chalkokondili 30, GR-10432 Athens, Greece*

Correspondence should be addressed to Panagiotis Trimintzios, panagiotis.trimintzios@enisa.europa.eu

Received 30 September 2009; Accepted 23 December 2009

Academic Editor: Francisco Falcone

Wireless Broadband offers incredibly fast, "always on" Internet similar to ADSL and sets the user free from the fixed access areas. In order to achieve these features standardisation was achieved for Wireless LAN (WLANs) and Wireless Metropolitan Area Networks (WMANs) with the advent of IEEE802.11 and IEEE802.16 family of standards, respectively. One serious concern in the rapidly developing wireless networking market has been the security of the deployments since the information is delivered freely in the air and therefore privacy and integrity of the transmitted information, along with the user-authentication procedures, become a very important issue. In this article, we present the security characteristics for the WiFi and the WiMAX networks. We thoroughly present the security mechanisms along with a threat analysis for both IEEE 802.11 and the 802.16 as well as their amendments. We summarise in a comparative manner the security characteristics and the possible residual threats for both standards. Finally focus on the necessary actions and configurations that are needed in order to deploy WiFi and WiMAX with increased levels of security and privacy.

1. Introduction

In 1997, the initial form of the 802.11 protocol was presented [1]. Since then, various amended protocols have been added. The reason was the demand for higher data rates, different modulations and frequency transmissions, improved Quality of Service (QoS), enhanced security and authentication mechanisms. When the technology was brought to the market, there were concerns if products from different vendors could meet interoperability.

This issue was addressed with the formation of an industry consortium named Wireless Fidelity Alliance (WiFi). WiFi Alliance implemented a test suite to certify interoperability for the adopted 802.11b products. The 802.11b protocol [2], an amendment of the initial 802.11, operates in the ISM band with data rates up to 11 Mbps, in infrastructure and in ad-hoc mode for client-to-client connections.

Later on, the IEEE 802.11g was introduced and certified as a continuity and extension of the 802.11b. 802.11g operates in the same frequency range with data rates up to 54 Mbps [3], providing compatibility with 802.11b devices. The higher data rates achieved with the usage of a wider range of modulation options. Another important amendment was the IEEE 802.11i protocol [4], in which, newer and stronger security and authentication mechanisms were added in order to address security deficiencies that were presented in WiFi.

After the commercial success of the standard-based equipment and the thriving demand for broadband wireless access, the vision of networks covering larger areas and extended services was the next undertake of the IEEE. As a consequence in 2001, the 802.16 standard was introduced; initially its scope was to solve the "last mile" problem. While the 802.11 protocol offers service for few hundred meters range and only for a few users, the new IEEE 802.16 standard was designed for deploying Wireless Metropolitan Area Networks (WMAN) and thereby it can provide services to hundreds or thousands of users, in a point-to-point (PP) or point-to-multipoint (PMP) setting.

In June 2004, the standard was ratified under the title "IEEE 802.16-2004 Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Broadband Wireless Access Systems" [5]. This protocol was an amendment of the earliest version 802.16-2001

with the integration of the 802.16a-2003 and the 802.16c-2002 standards. In 2005, the IEEE introduced the 802.16e-2005 amendment and the 802.16-2004 Corrigendum [6], which provide mobility along with enhanced security and authentication mechanisms. The initial specification was for fixed users, designed to operate in the 10–66 GHz frequency range. The new modifications for fixed and nomadic users include mesh and Non-Line-Of-Sight (NLOS) by adding coverage in the 2–11 GHz range.

The inherent QoS parameters in the standard include minimum traffic rate, maximum latency and tolerated jitter, helping thus the usage of low-tolerant services such voice and streaming video. Additionally, the standard provides services to support both Asynchronous Transfer Mode (ATM) and packet services. ATM is important because of its role in telecom carrier infrastructure since it is often used to support Digital Subscriber Line (DSL) services. ATM is also widely used to support voice transmissions. The packet operation in the 802.16 standard supports the IPv4, IPv6, Ethernet, and Virtual LAN (VLAN) services.

The IEEE 802.16 currently employs the most sophisticated technology solutions in the wireless world, and correspondingly it guarantees performance in terms of covered area, bit-rate, and QoS. In order to spread the use of the 802.16 standard solutions, verify the interoperability of 802.16 devices built by different manufacturers and certify interoperable devices, an analogous to WiFi consortium of wireless device manufacturers was created named as Worldwide Interoperability for Microwave Access (WiMAX) [7]. As wireless broadband technology has become very popular, the introduction of WiMAX will increase the demand for wireless broadband access in the fixed and the mobile devices. This development makes wireless security a very serious concern.

Although the functional characteristics of the 802.11 and the 802.16 are different, they do have some similarities in their architecture structure. One of them, the basis of the protocol functionality, is the mechanism of the Wireless Medium Access Control (MAC) and the Physical Layer (PHY) specification. The similarity in the structure of the MAC and the PHY layer will derive substantial results from the comparison of the two standards.

This article is organized as follows. In Sections 2 and 2.1 we provide a thorough description of the security mechanisms for the IEEE 802.11, the 802.16 and their amendments. Section 2.2 we summarise the security overview for WiFi and WiMAX is provided. In Section 3, we analyse the residual threats for the two standards. Due to the fact that the 802.11 protocol has many years of operation, an analytical description of the already known vulnerabilities is provided. On the other hand, the security mechanisms of the IEEE 802.16 and its amendments have not been tested in actual conditions for a substantial amount of time, as it is a relatively new technology, not deployed widely to determine possible serious threats and vulnerability issues. Therefore, the IEEE 802.16 threat analysis will be based on the already registered threats from the 802.11 and any possible operational weaknesses that might come up after the scrutinized analysis of the 802.16 security mechanisms. Section 3.1 summarizes in a nutshell the possible threats for both standards along with their amendments and Section 3.2 of this article we provide guidelines for usage and deployment of infrastructure design and optimal configuration for WiFi and WiMAX. Finally, in Section 5.1 we conclude and discuss the related open research challenges and the work that should be done in the future.

2. WiFi Security Mechanisms

Every security mechanism for wireless transmission is built to provide three basic functions: (i) Authentication to verify the identity of the authorized communicating client stations; (ii) confidentiality (Privacy) to secure that the wirelessly conveyed information will remain private and protected; (iii) integrity to secure that the transmitted MPDU from a source will arrive at its destination intact, without being modified. Authentication operates at the Link Level between WiFi stations. Confidentiality and Integrity is implemented in the MAC security sublayer, just a level higher from the PHY layer.

2.1. Wired Equivalent Privacy (WEP). The first security mechanism was the Wired Equivalent Privacy or Wireless Encryption Protocol (WEP). WEP has the following functions to implement the aforementioned security functions.

2.1.1. Confidentiality (Privacy). WEP uses the RC4 encryption algorithm. RC4 is a stream cipher that operates by expanding a short key into an infinite pseudo-random key stream. The station XORs the key stream with the plaintext and produces the cipher text. The first definition was the WEP-40 due to the use of a 40-bit shared key. Many vendors increased the key size to 104 bits providing the WEP-104.

To avoid encrypting two texts with the same key-stream, an Initialization Vector (IV) is used to enhance the shared secret key and create a different key (WEP seed) for each packet. The IV field is 32 bits long and contains three subfields. The first contains the 24 bit IV, the second a 2-bit Key Identifier and the third a 6-bit Pad subfield. The 24-bit IV size gives a total of 64 or 124 bits key. The encryption-decryption task remains the same despite the key size (see Figure 1). RC4 receives the payload concatenated with the Integrity Check Value (ICV) (Analysis for the WEP-ICV follows in "WEP Integrity" session) at the end, and encrypts it with the 64 or the 124 bit key described earlier. At its destination the message firstly gets decrypted. The receiver with the shared key that it possesses and with the IV from the received MPDU will decrypt the encrypted payload and ICV.

2.1.2. Integrity. To ensure the integrity of the MPDU data, WEP uses the Integrity Check Value (ICV) mechanism. ICV implements a 32 bit Cyclic Redundancy Check (CRC-32). For each transmitted MPDU payload, the CRC checksum is computed and concatenated at the end of the MPDU. Both the payload and the ICV are encrypted with the RC4 cipher. At its destination the message is decrypted and the CRC

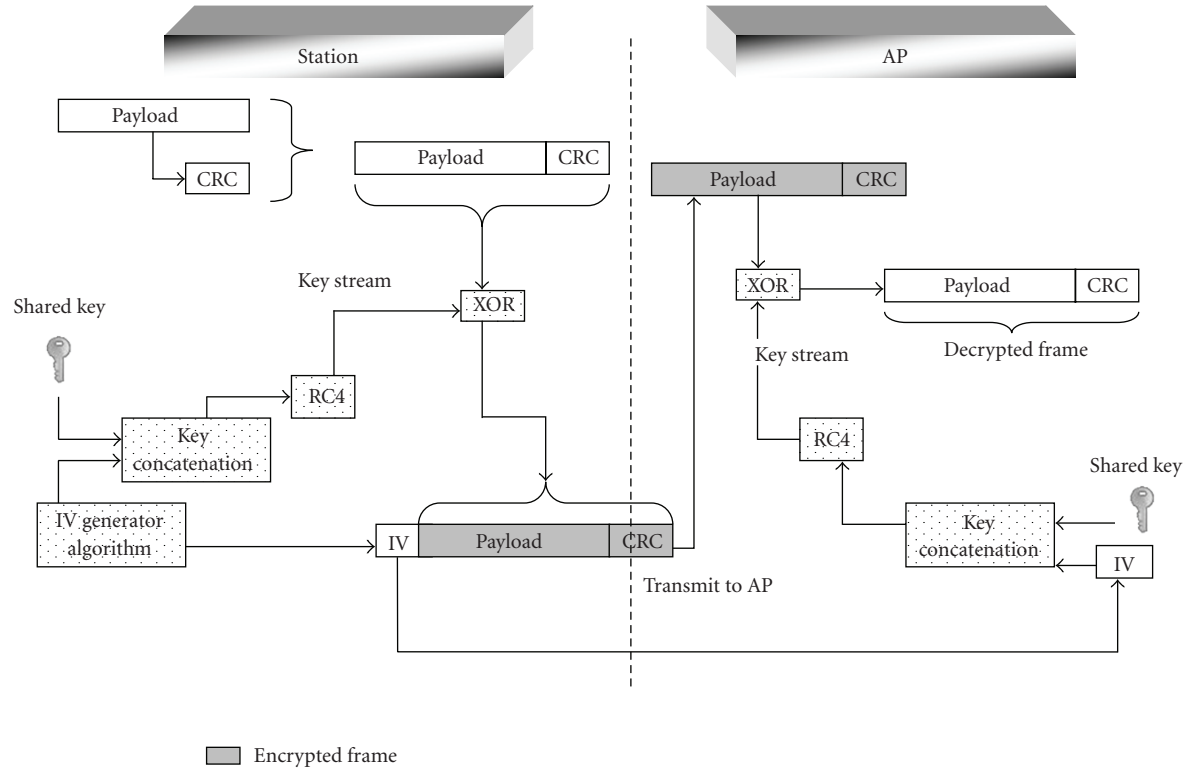

Figure 1: WEP confidentiality and integrity procedure.

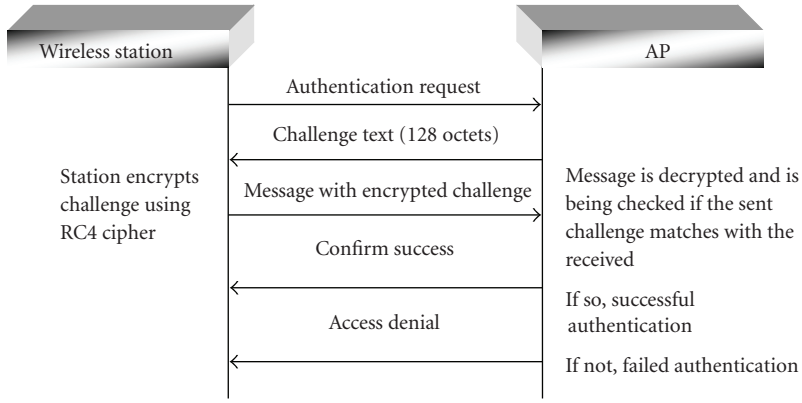

Figure 2: 4-way message authentication.

of the arrived payload is computed. If the CRC, which was produced by the source and it was sent with the message, is the same with the recomputed CRC, the message is valid and is forwarded to the Link Layer; otherwise, the message indicates integrity violation and it is discarded.

2.1.3. Authentication. WEP has two types of authentication: Open and Shared key. Open authentication actually is a non-authentication procedure since the AP accepts every station without identity verification. Thus, the station in a two-message exchange with the AP provides its identity and the request to authenticate. The AP responds with a message confirming successful authentication.

Shared key authentication (see Figure 2) requires the knowledge of a secret key to join the network. The key knowledge implies that the station is a trustful entity, and therefore authorized. The way that the key is obtained from a client station is not an issue for WEP. Another secure way must be implemented to ensure that only trusted entities will have this key. If the station possesses the key, it begins a four-way message exchange to achieve authentication. The first message from a station declares its MAC address and the authentication request. AP replies with a generated string, fixed at 128 octets, as a challenge text. The third message from station will send this challenge back to AP encrypted with an RC4 encryption, along with the ICV. The AP de-encapsulates

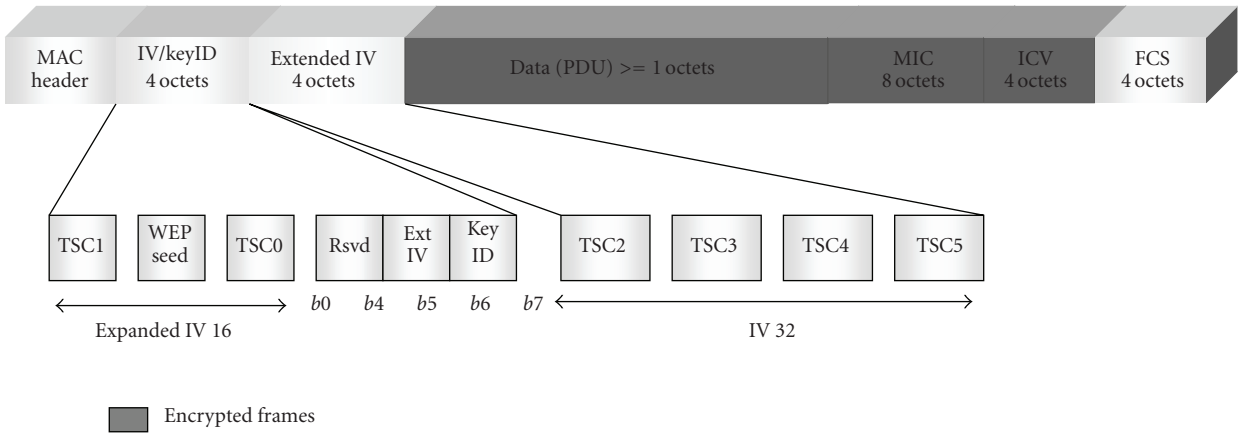

Figure 3: WPA MPDU Format.

the encrypted frame, checks the decrypted ICV, and if it is successful, the AP compares the received decrypted challenge text with the 128-byte message that was sent from it with the second message. If the two texts are the same, AP sends the last message for successful authentication. In any other case where ICV does not match or the challenge comparison is different, the AP notifies for unsuccessful authentication and rejects the station.

2.2. WiFi Protected Access (WPA). It was proved that WEP does not provide adequate security. Some of the WEP weaknesses are the following

(i) RC4 has a weak key schedule [8].

(ii) The cryptographic key and the IV are short and cannot be automatically and frequently updated.

(iii) CRC-32 is not capable of providing integrity as linear codes are susceptible to attacks on data integrity.

For the aforementioned reasons WiFi introduced the WiFi Protected Access (WPA) to enhance WEP. WPA is a part of the 802.11i standard, and it is designed to allow legacy equipment with WEP security to upgrade their firmware. WPA uses the Temporal Key Integrity Protocol (TKIP) for confidentiality and integrity while for authentication it additionally uses the 802.1X authentication protocol mechanism.

2.2.1. TKIP Confidentiality. TKIP like WEP uses the RC4 cipher for encryption-decryption. To reinforce security, TKIP doubles the IV field to 48 bits. This 48-bit field is used as a per-MPDU TKIP Sequence Counter (TSC), to create a packet sequence during transmission. If the receiver detects that a MPDU does not follow the increasing reception sequence, it drops the packet. This mechanism enhances security to replay attacks. The key mixing function is more complicated and it strengthens encryption. It generates a unique encryption key for each MPDU frame by combining the Temporal Key (TK), the Transmit Address (TA), and the TSC for the WEP seed. The WEP seed, which produced from the aforementioned parameters, operates just like the WEP IV, and with the RC4 key it creates the key stream. The encrypted parts of the MPDU are the payload, the MIC (analysis of MIC follows in TKIP Integrity) and the ICV (see Figure 3).

When the message arrives at its destination, the TSC number is checked to verify that the packet follows the increasing reception sequence. If so, the key forms the RC4 key-stream and decrypts the encrypted parts. The next step is the ICV check; if it is successful, the WPA integrity check follows.

2.2.2. TKIP Integrity. TKIP uses the Message Integrity Code (MIC) called "Michael". MIC enhances security against forgery attacks compared to the ICV usage in WEP. This time MIC is applied to MSDUs, and the MIC comparison is implemented in the MSDU-level as well. The reason is the increase of the implementation flexibility with re-existing WEP hardware. Michael with a 64-bit key is implemented on the MSDU Sender and Destination Address (SA, DA), the MSDU Priority, and the MSDU payload. MIC is 64-bit long and it is placed at the end of the MSDU payload. Knowing that a MSDU could be partitioned into more than one MPDU, the integrity check for each MPDU takes place with ICV. Then, with the concatenation of all the MSDU parts, each MSDU is checked with Michael. If the comparison of the decrypted MIC from the arrived MPDU, and the MIC which is created from the receiver, are the same, the message is valid. If not, the MSDU is discarded and measures are taking place.

2.2.3. Authentication. WPA uses the authentication methods described in WEP. Additionally, the 802.11i standard introduces the 802.1X authentication mechanism which is implemented when the WPA suite is used. A thorough analysis of the 801.1X authentication along with the Extensible Authentication Protocol (EAP) requires firstly the description of the Confidentiality-Integrity mechanisms of WPA2. Thus, the 802.1 X/EAP authentication mechanisms will be described in then WPA2 entity.

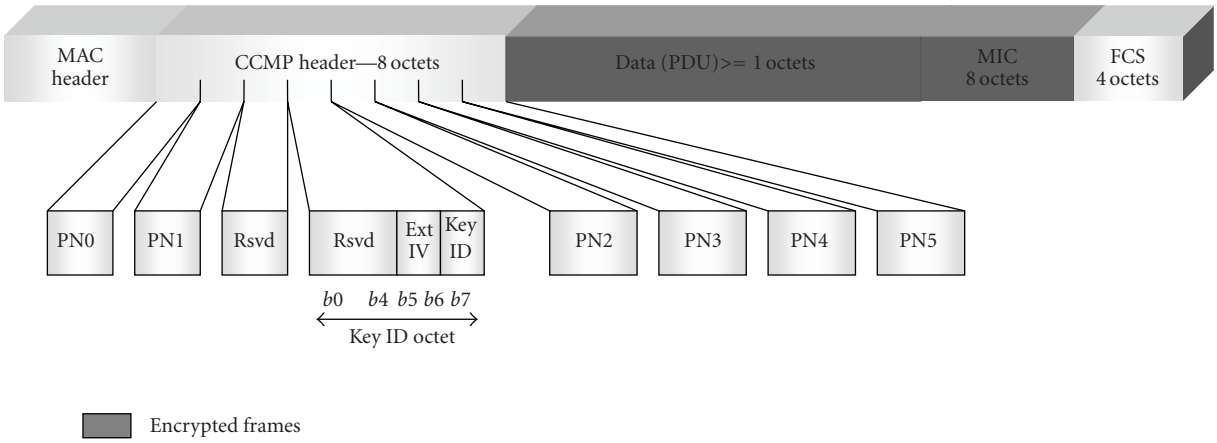

Figure 4: WPA2 MPDU Format.

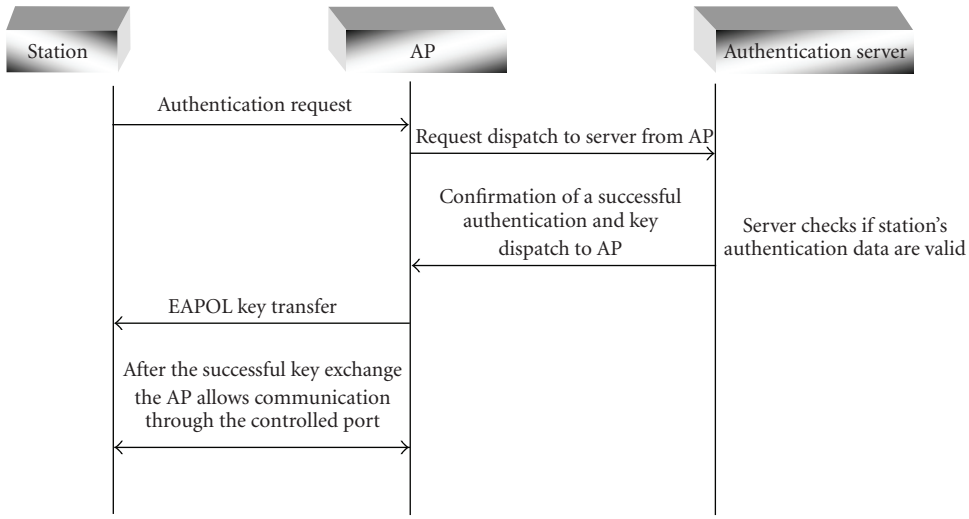

Figure 5: WPA2 Authentication procedure.

2.3. WPA2. The WPA2 name was given for the IEEE 802.11i from the WiFi Alliance. It was designed to provide stronger security with new mechanisms and hardware devices without the WEP bindings. Attention was given so that WPA devices could be associated with WPA2 access points. The security in 802.11i defines the Robust Security Network Association (RSNA), which is the indicator of the modern secured wireless communication implementation in WiFi, and separates security into two important modes: the pre-RSNA with WEP and WPA and to RSNA with WPA2 as described in this section.

2.3.1. Confidentiality. WPA2 uses the Counter-Mode/Cipher Block Chaining (CBC)-MAC Protocol (CCMP) for confidentiality as well as integrity. For data confidentiality CCMP uses AES in counter mode with 128 bit key and 128 bit block size. The encrypted parts of the MPDU are the payload and the MIC field (see Figure 4).

2.3.2. Integrity. CCM-MAC operations expand the original MPDU size by 16 octets—8 octets for the CCMP Header field and 8 octets for the MIC field. CCM requires a fresh temporal key for every session and a unique nonce value for each frame, protected by a given temporal key. For this purpose, a 48-bit packet number is used. CCM does not use the WEP ICV anymore. Leaving aside the integrity protection of the MPDU, CCM protects some Additional Authentication Data (AAD). The AAD is constructed from the MPDU header and it includes subfields from MAC frame control, addresses from source and destination fields, Sequence Control (SC), QoS control field, and therefore provides enhanced integrity protection.

2.3.3. Authentication. For authentication WPA2 provides the strong 802.1X method, which transmits key information between authenticator and supplicant. IEEE 802.1X has three main entities: The Supplicant (WS), the Authenticator (AP) and the Authentication server. The authenticator does not do the authentication; the Authentication server does this task through the authenticator. Between the supplicant and the authenticator the 802.1X protocol is implemented; between the authenticator and the authentication server the protocol

is not defined. Nevertheless, RADIUS is typically used. The EAP method used (de facto the EAP-TLS is used [9]) by IEEE 802.1X will support mutual authentication, as the station needs assurance that the AP is a legitimate AP.

The initial traffic for authentication (see Figure 5) takes place between the supplicant and the authentication server through the uncontrolled port. Once the authentication server authenticates the supplicant, it informs the authenticator for the successful authentication and it passes keying material to the authenticator. Key material exchange between the supplicant and the authenticator is implemented with the Extensible Authentication Protocol over LANs (EAPOL). If all exchanges are successful the Authenticator allows traffic through the controlled port.

2.3.4. Key Derivation and Management. Due to the fact that the 802.11i has more than one confidentiality protocols, the AP uses a ciphersuite to notify for all the data-confidentiality protocols allowed to be used (e.g., CCMP or TKIP). The client then chooses the parameters and it sends the choices back to the AP. The chosen parameters must match the available options from the list; if not, the AP will deny the association by sending a proper message. Right after the cipher suite is chosen, the key exchange is taking place. A key hierarchy is implemented to create keys for the EAPOL handshaking and the WPA2 security mechanisms. There are two key hierarchies in the 802.11i standard.

(i) Pairwise Key Hierarchy for Unicast Traffic Protection. The first key of the hierarchy is the 256 bit Pairwise Master Key (PMK). The PMK derivation depends on the authentication method used. If the 802.1X method is used, the PMK is derived from server and the first 256 bits of the Authentication, Authorization, and Accounting (AAA) key. If a preshared key is used, the password is used to create the PMK. The Pairwise key hierarchy generates the Pairwise Transient Key (PTK) from PMK. Some of the parameters are the source and the transmit address, plus, nonce from the client and the authenticator. From PTK three keys are derived. (i) The 128 bit EAPOL Key Confirmation Key (KCK), which is used for data origin authenticity in the authentication procedure that follows with HMAC-MD5, or SHA-1 algorithm. (ii) The 128 bit EAPOL Key Encryption Key (KEK), which provides traffic key confidentiality during authentication handshaking with RC4, or AES with Key Wrap. (iii) The 256 bit for TKIP or the 128 bit Temporal Key (TK) for AES-CCMP; it is used for WPA2 confidentiality.

(ii) Group Key Hierarchy for Multicast and Broadcast Traffic Protection. The first key created is the Group Master Key (GMK), which is a random number, which AP can periodically reinitialize it. The key which is derived from GMK is created with a pseudorandom function with parameters from GMK, the authenticator MAC address and a nonce from the authenticator, called Group Temporal Key (GTK). Its length is 256 bit with TKIP, and 128 bit for CCMP. The temporal key derived from GTK is 256 bit with TKIP, and 128 bit for CCMP and it is used for confidentiality.

Two are the EAPOL-key exchanges in the 802.11i standard: the 4-way and the group handshake.

The supplicant and the authenticator use this handshake to confirm the existence of the PMK, verify the selection of the cipher suite, and derive a fresh Pairwise Transient Key (PTK) for the following data session [10]. The 4-way handshake is comprised of 4 messages between the supplicant and the authenticator [11] (see Figure 6).

(i) *Message* 1. The authenticator sends a nonce (ANonce) to supplicant.

(ii) *Message* 2. The Supplicant creates its own nonce (SNonce) and sends it to authenticator. With ANonce and SNonce available, the supplicant calculates the PTK. The supplicant also sends the security parameters that it used during association, and the message is authenticated and verified with KCK from authenticator.

(iii) *Message* 3. The authenticator sends the GTK encrypted with KEK and the security parameters that sent out with its beacons. The message then is authenticated with KCK from supplicant to verify that the information sent from authenticator is valid.

(iv) *Message* 4. With this message, PTKs are ready to be used from WPA2 confidentiality protocol.

With the Group key handshake, a 4-way handshake precedes this procedure and includes the GTK conveyance in Message 3. The group key handshake updates the GTK.

(i) *Message* 1. The authenticator sends to the supplicant the GTK encrypted using the KEK and the message is subject to an authentication check.

(ii) *Message* 2. With this message, the group temporal keys (GTKs) are ready to be used from the WPA2 confidentiality protocol.

When clients roam between access points the result is a decrease in system performance as the load to authentication server is increased. A convenient way of the WPA2 to effectively resolve this issue is the key caching. With key caching the client station and the access point retain the security association when the client station roams to another access point. When a client returns to an access point, it sends the key name in the association request from AP. The client can send more than one key name in the association request. If the access point sends a success in the association response, then the client and access point proceed directly to the 4-way handshake.

After the thorough analysis of the WPA2, it must be stressed that many modern hardware devices use AES-CCMP in the WPA security, besides the TKIP option, combined with shared-key authentication, instead of the 802.1X authentication that WPA2 uses. This case resembles

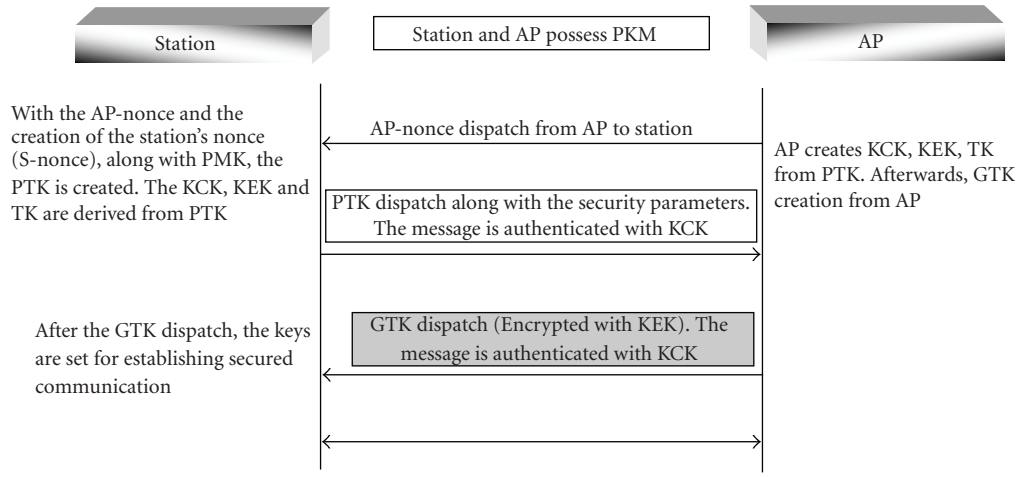

Figure 6: EAPOL key material exchange.

with WPA2 security and it should be referred as such, for the following two reasons.

(1) Although WPA is a part of the 802.11i standard, it is designed to allow legacy equipment with WEP security to upgrade their firmware.

(2) The AES-CCMP implementation in the 802.11i standard defines the Robust Security Network Association (RSNA), and indicates the modern secured wireless communication implementation in WiFi.

3. WiMAX Security Mechanisms

Security in 802.16/e was thoroughly designed as an important part of the standard architecture due to the additional possible weaknesses that wireless communication endures, especially now where the specific network deployment is to cover much larger areas. The security protocol is applied in the privacy sublayer which is positioned at the bottom of the MAC layer, and it provides mechanisms to ensure confidentiality, integrity and client authentication with the implementation of a Key Management Protocol (PKM). PKM provides also secure key distribution between BS and SS. The security information set (keys and cryptographic suites) between BS and SS is defined with the implementation of the Security Association (SA). The information included in a SA varies according to the suite it is used. The SA maintains the security state relevant to a connection [12]. SA is identified using a 16-bit SA identifier (SAID). There are three SA types.

(i) *Primary SA.* Each SS entering the network establishes an exclusive Primary SA with its BS. SS's SAID will be equal to the basic Connection ID (CID). The task of the Primary SA is to map the Secondary Management Connection.

(ii) *Static SA.* Static SAs are provisioned from the BS and they are created during the initialization process of a SS. For the basic unicast service a Static SA is created. If a SS has subscribed to additional services, additional SAs are created respectively. Static SAs can be shared by multiple SSs (multicasting).

(iii) *Dynamic SA.* A Dynamic SA is created and terminated on the fly, in response to the initiation and termination of specific service flows. Like Static SAs, Dynamic SAs can be shared by multiple SSs.

Primary and Basic Management connections are not mapped to a SA, while all transport connections are mapped to an existing SA. The BS ensures that each SS has access only to authorized SAs. Key synchronization between SS and BS is regulated from PKM.

3.1. Security Mechanisms in 802.16. The PKM protocol is used by the SS for authentication, traffic key material derivation by the BS, periodic reauthorization, and key refresh.

3.1.1. Authentication. The SS authentication is controlled from the Authorization Finite State Machine (FSM) (see Figure 13). The state machine consists of six stages (Start, Authorize wait, Authorized, Reauthorize Wait, Authorize Reject Wait and Silent), and eight distinct events (Communication Established, Timeout, Authorization Grace Timeout, Reauthorize, Authorization Reply, Authorization Invalid, Permanent Authorization Reject, Authorization Reject). In the authentication procedure the BS handles the following tasks.

(i) Authenticates the identity of a SS,

(ii) Assigns to the authenticated SS the SAIDs and the properties of Primary, and Static SAs key information,

(iii) Provides to the authenticated SS the shared secret, a 160-bit Authorization Key (AK) to initiate the following key management process.

The authorization process (see Figure 7) begins with the Authentication Information message from SS to BS.

The message contains the X.509 certificate which is bound with SS's MAC address. The certificate is issued by the manufacturer or an external authority for the SS. The X.509 authentication service is part of the X.500 series of recommendations that define a directory service. The directory is, in effect, a server or distributed set of servers that maintain a database of information about users. The core of X.509 is the public key cryptography and the digital signatures, and since the standard does not dictate a specific algorithm, RSA (asymmetric cryptography) is recommended [13]. The scheme is complete with the existence of a Certificate Authority (CA). CA issues certificates and binds each entity with a private-public key pair [14]. It is imperative that both parties entrust the CA. In 802.16 authentication, the issuer is the manufacturer or another trusted entity.

The X.509 v.3 for the 802.16 standard contains the following information:

(i) version of the X.509 certificate,

(ii) the unique Certificate serial number which the CA issues,

(iii) certificate signature. Public Key Cryptography Standard (PKCS) #1 with RSA cipher and SHA-1 hashing algorithm,

(iv) certificate (CA) issuer,

(v) certificate validity period,

(vi) certificate subject, which indentifies the entity whose public key is certified,

(vii) subject's public key, which provides the certificate holder's public key, identifies how the public key is used, and it is restricted to RSA encryption. The key size is at least 1024 bit and 2048 bit maximum,

(viii) the certificate issuer unique ID; Optional field to allow reuse of issuer name over time,

(ix) the certificate subject unique ID; Optional field to allow reuse of subject name over time,

(x) certificate extensions,

(xi) signature algorithm (PKCS#1),

(xii) signature value which is the digital signature of the Abstract Syntax Notation 1 Distinguished Encoding Rules (ASN.1 DER) encoding of the rest of the certificate.

The first message that SS sends is informative and it provides a mechanism for the BS to obtain information for the certificate of the SS. However, the BS may choose to ignore it. In the second message (Authorization Request) that is sent right after the first one, the SS requests authorization. The message includes (i) the X.509 certificate, (ii) the list of the cryptographic suite identifiers, each implementing a pair of packet data encryption and authentication algorithms that SS supports, (iii) the SS's Basic CID, which is the first static CID that BS assigns to SS during initial ranging. As mentioned earlier, the primary SAID is equal to the Basic CID.

When the BS receives the message, it authorizes the SS via the X.509 certificate, it checks for basic unicast services and other possible additional services the SS has subscribed for, and finally, it determines the cryptographic suite from the SS's list of the second message. Then, with a random or pseudo-random function, the BS generates the AK and encrypts it with the SS's public key. The encrypted AK is sent from the BS in an Authorization Reply message along with:

(i) A 4-bit key sequence number that distinguishes successive generations of AKs.

(ii) The SAIDs of the single primary and static SAs the SS is authorized to obtain key material for. The authorization reply does not identify any Dynamic SAs.

When the SS receives the message, it decrypts the AK with its private key, reads the defined cipher suite and the SAIDs, and then proceeds to key exchange with the BS. The AK remains active until it expires according to the predefined lifetime set by the BS. The SS periodically refreshes the AK by issuing authorization requests. The BS is able to support two active AKs simultaneously for each SS. Those keys must have overlapping times. Additionally, BS is always ready to send an AK to a SS upon request. The AK transition period begins when the BS receives an authorization message from a SS and the BS has a single active AK for that SS. Right after the BS receives the message, it activates the second AK which has a sequence number increased by one from the older AK, and it sends it to the SS. The lifetime of the second AK is the remaining lifetime of the older AK, plus the predefined AK lifetime. The lifetime ranges from one day to 70 days, with a default value of 7 days. If the SS does not reauthorize itself before the expiration of the current AK key, the BS does not create the sequentially next AK and considers the SS unauthorized.

3.1.2. Key Derivation and Management. With the AK delivered to SS, a key derivation will proceed to create the necessary traffic key material to implement the security mechanisms. From AK three keys will be derived.

(i) The Key Encryption Key (KEK). KEK is responsible for the encryption of the Temporal Encryption Key (TEK), that BS sends to each SS. TEKs are used for the MPDU encryption to ensure confidentiality.

(ii) The Downlink Hash function-based Message Authentication Code (HMAC_KEY_D). For the BS, the HMAC_KEY_D is used to calculate the HMAC digest for some of the management messages that it sends to SS, while for the SS it is used to verify the HMAC-Digest from the aforementioned received messages.

(iii) The Uplink Hash function-based Authentication Code (HMAC_KEY_U). For the SS, the HMAC_KEY_U is used to calculate the HMAC-Digest for some management messages that it sends to the BS, while the BS uses it to verify the HMAC-Digest of the management messages sent from the SS.

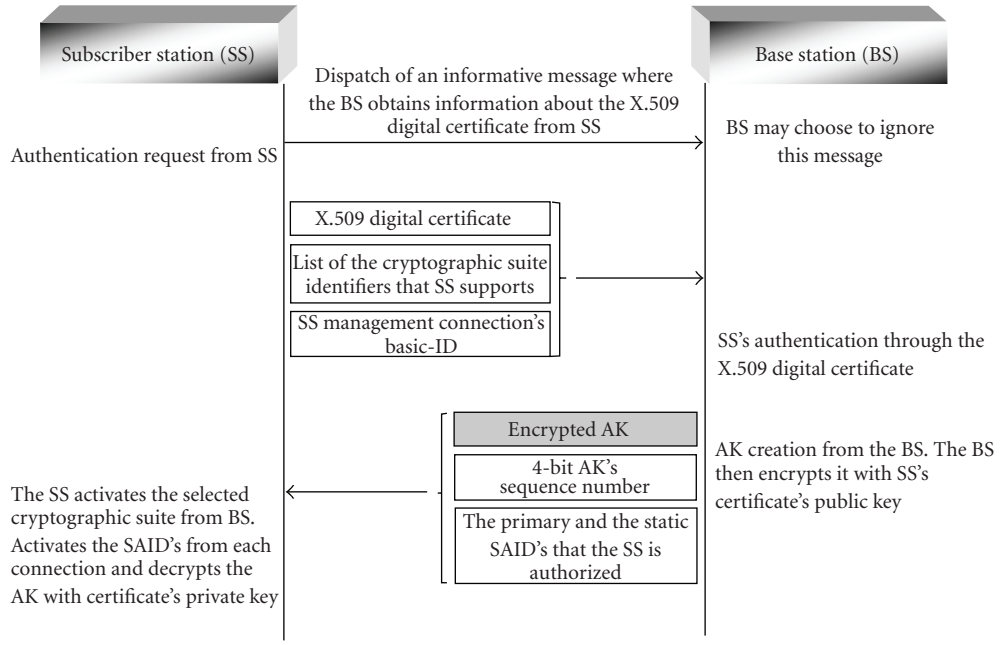

Figure 7: 802.16 Authentication Process.

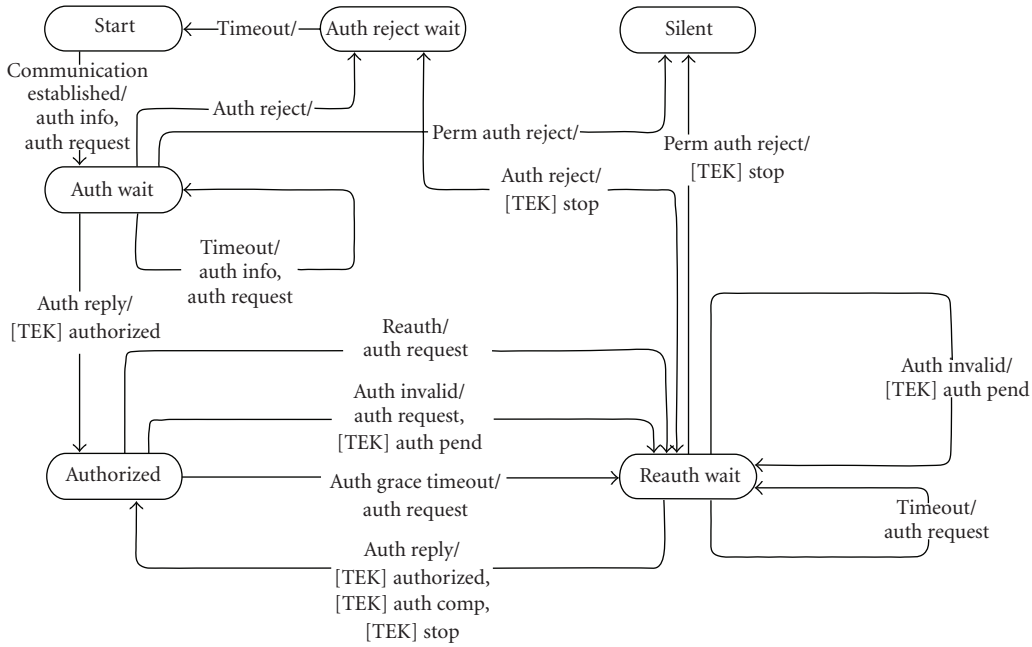

Figure 8: Authorization Finite State Machine Flow Diagram.

The BS is responsible to keep the keying information for every SS that joins the network. After key derivation the SS starts a separate TEK state machine for each of the SAIDs (the single primary and any static SA that the BS has assigned to SS). The TEK state machine (see Figure 8) consists of six stages (Start, Operational Wait, Operational Reauthorize Wait, Operational, Rekey Wait, Rekey, Reauthorize Wait), and nine events (Stop, Authorized, Authorization Pending, Authorization Complete, TEK Invalid, Timeout, TEK Refresh Timeout, Key Reply, Key Reject). Its task is to manage key material associated with the respective SAID. Each TEK state machine operates with a key request scheduling algorithm to refresh key material for their respective SAID. The BS always keeps two sets of active TEKs along with their respective 64-bit IV for each SAID. For TEK and IV generation, the BS uses a random or a pseudorandom function. The lifetime for each TEK is between 30 minutes to 7 days, with the default value set to 12 hours. The two TEKs

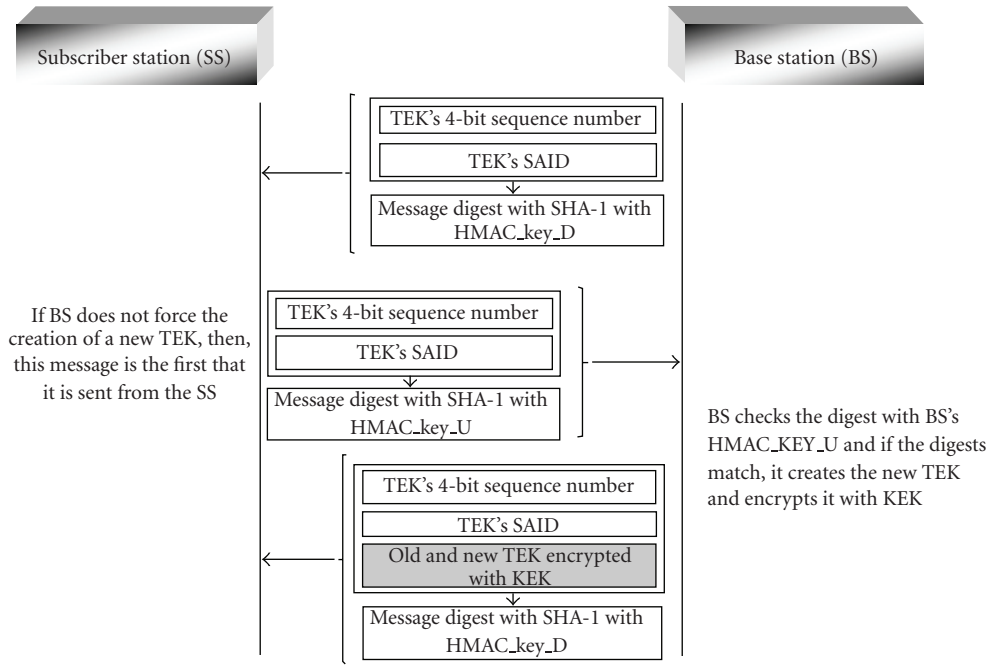

Figure 9: SA-TEK 3-way handshake.

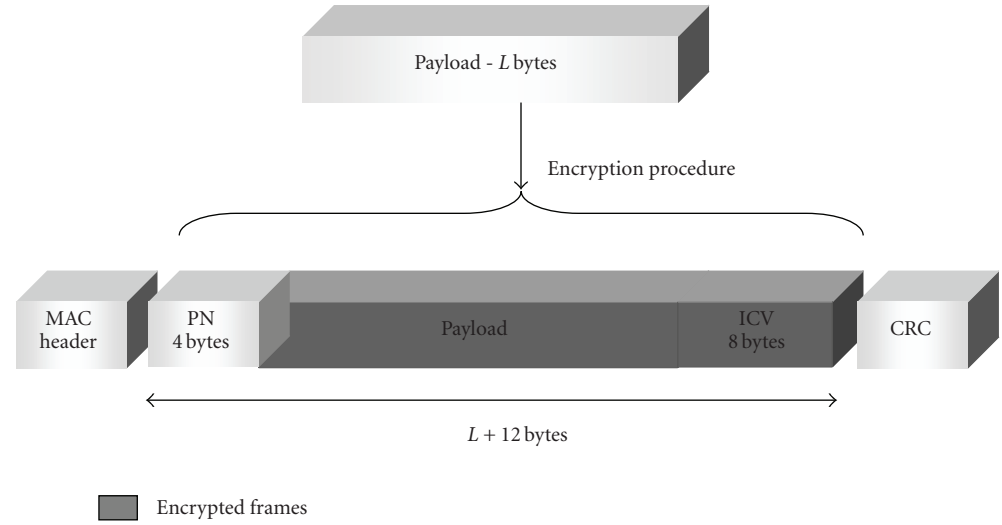

Figure 10: MAC 802.16 encryption frames.

have overlapping lifetimes, just like the AK keys, and the sequence number of the newer is the older number plus one. Each new TEK becomes active halfway through the lifetime of its successor. For each SAID, the BS uses the older of the two active TEKs for encryption of the downlink traffic, while for the uplink traffic uses the older or the newer.

The PKM protocol for the TEK refresh procedure uses the SA-TEK 3-way handshake (see Figure 9) [12].

(*i*) *Message* 1. This message is optional, and BS uses it only when it wants to force a re-key of an SA, or create a new one. In this message the BS sends the key sequence number, its SAID and the digest of this message with the HMAC_KEY_D.

(*ii*) *Message* 2. If BS does not force re-keying, message 2 is the first message that the SS sends to re-key each SA. In this message, the SS sends to BS the key sequence number, its SAID, and the digest of the message with the HMAC_KEY_U.

(*iii*) *Message* 3. The BS receives the second message, verifies the digest with HMAC_KEY_U and if is successful, it sends back the key sequence number, the SAID, the old and the new TEK with their parameters, along with the message digest. The BS encrypts the old and the new TEK with KEK and sends it to SS.

For the Mesh Mode, each node after authorization starts for each of its neighbors a separate TEK state machine

for each of the SAIDs identified during the authentication procedure. The node has the task to maintain the two active TEKs for each SAID between itself and all the other nodes that it initiated the TEK exchange with. The TEK state machine is responsible to maintain keying material. The neighbor replies to the Key Request message with a Key Reply message. The message contains the BS's active TEK for a specific SAID and it is encrypted with the node's public key.

3.1.3. Confidentiality. Confidentiality includes data and TEK Encryption.

Data Encryption. In data encryption the encrypted frames are the MPDU payload along with the 64-bit ICV of the payload (see Figure 10). The ICV is added right after the PDU. At the front, a 32-bit Packet Number (PN) is appended. For the sake of uniqueness, there are separate ranges of values for the uplink and the downlink [15]. According to the TEK length, two encryption methods are implemented.

(i) DES in Cipher Block Chaining (CBC) mode, when TEK is 64 bit. DES in CBC mode uses a 56-bit key with a 64-bit block encryption along with the 64-bit IV. The function actually expects the 64-bit TEK key, but only the 56 bits are used [13]. With the DES-CBC mode, each encrypted ciphertext block is XORed with the next plaintext block to be encrypted, and therefore, it makes the blocks dependent on all the previous blocks. Consequently, in order to find the plaintext of a particular block, the ciphertext, the key, and the ciphertext of the previous block must be known. The first encrypted block has no previous ciphertext, and so the plaintext is XORed with the IV. This mode of operation improves security from the regular DES.

(ii) AES in CCM mode when TEK is 128-bit. The AES in CCM mode uses a 128-bit key and 128-bit block size. The key-PN combination will not be used more than once. The reason is that two sent packets encoded with the same key-PN combination eliminate the security guarantees of the CCM mode. For this reason, and only in the AES-CCM mode, when more than half of the available numbers of the 32-bit PN have been exhausted, the SS schedules a new Key Request, to obtain new key material and avoid this incident.

TEK Encryption. The TEK encryption is again dependent on its key-size. If the size of the TEK is 64-bit, the 112-bit 3-DES is used. The keying material of 3-DES consists of two distinct DES keys. The 64 most significant bits of the KEK are used in the encryption. If the TEK size is 128-bit, the 128-bit AES in ECB mode will be used with a 128-bit KEK. Another encryption method for the 128-bit TEK is the RSA encryption with the SS's public key.

3.1.4. Integrity. For data traffic integrity, ICV is calculated from two modes:

(i) CBC mode. The downlink CBC IV is initialized as the XOR of the IV included in the TEK's SAID, and the content of the PHY synchronization field of the latest DL_MAP. The uplink CBC IV is initialized as the XOR of the IV included in the TEK's SAID, and the content of the PHY synchronization field of the DL_MAP that is in effect when the UL_MAP is created.

(ii) CCM mode**.** The CCM provides data integrity and data origin authentication for some data outside the payload. The ICV is computed from the ESP header, the Payload, and the ESP trailer fields, which is significantly smaller than the CCM-imposed limit. The ESP payload is composed from the IV, the encrypted payload and the Authentication data as it is defined in the RFC 4309 ("Using Advanced Encryption Standard CCM Mode with IPsec Encapsulating Security Payload").

For the management messages integrity, two 160-bit keys (HMAC_KEY_D, HMAC_KEY_U) are used to create the HMAC digest for integrity protection and authentication, by implementing the Secure Hash Algorithm (SHA-1). The digest is calculated over the entire MAC management message, except from the HMAC digests and the HMAC tupple attributes. The HMAC Sequence number in the HMAC tupple is the AK sequence number from which the HMAC_KEY has been derived.

3.2. Security Mechanisms in 802.16e. Although IEEE 802.16-2004 has a strong security protocol, the introduction of the 802.16e corrigendum with its mobility services has enhanced and corrected weaknesses appearing in the 802.16 standard. Due to mobility features introduced with 802.16e, the SS becomes a Mobile Station (MS) as well.

3.2.1. Authentication. With the 802.16e standard, the PKM protocol besides the unilateral authentication of the SS, it can implement mutual authentication for BS and SS. Two methods are used for authentication (see Figure 11): The known X.509 digital certificate with RSA public key encryption as described in the 802.16 authentication, and the EAP method. EAP is a generic authentication protocol and thereby it has to use a particular credential for authentication selected by the operator. Two are the credential types: The X.509 digital certificate of EAP-TLS, and a Subscriber Identity Module for EAP-SIM. The EAP methods are not part of the protocol, but they must fulfill some mandatory criteria (Generation of Symmetric Keying Material, Key strength, Mutual Authentication Support, Share State Equivalence, Resistance to Dictionary attacks, Protection of Man in the Middle attacks) as defined in RFC 4017.

The new feature in 802.16e is the implementation of two Privacy Key Management protocols PKM v.1, and PKM v.2. The difference between the two versions is that PKM v.2 implements more enhanced security features than PKM v.1 does. For both versions, the Authorization Finite State Machine (FSM) remains as described in 802.16 standard.

3.2.2. PKM v.1 Authentication. Authentication with PKM v.1 is the same as described in the 802.16 standard, and it is

unilateral (only SS is authenticated). The procedure uses X.509 v.3 digital certificates with RSA public key encryption for authorization and the following SAID allocation for the single primary, and any static SAs the SS is subscribed for, along with the AK derivation. For the SS's X.509 certificate, the Certificate Issuer Unique ID and the Certificate Subject Unique ID fields are omitted. The EAP in PKM v.1 is optional and applicable only if specifically required. As noted in "Authentication, Authorization, and Accounting (AAA) Key Management Requirements (RFC4017)": *EAP selects one end-to-end authentication mechanism. The mechanisms defined in [RFC3748] only support unilateral authentication, and they do not support mutual authentication or key derivation. As a result, these mechanisms do not fulfil the security requirements for many deployment scenarios, including Wireless LAN authentication [RFC4017]. To ensure adequate security and interoperability, EAP applications need to specify mandatory-to-implement algorithms.* IEEE 802.16e does not specify a mandatory-to-implement EAP method, nor does it specify the required security properties of EAP methods are to be used. The specification as it stands permits implementations to use the EAP MD5-Challenge, which does not generate keys and is vulnerable to dictionary attacks [16].

3.2.3. PKM v.2 Authentication. In PKMv2, RSA and EAP can be used in different deployments such as RSA, RSA-EAP, EAP and EAP-EAP. With two authentication schemes, there are two sources possible for keying material derivation. The RSA based authentication initially creates the pre-Primary AK (pre-PAK), and the EAP creates the Master Session Key (MSK), both for key derivation and management.

The enhancement in the protocol is the mutual authentication between BS and SS. With mutual authentication, the BS presents its own certificate to each SS joins the network. This certificate presents the following.

(i) Country Name (Country of operation)

(ii) Organization Name (Name of infrastructure operator)

(iii) Organizational Unit Name (Wireless MAN)

(iv) Common Name (Serial number)

(v) Common Name (The operator defined BS ID).

Like in PKM v.1, the Certificate Issuer Unique ID and the Certificate Subject Unique ID of the SS's X.509 certificate fields are omitted.

Mutual authentication is performed in two schemes. In the first only the mutual authentication is used, while in the second, mutual authentication is followed by EAP authentication. In the latter case, the mutual authentication is implemented only for initial network entry, while EAP is implemented in the re-entry authentication.

The authorization process (see Figure 12) begins again like in 802.16 with the Authentication Information message from SS to BS. Right after, the SS sends the Authorization Request message consisted of: (i) the SS's X.509 certificate, (ii) the list of the cryptographic suite identifiers, each implementing a pair of packet data encryption and authentication

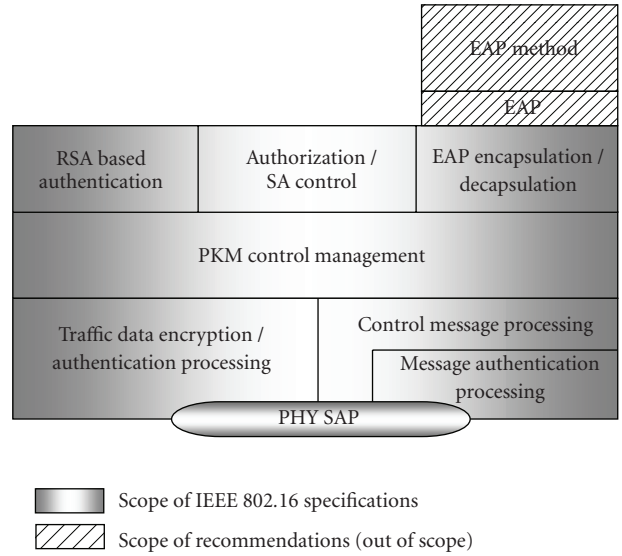

Figure 11: 802.16e security sublayer.

algorithms that SS supports, (iii) the SS's Basic CID, which is the first static CID that the BS assigns to the SS during initial ranging, (iv) A 64-bit random number generated in the SS (SSNonce).

Again, when the BS receives the message, it validates the SS's identity with the X.509 certificate, it checks for basic unicast services and possibly additional statically services the SS is subscribed for, and finally, it determines the cryptographic suite from SS's list from the second message. Then, the BS generates the pre-PAK and encrypts it with the SS's public key. The encrypted pre-PAK is sent from BS in an Authorization Reply message along with the following.

(i) The BS's certificate.

(ii) A 4-bit key PAK sequence number that distinguishes successive generations of AKs.

(iii) The lifetime of PAK

(iv) The SAIDs of the single primary and static SAs the SS is authorized to obtain key material for.

(v) The 64-bit SSNonce.

(vi) A 64-bit random number (BSNonce) generated in the BS to ensure along with SS's nonce the liveness of the message for replay attacks prevention.

(vii) An RSA signature for every attribute in the authorization reply message to ensure message integrity.

When the SS receives the message; it decrypts the pre-PAK with its private key, reads the defined cipher suite and the SAIDs, and proceeds to key exchange with BS.

3.2.4. PKM v.2 Key Derivation and Management. In 802.16 with PKM, the AK derived from BS right after the Authorization Request from SS; the same is implemented with PKM v.1. In PKM v.2 the different authentication schemes (RSA, RSA-EAP, EAP, EAP-EAP) use different key material to

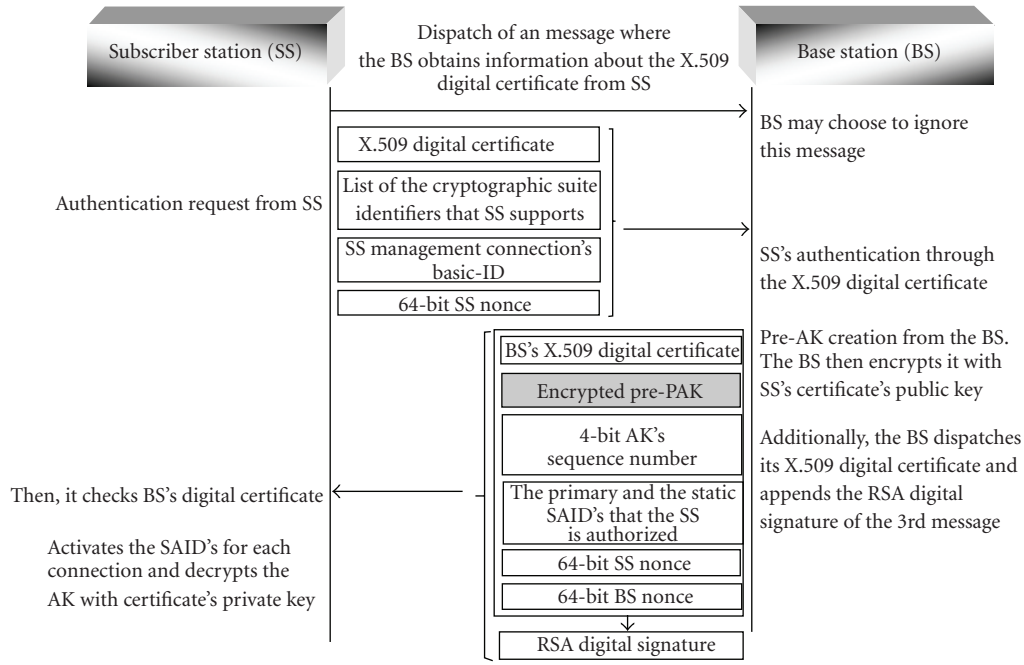

Figure 12: 802.16e Authentication Process with PKM v.2.

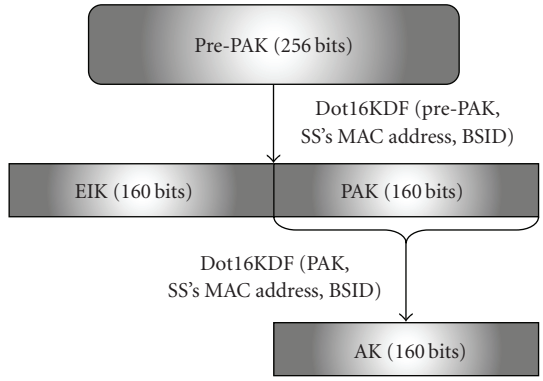

Figure 13: AK derivation with RSA authentication.

construct the 160-bit AK. All the key derivations though, are based on the Dot16KF algorithm, a CTR mode construction that can be used for the creation of an arbitrary amount of keying material from source keying material. If RSA authentication is used, the initial key material is the 256-bit pre-PAK sent from BS to SS. If EAP is used, the key transferred to 802.16e layer is the 512-bit Master Session Key (MSK), which is known to the AAA server, the Authenticator, and the SS. For every authentication scheme, the AK will derive with the following way.

(*i*) *RSA Authentication Only.* From pre-PAK, the SS's MAC address and the BSID, two 160-bit keys are generated. The PAK and the EAP Integrity Key (EIK). With the two new keys along with SS's MAC address and the BSID, the AK is derived (see Figure 13).

(*ii*) *EAP Authentication Only.* From MSK, the 160-bit Pairwise Master Key (PMK) is derived, and optionally the EIK with a MSK truncation to 320 bits. From PKM, the SS's MAC address and the BSID, the AK is derived. During authentication the BS will provide to SS the respective 4-bit PMK sequence number, as it happens with PAK and RSA. The SS caches the PMK upon successful authentication, as the Authenticator does upon its receipt via the AAA protocol. When a new PMK is cached for an SS, the authenticator deletes the old PMK which was used for the specific SS (see Figure 14).

(*i*) *RSA-EAP Authentication.* With the RSA encryption as it was described before, the PAK and the EIK are derived. From EAP in a similar way as before, the PMK is generated. From PAK XORed with PMK, the SS's MAC address and the BSID, the AK is finally created (see Figure 15).

(*ii*) *EAP-EAP Authentication.* From the first EAP authentication, two keys are generated; the PMK-1 and the EIK. From

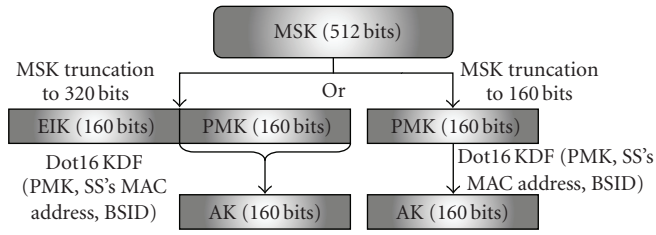

Figure 14: AK derivation with EAP authentication.

the second EAP authentication, only the second PMK-2 is created. With PMK-1 XORed with PMK-2, the SS's MAC address and the BSID the AK is derived (see Figure 16).

Like in 802.16, the SS periodically refresh its AK by reissuing Authorization Requests to the BS, and both SS and BS hold simultaneously two active AK's with overlapping times. The only enhancement in PKM v.2 for the AK is the introduction of a 64-bit ID for each AK (AKID). The AKID is created from AK, AK sequence number, the SS's MAC address and the BSID.

After the AK generation as described in 802.16, three keys are created. One of the three keys is the 128-bit KEK for TEK encryption during the SA-TEK 3-way handshake. The other two keys, the downlink message authentication key and the uplink authentication key will derive according to the used MAC mode. With PKM v.2 two MACs can be implemented. The known from 802.16 HMAC and the new Cipher based MAC (CMAC). In the latter case, the calculated hash value is derived from the CMAC algorithm with AES. The value is calculated over a field that contains: (i) the 64-bit AKID, (ii) the 32-bit CMAC packet number counter, (iii) the 16-bit connection ID, (iv) a 16-bit zero padding for the header alignment with the AES block size, and (v) the entire MAC management message. With CMAC the downlink authentication key CMAC_KEY_D is used to authenticate management messages in the downlink direction, while the respective CMAC_KEY_U is used to authenticate management messages in the uplink direction. Therefore, from AK and the implemented MAC, two options are available.

(i) AK with HMAC**:** In this case the derived keys are: the 128-bit KEK, the 160-bit HMAC_KEY_U and the 160-bit HMAC_KEY_D,

(ii) AK with CMAC**:** In this case the derived keys are the 128-bit KEK, the 128-bit CMAC_KEY_U. and the 128-bit CMAC_KEY_D.

It must be stressed that if only EAP authentication is used, the EIK will be used instead of the AK to generate the aforementioned keys.

The TEK state machine remains the same as described in 802.16 managing key material associated with the respective SAID, but due to the supported multicast features TEK consists of an additional state (Multicast and Broadcast Rekey Interim Wait), and two more events (Group- KEK Updated and GTEK Updated) to the rest described in 802.16. The difference is that the PKM v.2 implements an enhanced

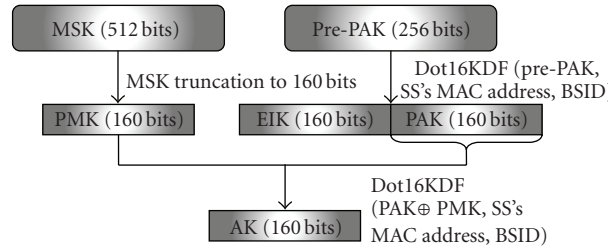

Figure 15: AK derivation with RSA-EAP authentication.

SA-TEK 3-way handshake, which operates in the following way (see Figure 17).

(*i*) *Message* 1. During the initial network entry or a reauthorization, the BS sends a SA-TEK challenge, which includes a random number (BS-Nonce), to the SS with HMAC/CMAC protection. If the BS does not receive a SA-TEK Request message within a certain period of time, it resends the SA-TEK challenge. If again for a certain number of times the BS does not receive a SA-TEK Request, it starts another full authentication procedure or it drops the SS.

(*ii*) *Message* 2. The SS sends the SA-TEK request along with the random number from the SA-TEK challenge, protected with the HMAC/CMAC. In case where the SS does not receive a SA-TEK Response from the BS, it transmits the message again for a specific number of times. If again receives no Response, it fully initiates the authentication procedure.

(*iii*) *Message* 3. When the BS receives the SA-TEK Request from the SS, it performs a number of checks before sending the SA-TEK Response message: (i) confirms that the AKID corresponds to the current AK. If it does not correspond, the BS ignores the message; (ii) verifies the HMAC/CMAC. If it is invalid, the BS ignores the message; (iii) verifies that the BSNonce received from SS with the SA-TEK Request matches with the sent random number in the first message. This process adds freshness to the messages and therefore prevents replay attacks. If the number is different, the BS ignores the message; (iv) checks the SS's security parameters, and if they do not match it reports it to the higher layers. If the validation is successful the BS sends the SA-TEK Response message protected with HMAC/CMAC. For unicast SAs, the BS for each SAID sends the TEK, the TEK's lifetime, the TEK's sequence number, and the 64-bit CBC IV, encrypted

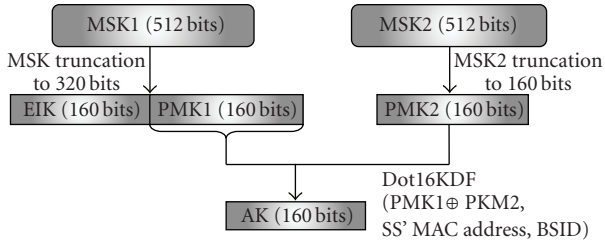

Figure 16: AK derivation with EAP-EAP authentication.

with KEK. In case of group or multicast SAs, the BS for a specific GSAID sends the GTEK, the GKEK, the GTEK remaining lifetime, the GTEK's sequence number and the CBC IV, encrypted with KEK.

When the SS receives the SA-TEK Response message it verifies the HMAC/CMAC digest. If it is valid the SS installs the TEK and its parameters, otherwise, the SS ignores the message.

3.2.5. Multicasting Key Derivation. In multicasting, the key derivation starts with the random generation of the 128-bit Group KEK (GKEK) from the BS and the 64-bit GKEK ID. The key encrypted with KEK is transmitted to SS. There is one GKEK per Group Security Association (GSA) and it is used to encrypt the Group TEK (GTEK) sent in multicast messages to the SSs join the group. GTEK is used to encrypt multicast data packets and it is randomly generated from the BS. GKEK generates the CMAC_KEY_GD for the authentication of multicast messages. The GSA contains keying material and it is used to secure multicast groups. It is defined separately from SAs because they offer lower security, since each of the members joining the group share the keying material and consecutively can forge traffic as if it came from any other member of the group.

3.2.6. Confidentiality with PKM v.2. The length of the TEK an the KEK keys must be either 64 or 128 bits. If the SA implements a cipher suite with a block size of 128 bits, the TEK and the KEK are 128-bit long. Otherwise the length is 64 bits.

Data Encryption. In data encryption, the encrypted frames are the MPDU payload along with the 64-bit Ciphertext Message Authentication Code (see Figure 18). The Ciphertext MAC is added right after the PDU, while at the front, the 32-bit Packet Number (PN) is appended. Again, for the PN there are separate ranges of values for the uplink and the downlink. According to the TEK length, three encryption methods are implemented.

(i) DES in Cipher Block Chaining (CBC) mode using a 56-bit key with 64-bit block encryption along with the 64-bit IV,

(ii) AES in CCM mode with 128-bit key and 128-bit block size,

(iii) AES in CBC mode with 128-bit TEK key and 128-bit block size.

TEK Encryption. The KEK is used for the encryption of the TEK. If it is to encrypt a 128-bit TEK, the 128-bit of the KEK are used directly, otherwise, if TEK is 64-bit long the KEK splits in two 64-bit DES keys. The TEK encryption methods are

(i) 3-DES for 64-bit TEK encryption

(ii) AES in ECB mode for 128-bit TEK encryption

(iii) RSA with SS's public key for 128-bit TEK encryption

(iv) AES Key Wrap for 128-bit TEK encryption. The AES Key Wrap is designed to encrypt key data, and the algorithm accepts both the ciphertext and the ICV, as it is defined in the RFC 3394 ("Advanced Encryption Standard Key Wrap Algorithm").

Group KEK Encryption. The GKEK is encrypted with KEK and the encryption methods are the aforementioned methods used for the TEK.

3.2.7. Integrity with PKM v.2. For the MPDU payload integrity, the ICV can be derived from three modes.

(i) DES-CBC mode. The downlink CBC IV now is initialized as the XOR of the IV included in the TEK's SAID, and the content of the PHY synchronization field of the current frame number. The uplink CBC IV is initialized as the XOR of the IV included in the TEK's SAID, and the content of the PHY synchronization field of the Frame Number of the frame where the relevant UL_MAP was transmitted.

(ii) AES-CCM mode. The integrity procedure of the AES-CCM is the same as it was described for the 801.16 and the PKM protocol.

(iii) AES-CBC mode. The CBC IV created with the XOR of: (i) the CBC IV parameter included in the TEK keying information, (ii) the 128-bit concatenation of the 48-bit MPDU header, (iii) the PHY synchronization value of the MPA that the data transmission occurs, (iv) the 48-bit MAC address and the Zero hit counter.

For management message integrity protection and authentication two MAC modes are implemented.

(i) The HMAC digest with the Secure Hash Algorithm (SHA-1). In PKM v.2 the short-HMAC calculation include the HMAC packet number concatenated after the MAC management message. The HMAC packet number is the AK sequence number.

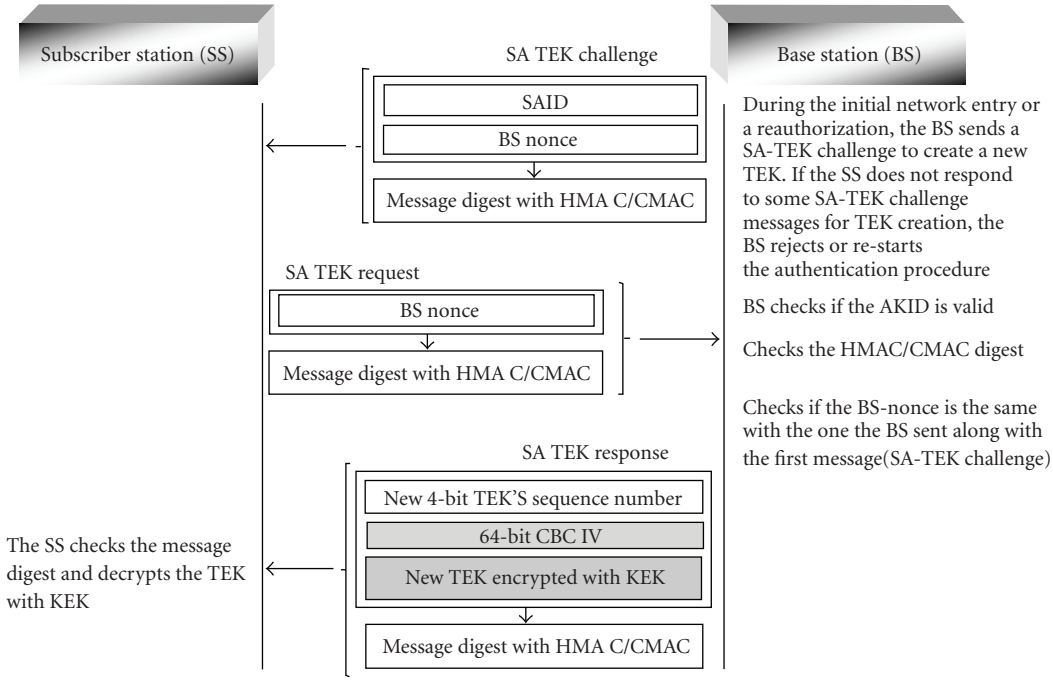

Figure 17: SA-TEK 3-way handshake with PKM v.2.

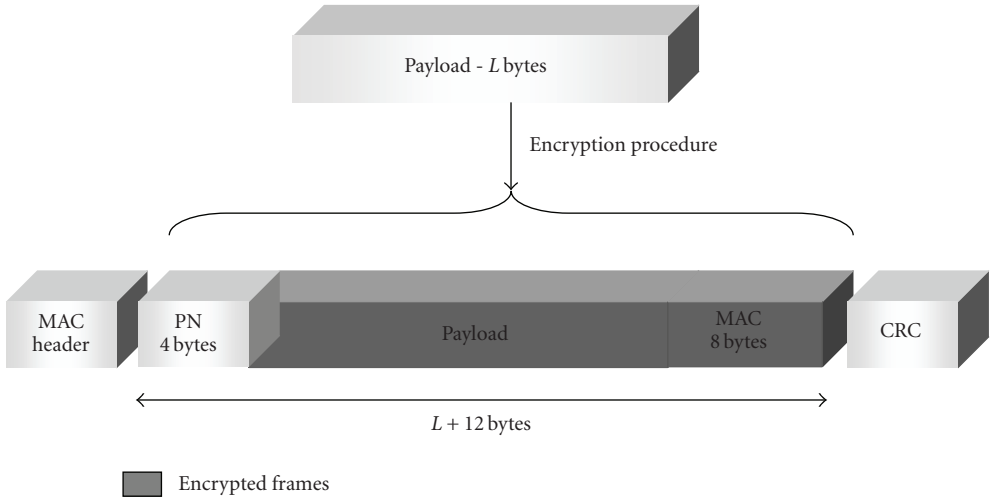

Figure 18: MAC 802.16e encryption frames.

(ii) The CMAC value is implemented as it was described earlier in the PKM v.2 Key derivation and management entity.

4. WiFi-WiMAX Security Comparison

In this section we present a summary of the security mechanisms for authentication, key derivation and management, confidentiality, and integrity procedures applied in WiFi and WiMAX networks.

From the security description in sections WiFi and WiMAX, and with the aid of the following Table 1, it is easy to conclude that WiMAX security is much stronger than it is in WiFi. One of the reasons of course is the large areas that WiMAX covers, and therefore, such conditions demand secure operational conditions of the network, which requires strong security mechanisms.

On the other hand WiFi undoubtedly covers small areas comparing to WiMAX but many WiFi network deployments in companies, industries, agencies and in many cases domestic users, handle valuable confidential information that cannot be compromised. In this case, WiFi security is demanded to be as strong in performance as it happens with the WiMAX mechanisms. Having said that, it is apparent that WEP and WPA security, with RC4 encryption and shared-key authentication, is not adequate to provide guaranteed confidentiality, integrity and secure user-authentication.

Table 1: WiFi and WiMAX security comparison.

(a)

IEEE Protocol		WiFi		
		WEP	WPA	WPA2
Authentication	Method	Open System Authentication Shared Key Authentication	802.1X authentication Shared Key Authentication	802.11X authentication with (RADIUS) server. The EAP method used by IEEE 802.1X will support mutual authentication, as the STA needs assurance that the AP is legitimate.
Key Derivation and Management	Key Management and short description	The keys from traffic encryption are consisted of the concatenation of the 40 bit shared key and the 24 bit IV for a 64 bit key. Most of the vendors use a 104 bit shared key concatenated with the 24 bit IV to create a 124 bit key	TKIP. The 48-bit IV field is used as MPDU TKIP Sequence Counter (TSC). TKIP uses key mixing consisted of the Temporal Key (TK), the Transmit Address (TA), and the TSC for the WEP seed. The WEP seed produced from the aforementioned parameters operates just like the WEP IV. Therefore, assures that every data packet is sent with its own unique encryption key	*Pairwise key hierarchy* for unicast traffic protection. The first key is the 256 bit PMK. PMK derivation depends on the authentication method. If 802.1X is used, the PMK derives from server and the first 256 bits AAA key. If pre-shared key is used, the password is used to create the PMK. PMK generates the PTK from PMK. From PTK three keys are derived. (I) The 128 bit EAPOL KCK, for data origin authenticity in the authentication procedure. (II) The 128 bit EAPOL KEK. (III) The 256 bit for TKIP or 128 bit for AES-CCMP Temporal Key (TK) for WPA2 traffic confidentiality. *Group key hierarchy* for multicast and broadcast traffic protection. The first key created is the GMK. The key GTK. Its length is 256 bit with TKIP, and 128 bit for CCMP. The TK derived from GTK is 256 bit with TKIP, and 128 bit for CCMP and it is used for confidentiality
Confidentiality	Traffic Key Encryption Algorithm	None	None	TK encryption: (I) RC4 with 128-bit KEK. (II) With AES Key Wrap with 128 bit KEK.
	Cipher Algorithms for traffic Data and Key size	RC4 with 64 bit key (WEP-40) RC4 with 128 bit key (WEP-104)	RC4 with 256-bit key.	AES-CCM with 128 bit TK
	Encrypted Frames	MPDU + ICV	MPDU + MIC + ICV	MPDU + MIC
Integrity	Integrity Algorithm	32 bit ICV with CRC-32	(i) 64 bit Michael MIC. (ii) 32 bit ICV	(i) 64 bit CCM MIC for traffic messages (ii-a) HMAC-MD5 with KCK, (ii-b) HMAC-SHA1 with 128 bit KCK for EAPOL 4-way handshake.
	Protected Frames	MPDU	[Michael MIC]: MSDU Sender and Destination Address (SA, DA), the MSDU Priority, and the MSDU payload [ICV]: MPDU	[MIC]: MPDU+ Additional Authentication Data (AAD). The AAD is comprised of the MPDU header, subfields from MAC frame control, addresses from source and destination fields, Sequence Control (SC), QoS control field. [HMAC]: EAPOL 4-way handshake messages

(b)

	IEEE Protocol	WiMAX	
		802.16	802.16e
Authentication	Method	Privacy Key Management Protocol (PKM). Only SS authentication with X.509 version 3 and RSA public-key cryptography	2 PKM versions. V.1 is the 802.16 PKM, and V.2 is more enhanced with mutual authentication option (BS presents its certificate to SS). Two authentication schemes can be used separately or combined: RSA, EAP, RSA-EAP, EAP after EAP authentication. For RSA, client authentication with X.509 v.3 certificates. EAP uses credentials: X509 certificate for EAP-TLS, or Subscriber Identity Module for EAP-SIM.
Key Derivation and Management	Key Management and short description	After Certificate approval, BS sends authorization reply with Authorization Key (AK) encrypted with client's Public Key, and the Security Association set Identity (SAID). From AK derives KEK, HMAC_KEY_U, HMAC_KEY_D, (U for uplink and D for downlink). The last two keys used for the HMAC digest for management messages. For every SAID, a TEK state machine is responsible for key material usage. TEK sends periodically messages for key content refresh. TEK key material is used for uplink and downlink encryption. BS maintains 2 sets of active AKs and TEKs, old and new for each SAID. There is a 4-bit AK sequence number increased by one for each new AK. Additionally a 32-bit packet number (PN). Both prevent replay attacks	AK in PKM v.2 operates as in PKM. In PKM v.2, there two key material primary sources. For RSA, BS' initial key material is the 256-bit pre-PAK (primary authorization key). Pre-PAK gives 160 bit PAK and 160 bit EIK (EAP Integrity Key). PAK+EIK+SS MAC address + BSID generate AK. For EAP only, the initial key is the 512-bit Master Session Key (MSK) and generates the 160 bit Pairwise Master Key (PMK) and optionally the 160 bit EIK with MSK truncation to 320 bits. From PMK+SS' MAC address + BSID AK derives. For RSA-EAP, PAK and EIK derive from RSA and PMK from EAP. AK is generated from PAK XOR PMK+ SS' MAC address + BSID. For EAP after EAP, PMK1 and EIK derive and from 2nd EAP PMK2 derives. PMK1 XOR PMK2+SS' MAC address and BSID, the AK derives. From AK 3 keys derive: One is the 128-bit KEK and the other two are: (I) The 160 bit HMAC_KEY_U and HMAC_KEY_D, if HMAC is used, and (II) The 128 bit CMAC_KEY_U and CMAC_KEY_D, if CMAC is used. If EAP only is used, the three aforementioned keys will derive from EIK. All key derivations are based on the Dot16KF algorithm
Confidentiality	Traffic Key Encryption Algorithm	(i)112 bit 3-DES with 64 bit KEK, if TEK is 64 bits. (ii) AES in ECB mode with 128 bit KEK, if TEK is 128 bits. (iii) RSA encryption with SS's public key if TEK is 128 bits.	(i) 112 bit 3-DES with 64 bit KEK, if TEK is 64 bits. (ii) AES in ECB mode with 128 bit KEK, if TEK is 128 bits. (iii) RSA with SS's public key if TEK is 128 bits. (iv) AES Key Wrap with 128-bit KEK for 128-bit TEK encryption.
	Cipher Algorithms for traffic Data and Key size	(i) DES- CBC with 56 bit TEK and 64 bit block encryption along with 64 bit IV. (ii) AES in CCM mode with 128 bit TEK.	(i) DES in CBC mode. (ii) AES in CCM mode. (iii) AES in CBC mode with 128 bit TEK.
	Encrypted Frames	MPDU + ICV	MPDU + MAC (Message Authentication Code)
Integrity	Integrity Algorithm	(i) DES-CBC mode for 64 bit ICV. (ii) AES-CCM mode for 64 bit ICV. (iii) SHA-1 for HMAC.	(i) DES-CBC mode for 64 bit MAC. (ii) AES-CCM mode for 64 bit MAC. (iii) AES-CBC mode for 64 bit MAC. (iv) SHA-1 for HMAC Digest. (v) AES-CMAC value.
	Protected Frames	[ICV]: MPDU + additional packet information. [HMAC]: Management messages.	[MAC]: MPDU = additional packet information. [HMAC]: Management messages. [CMAC]: Management messages + additional information.

On the other hand, the Robust Security Network Association (RSNA) with the 802.11i and the WPA2 does provide a secure wireless network operation, and it is the only security mechanism in WiFi that operates with AES encryption, CCMP integrity mechanisms, key derivation and management with EAPOL, and secured user-authentication with the 802.1X protocol, that resembles with the strong mechanisms that WiMAX uses.

5. Threat Model for WiFi and WiMAX Networks

Wireless networks face potentially more threats due to the lack of physical infrastructure. Some of the consequences of these attacks include the loss of proprietary information, legal and recovery costs, and the loss of network service. Network security attacks are typically divided into passive and active attacks [17].

In passive attacks an unauthorized entity monitors the traffic, but does not modify its content. Passive attacks are divided in two categories.

(1) eavesdropping, where the adversary monitors the transmissions between a station/SS and an AP/BS,

(2) traffic analysis where the adversary listens into the transmission in order to obtain information from the transmitted packet-flow.

In active attacks, the adversary proceeds to actions in order to achieve his malicious intentions, using sometimes information obtained from earlier passive attacks. Active attacks can be divided in four categories.

(1) Masquerading (Spoofing). This type of attack is actually a man-in-the-middle attack, where an adversary places himself between two parties and manipulates the communication between them. There are two types of spoofing: AP/BS, and MAC address spoofing. In the first, the adversary pretends to be a legitimate AP/BS and tricks users to join the rogue AP/BS network and therefore gains access to information, possible valuable for malicious purposes. With MAC address spoofing, where the MAC address is used to authenticate a station/SS, an adversary can replicate the address of a user.

(2) Replay attacks. With this attack an adversary reuses valid transmitted packets that he has intercepted, without modifying the message during retransmission.

(3) Message modification attacks, where the adversary tampers the content of legitimate messages.

(4) Denial-of-Service (DoS), where the adversary prevents the normal network operation with various ways in PHY and in MAC layer. In PHY layer the attack methods are: (i) jamming, where a device emits electromagnetic energy on the network's frequencies. The energy makes the frequencies unusable by the network, causing a denial of service. (ii) Scrambling, which is similar to jamming but it is applied for short intervals of time and targeted to specific frames or parts of frames, usually control or management messages, in order to disturb the normal network operation [15]. In MAC layer the attack is implemented with the transmission of messages, aiming to decrease the network efficiency.

5.1. WiFi Threat Analysis. The operation of WiFi for almost a decade has revealed various serious security weaknesses like cryptographic vulnerabilities, network exploitations and denial of service attacks, which easily can compromise the wireless network security.

5.1.1. Passive Attacks. The passive attacks in WiFi networks can provide valuable information to adversaries. With eavesdropping, it is possible to gain information about the parties' identity and the time they communicate. With traffic analysis it is possible to analyze traffic patterns and determine the content of communication, as short bursts of activity could mean instant messaging and steady streaming could reveal video conferencing. Additionally monitoring and traffic analysis is the first step to proceed and break cryptographic keys and thereby compromise the network confidentiality and the authentication procedures. Passive attacks, due to the characteristics of the wireless network, are applicable to all WiFi schemes, namely WEP/WPA/WPA2, since all packet traffic can be sniffed and stored.

5.1.2. Active Attacks

Key Cracking. As mentioned earlier, traffic analysis is the first step to cryptographic keys cracking. Indeed, the IV portion of the RC4 key is not encrypted, which allows an eavesdropper by analyzing a relatively small amount of network traffic to recover the key having the IV value known with the advantage of the small 24-bit IV key space, and a weakness in the way WEP implements the RC4 algorithm. Thus, if two messages have the same IV, and the plaintext of either message is known, it is relatively easy for an adversary to determine the plaintext of the second message [8]. Additionally, many messages contain common protocol headers or other easily guessable contents, and therefore, it is possible to identify the original plaintext contents with minimal effort. Even traffic with sequentially increasing IV values is susceptible to attack. There are 16.777.216 million possible IV values; on a busy WLAN, the entire IV space may be exhausted in a few hours. When the IV is chosen randomly, which represents the best possible generic IV selection algorithm, by the birthday paradox two IVs already have a 50% chance of colliding after about 2^{12} frames [18, 19]. As analyzed before, the use of stream ciphers is dangerous and therefore WEP and WAP face a serious threat. With the implementation of AES-CCM with 128-bit key in WPA2, the traffic data confidentiality is well secured. Shared key authentication in WEP and WPA can be breached quite easily. One way is a man in the middle attack where an adversary eavesdrops, captures and views the clear-text challenge value and the encrypted response.

Then he can analyze with off-line brute-force or dictionary attacks the clear-text and the encrypted challenge and thus determine the WEP key stream. Moreover, authentication attack can be achieved by injecting properly encrypted WEP messages without the key [18]. Another problem with shared key authentication is that all devices have to use the same WEP key because WEP does not support key management as WPA and WPA2 when they use 802.1X authentication with EAPOL 4-way handshake. Therefore, if the key is compromised, it needs immediately to be replaced from all stations.

Masquerading: Spoofing. Another way to surpass authentication is the MAC address spoofing [10]. Even if the 48-bit address is large enough to prevent brute force guessing, methods for MAC address filtering and the fact that the address is broadcasted freely in the wireless network, makes it easy for an adversary to obtain it by sniffing the victim's communication. With various programs available to change the MAC address in a PC network adapter within minutes, even if the value in the hardware is encoded and cannot be changed, the firmware value can be altered [20]. Moreover, due to the fact that the AP is not authenticated to the station, an adversary can masquerade a legitimate AP and spoof a station to join the malicious network. The 802.1X supports mutual authentication and therefore the station is secured that the AP is legitimate. On the other hand, 802.1X with EAP-TLS prevents an adversary from forging, modifying, and replaying authentication packets, provided mutual authentication is used. Nevertheless, during the 4-way handshake a session hijacking is possible after the 3rd message sent from AP for successful EAP. At this point, the adversary sends a disassociation management frame to the station-victim to get disassociated, while the 802.1X state machine of the authenticator still remains in the authenticated state. The consequence of this is the network access gaining from the adversary using the MAC address of the authenticated supplicant [21]. Besides that, 802.1X authentication is a very strong authentication mechanism and undoubtedly is preferred in WLANs.

Replay Attacks. WEP does not provide protection against replay attacks because it does not include features such as an incrementing counter, nonce, timestamps that could detect replayed messages immediately. In WPA/WPA2 the 48-bit unique number for each packet is sufficient to prevent replay attacks.

Message Modification. Except from the confidentiality breaching of the implemented algorithms, the integrity algorithm, the CRC-32 can be tampered with bit flipping attacks, since an adversary knows which CRC-32-bit will have to change when message bits are altered even if the CRC-32 ICV is encrypted, because a property of stream ciphers, such as WEP's RC4, is that bit flipping survives the encryption process, as the same bits flip whether or not encryption is used [22]. Michael MIC on the other hand prevents an adversary from inserting modified messages. Even if the adversary intercepts a packet and forwards it to the victim-station later with a valid encrypted MIC, the station will check that the PN is out-of-order and the packet will be discarded. With CCM the integrity of the message is much more secured because besides the payload, CCM authenticates Additional Authentication Data (AAD) as MAC frame control, Sequence Control (SC), addresses from source and destination fields, making thus the message modification impossible, even in the fields sent clear in the air. Additionally message authentication in EAPOL 4-way handshake provides a secure way to key distribution. Although 802.11i protects data frames, it does not offer integrity protection to control or management messages. An attacker can exploit the fact that management frames are not authenticated, and thereby, he can use such messages to destabilize the normal network operation. A message modification threat concerning all WiFi schemes is the IP redirection attack. In this attack the AP acts a router with internet connectivity, which is usually the case, and the adversary all it has to do is to sniff an encrypted packet off the air [18], modify it by giving it a new IP destination, and redirect it to an address belongs to him. Later on, the AP will decrypt and send the packet to the new malicious destination, where the adversary can read the packet in the clear.

DoS Attacks. DoS attacks in WiFi can cause serious implications in the network efficiency. In the PHY layer, jamming can affect the network operation not only intentionally by an adversary, but from other WLANs transmitting in the same frequency, which is something possible since channels in the ISM band are very few. In the MAC layer, the availability can be suspended with flooding attack, where the adversary takes advantage of the CSMA/CA mechanism by constantly transmitting many short-length packets in a fast rate. The effect of this effort is that each station within the network range assumes that the medium is busy and, therefore, each station listens to the medium and waits patiently for its turn to transmit for as long the adversary uses this attack. The implementation of this attack can be achieved easily [23] by placing a wireless network interface card into a test mode where it continuously transmits a test pattern. Another DoS threat is the De-authentication attack, where the adversary, as a legitimate AP, uses the deauthentication message to all stations ordering them to quit the network. The attack is successful since the AP address has been found, which is easy as it is transmitted in the clear, and the adversary has only to listen to the medium and obtain it [24]. With the address available, the adversary transmits the de-authentication message as a legitimate AP. Consequently, every station gets misled and stops communication with the network, having again to repeat the authentication procedure. Another threat is packet removal by an adversary and thus prevention from reaching its destination. This can be done if the adversary interferes in the reception process by causing CRC errors so that the receiver drops the packet. Additionally, if the adversary uses a bidirectional antenna, he can delete the packet on the receiver's side, and simultaneously using another antenna to receive the packet

for himself if he wants so [10]. The aforementioned DoS attacks can be implemented in every WiFi scheme.

5.2. WiMAX Threat Analysis. The security in IEEE 802.16-2004 and 802.16e standards is one of the most important issues in the protocol architecture. The implementation of strong and efficient mechanisms makes the WiMAX security very efficient. Nevertheless, in this short period of their existence, various weaknesses have emerged. Some of the possible threats are similar to the ones that WiFi faced; this observation stresses on the importance of the WiFi threat analysis and the prevention measures that can be taken for WiMAX. Of course, threats in WiFi did not appear right after the introduction of the standards; it took a long period of efforts and computing time from hackers, Government Agencies, Universities, and Research Institutions to reveal the security vulnerabilities issues. This is very important because WiMAX is new and not sufficiently operated to reveal the actual weaknesses it might face, making thus the threat analysis evaluation based on WiFi attacks and estimated vulnerabilities from the new mechanisms of the standard.

5.2.1. Passive Attacks. As mentioned earlier, passive attacks are achievable in a wireless network during packet transmission. Eavesdropping and traffic analysis threats can be used to determine the behavior of an entity about the transmitting times. Moreover, due to the fact that management messages are sent in the clear, they can provide valuable information about the location of the SS at a certain period of time [15]. Additionally monitoring and traffic analysis is necessary to proceed with cryptographic keys cracking to compromise the confidentiality and authentication mechanisms.

5.2.2. Active Attacks

Key Cracking. Cryptographic immunity in WiMAX is based on the fact that the AK remains secret between the BS and the SS. If this is not the case, security is breached. Therefore, the AK generation mechanism and the AK generation material are two important issues. The AK creation according to the standard is assumed to be random with the usage of a uniform probability distribution; if this is the case, it must be explicitly defined. Another important matter is the key material used for the AK generation. The standard defines the BS responsible for the AK creation. The potential problem is if the random number generator appears specific bias to expose the AK. The same issue appears with TEK generation, as the standard fails to specify that the TEK is created using a uniform probability distribution and a cryptographic-quality random number generator [12]. TEK's lifetime is important if the usage period is approaching its maximum value (7 days) and the DES-CBC cipher is implemented. In 1998, the Electronic Frontier Foundation [13, 25] broke a DES encryption in less than three days period, using a DES cracker-machine with a structure costing less than 250.000$. It is obvious that after a decade where computation efficiency is enormous and the hardware costs are constantly decreased, the DES cipher should be considered weak. DES uses a 64-bit block size. One theorem [12] describes that a CBC mode using a block cipher with an n-bit block cipher loses its security after operating on $2^{n/2}$ blocks with the same encryption key. Therefore, with $n = 64$, the maximum safely protected 64-bit blocks are 2^{32}. With an average throughput of 10 Mbps the 2^{32} blocks are produced within 7.6 hours approximately and thereby if TEK's lifetime is at the default value, namely 12 hours, the security can be compromised. Furthermore, the CBC mode requires a random IV to ensure security but the standard uses a predictable IV [12]. On the other hand, AES with key size of 128 bits, and the consideration of the current and the projected technology, makes brute-force attacks impractical [13]; thereby, the usage of AES-CCM and additionally the AES-CBC for the 802.16e, makes data traffic secured. Nevertheless, AES-CCM faces a potential threat when the key-PN combination is used more than once; the reason is that two packets encoded with the same key-PN combination eliminate the security guarantees of the CCM mode. To prevent this, the new key request as described in the standard, demands renewal when more than half of the available numbers of the 32-bit PN have been exhausted. Finally, TEK encryption is well secured with all encryption schemes. Considering though energy consumption, the RSA encryption of TEK with SS's public key and the calculating cost, makes this scheme useful only if for some reason the KEKs cannot be usable for a period of time.

Masquerading: Spoofing. In case of unilateral and not mutual authentication, a rogue BS can masquerade a legitimate BS and spoof a number of SSs by using the BS's address, stolen over the air by intercepting management messages. Nevertheless, since the adversary has to transmit during the legitimate transmission, the procedure is more difficult due to the time division model [15]. Moreover, the signal of the rogue BS must be stronger from that of the legitimate BS. If this is done, the adversary waits until a time slot is allocated to the legitimate BS and commences the attack. As in WiFi, the threat of MAC address spoofing is viable. As it is defined in the standard, each SS has a 48-bit MAC address burned into the firmware and it is used as verification element during authentication procedure from the BS. Currently all 802.16 based network equipment is in the form of standalone units, where MAC address modifications require changes at the firmware level which is difficult unless aid if provided from the manufacturer [20]. Unfortunately this will change since one of the WiMAX Forum members, Intel, announced that it plans to sell IEEE 802.16 compliant chipsets inside laptops [26]. If this is to be implemented, spoofing a MAC address will be easy for WiMAX as it is for WiFi.

Replay Attacks. The PKM v.1 authentication protocol is susceptible to replay attacks since the first and the second message from the SS, and the third message from the BS, do not provide any freshness with nonce or time-stamping, nor implement any message authentication scheme. If the adversary replays any of the three messages the receiver, either the BS or the SS, cannot determine who really the

sender is. Despite the fact that replay authentication messages attacks cannot expose the strongly encrypted AK, it can lead though to a severe result. The reason is that if BS has a timeout value to reject authorization requests (Auth-REQ) from the same SS within a certain period of time, the rightful request from the victim SS will be ignored and thereby leads to Denial of Service (DoS). In case where the BS accepts the requests, a new AK generation will take place continuously leading to exhaustion of the BS's capabilities [27]. In PKM v.2 RSA authentication, the BSNonce along with the SSNonce from the second message ensure freshness against replay attacks on the third message. Nevertheless, a replay attack on the second message just as described before in PKM v.1 is possible since the BS cannot realize that the SSNonce is not fresh. A replay attack can appear in both PKM SA-TEK 3-way handshake versions. In PKM v.1, a request message sent from a SS at an earlier time can be constantly replayed by an adversary, forcing the BS to reply with new TEK key material, exhausting thus the BS's capabilities. Nevertheless, message replay attack cannot succeed anytime. The threat is successful only if the used for the replay attack intercepted message had the same AK during the actual time of the attack. That is, each message is authenticated with an HMAC digest; if the HMAC_KEY_U used for the digest during the message creation, derived from a different AK than the current, the digest would not match and the message would be discarded, leading thus to a failed replay attack. Unfortunately, AK's lifetime ranges between 1 to 70 days with default value the 7 days, making thus the attack very possible for a long period of time. In PKM v.2 the replay attack cannot succeed because of the BSNonce in the SA-TEK challenge message. Since the fact that the BS sends SA-TEK challenges with different nonce, the adversary cannot succeed if he replays the SA-TEK request message, because the BSNonce in the replayed message is not longer valid and thereby, the message will be discarded from the BS. The data traffic is also secure from replay attacks, since each packet has a 32-bit number (PN) preventing from repeated packet numbers.

Message Modification. Authentication and integrity protection in each MPDU payload with DES-CBC, AES-CCM, and additionally AES-CBC for PKM v.2 makes message modification a failed attack. Moreover, management message authentication with HMAC and CMAC is secured to modification. Another weak point appears in the third message sent by the BS in PKM v.1 authentication procedure where message integrity mechanism does not exist. A man in the middle attack is possible to intercept and modify the third message, causing a serious DoS attack. Since that the message does not have any integrity mechanism the adversary can modify the encrypted AK and send it to the victim SS. The SS will decrypt a different AK from the initial legitimate key generated from BS. The usage of the wrong AK key from the SS will lead to the creation of non-legitimate KEK, HMAC_KEY_D, HMAC_KEY_U keys, and consecutively to the decryption from the SS of the TEK sent from the BS with a wrong KEK. As a consequence, the communication between SS and BS will be impossible, since all management messages sent from SS will have different HMAC digests and they will be discarded from BS and vice versa, and moreover, the data traffic encryption-decryption procedure with TEK will lead to the impossible revelation of the plaintext. The problem is fixed in PKM v.2 since the BS uses RSA signature to ensure the integrity of the message and thereby any modification on the encrypted AK will be known to the SS, since the signature comparison from the BS and the signature of the modified message from SS will be different, and therefore the message will be discarded. Leaving aside the secure message authentication implemented in WiMAX, replay and message injection attacks face another difficulty—the timing and the synchronization to inject a message. The adversary has to find an open slot in the schedule and get prepared for his transmission. Even if the adversary knows the propagation delay as a part of the initialization procedure, when he has to inject the message from a BS, he does not know how much propagation delay will meet. Moreover, the adversary has to surpass the stateful characteristic of the WiMAX MAC layer. MAC accepts messages only at certain times, and thereby, it will not respond to messages exceeding this period of time [20]. Therefore, the aforementioned difficulties make replay and message injection a very difficult task to do.

DoS Attacks. WiMAX like every wireless network is susceptible to jamming and scrambling. Nevertheless jamming can be detected quite easily and cannot affect the network severely. Scrambling as mentioned, targets selective control or management messages in order to destabilize the normal network operation, especially when they are time sensitive messages such as channel measurement report requests or responses, which are not delay tolerant. Moreover slots of data traffic can be scrambled, forcing the victim-users to retransmit. Scrambling though needs to surpass important technical difficulties to be successful. The reason is that the adversary must interpret control information and send noise during specific intervals [15]. As shown in WiFi, a deauthentication attack leads to serious DoS. In WiMAX the corresponding message is the Reset Command (RES-CMD) message, where the SS upon receiving this message begins complete reset. An exploitation of this message by an adversary is not possible since the specific management message is authenticated, and thus, a serious DoS attack is prevented. Nevertheless, through the authorization state machine and the Auth Invalid message, a similar DoS attack is possible. The Auth Invalid message can be exploited by an adversary for the flowing reasons.

(i) It is not authenticated and thus can be easily created.

(ii) The message will be accepted from the SS at anytime.

(iii) The message does not utilize the PKM Identifier serial number, and therefore the SS will not discard it as a message with an unmatched Identifier field.

Thereby, if the adversary attacks with this message, it causes a SS transition from the Authorized state to the Reauth Wait state. When the Reauth Wait timer expires, a Reauth Request is sent by the SS, requesting another chance to rejoin the

Table 2: WiFi and WiMAX threat analysis comparative overview.

(a)

IEEE Protocol		WiFi		
		WEP	WPA	WPA2
Passive attacks	Eavesdropping	Cannot be avoided. (i) Traffic patterns can determine the content of communication (Video conferencing, Instant messaging) (ii) Station's and AP's MAC address interception	Cannot be avoided. (i) Traffic patterns can determine the content of communication (Video conferencing, Instant messaging) (ii) Station's and AP's MAC address interception	Cannot be avoided. (i) Traffic patterns can determine the content of communication (Video conferencing, Instant messaging) (ii) Station's and AP's MAC address interception
	Traffic analysis	Cannot be avoided	Cannot be avoided	Cannot be avoided
Active attacks	Key cracking	RC4 key cracking very possible	RC4 key cracking very possible	AES provides safety—No key cracking possible
	User-Authentication Breaching	(i) Shared key authentication weak due to RC4 (Brute force, dictionary attacks) (ii) Firmware change leads to authentication breaching	(i) Shared key authentication weak due to RC4 (ii) Firmware change leads to authentication breaching (iii) 802.1X very secure	(i) Firmware change leads to authentication breaching (ii) 802.1X very secure
	Masquerading (Spoofing)	(i) Station masquerading (ii) AP masquerading	(i) Station masquerading (ii) AP masquerading (When 802.1X is not used)	802.1X authentication very strong but session hijacking is possible after the 3rd message from the AP for successful EAP
	Replay attacks	Yes, no mechanism to prevent replay attacks	48-bit TKIP sequence counter (TSC) to prevent replay attacks	48-bit packet counter to prevent replay attacks
	Message modification attacks	CRC-32 weak to prevent such attacks	(i) CRC-32 weak to prevent such attacks (ii) MIC prevents such attacks on MSDU	CCMP provides safety in modification attacks
	DoS attacks (PHY layer)	Jamming	Jamming	Jamming
	DoS attacks (MAC layer)	(i) Network block with CSMA/CA exploitation (ii) De-authentication attack (iii) Deliberate CRC errors	(i) Network block with CSMA/CA exploitation (ii) De-authentication attack (iii) Deliberate CRC errors	(i) Network operation blocking with CSMA/CA exploitation (ii) De-authentication attack

(b)

IEEE Protocol		WiMAX	
		802.16	802.16e
Passive attacks	Eavesdropping	Cannot be avoided. (i) Information disclosure of the SS's location at certain period of times due to the fact that management messages are sent in the clear (ii) SS's and BS's MAC address interception	Cannot be avoided. (i) Information disclosure of the SS's location at certain period of times due to the fact that management messages are sent in the clear (ii) SS's and BS's MAC address interception
	Traffic analysis	Cannot be avoided	Cannot be avoided

(b) Continued.

	IEEE Protocol	WiMAX	
Active attacks	Key cracking	(i) With DES-CBC there is possibility of cracking if TEK (ii) With AES-CCM, threat if PN-key combination is used more than once (iii) TEK encryption well secured	(i) With DES-CBC there is possibility of cracking (ii) With AES-CCM, threat if PN-key combination is used more than once (iii) With AES-CBC, no key cracking possible (iv) TEK encryption well secured
	User-Authentication Breaching	If network equipment stop being standalone units, as it is the case now, and instead 802.16 compliant chipsets take their place inside laptops, as it was announced from WiMAX forum members, the change of Firmware can lead to authentication breaching	If network equipment stop being standalone units, as it is the case now, and instead 802.16 compliant chipsets take their place inside laptops, as it was announced from WiMAX forum members, the change of Firmware can lead to authentication breaching
	Masquerading (Spoofing)	(i) SS's MAC address spoofing (ii) Lack of mutual authentication could lead to BS's spoofing	(i) SS's MAC address spoofing (ii) Lack of mutual authentication with PKM v.1 could lead to BS's spoofing
	Replay attacks	(i) In PKM authentication, replay attack on the 2nd and 3rd message (ii) In SA-TEK 3-way handshake replay attack possible if AK hasn't changed	(i) In PKM v.1 authentication, replay attack on the 2nd and 3rd message (ii) In PKM v.1 SA-TEK 3-way handshake replay attack possible if AK hasn't changed (iii) In PKM v.2 authentication, replay attack on the 2nd message
	Message modification attacks	(i) Message modification of the 3rd message in PKM of the encrypted AK (ii) For data traffic integrity, DES-CBC and AES-CCM mode ensure safety on message modification attacks (iii) The HMAC protected Management messages are safe on modification attacks	(i) For data traffic integrity, DES-CBC, AES-CCM and AES-CBC mode ensure safety on message modification attacks (ii) The HMAC and CMAC protected Management messages are safe on modification attacks
	DoS attacks (PHY layer)	(i) Jamming (ii) Scrambling (on control and management messages)	(i) Jamming (ii) Scrambling (on control and management messages)
	DoS attacks (MAC layer)	(i) Message modification of the 3rd message in PKM (ii) Replay attacks on 2nd message in PKM authentication (iii) Replay attack in SA-TEK 3-way handshake, if AK hasn't changed (iv) DoS attacks with Reset Command (RES-CMD) management message (v) DoS attacks with Ranging Response (RNG_RSP) set to value 2 [Abort]	(i) Message modification of the 3rd message in PKM v.1 (ii) Replay attacks on 2nd message in PKM v.1 and v.2 authentication (iii) Replay attack in PKM v.1 SA-TEK 3-way handshake, if AK hasn't changed (iv) DoS attacks with Reset Command (RES-CMD) management message (v) DoS attacks with Ranging Response (RNG_RSP) set to value 2 [Abort]

network. The period of the Reauth Wait timer is measured in seconds and if additionally an Auth Reject message is sent at this point, it will lead the SS to the Silent state where it ceases subscriber traffic, responding only to BS's management messages [20]. The usage of the Auth Reject message is achievable since that it is not authenticated as well. The Ranging Request (RNG-REQ) message is the very first message sent by an SS seeking to join a network where the SS requests transmission timing, power, frequency and burst profile information. RNG-REQ is also sent periodically for SS's adjustments. Moreover, the BS can use this message when it demands uplink and downlink channel changing, power transmission modifications and finally, termination of all transmissions and MAC re-initialization of a SS. It

is obvious that if this message could be exploited by an adversary, it would cause a serious DoS attack. Unfortunately, this message is not encrypted, authenticated and it is stateless, making it thus a candidate for DoS attack. Thereby, an adversary can spoof a specific SS by sending an RNG-RSP message, with the ranging status field set to value 2, which means "abort" [20]. The SS's address can be easily obtained by sniffing the channel IDs it uses.

5.3. WiFi-WiMAX Threat Analysis Overview. In this entity with the aid of the following table (see Table 2) we present a summary of the possible threats that WiFi and WiMAX could face during the network operation.

In WiFi, the establishment of the Robust Security Network Association (RSNA) with the 802.11i founds the implementation of a really secure wireless network operation. The pre-RSNA period with WEP and WPA, and the implementation of RC4 encryption in the information confidentiality (privacy) and the user authentication operation, is not secure and easily can be breached. Additionally, the CRC32 checksum cannot guarantee the information integrity of the MPDU's. Moreover, the often key renewal is not an easy task because it requires a key method delivery which is out of the pre-RSNA WiFi operation. On the other hand, the RSNA period forms a secure operation of WiFi. The usage of the AES-CCMP encryption scheme in the confidentiality (privacy) of the information makes key cracking impossible, The CCMP implementation guarantees the integrity of the MPDU along with some Additional Authentication Data (AAD), and the 802.1X authentication provides secure key management and user authentication procedure. Nevertheless, due to the nature of the protocol architecture, the RSNA appears the same weaknesses like WEP and WPA, with two important DoS attacks:

(i) transmission prevention with the fast and constant transmission of short packets, taking advantage of the CSMA/CA algorithm operation,

(ii) De-Authentication attack which uses the ability of the MAC address forging with a simple firmware change.

As mentioned before, WiMAX implements much more enhanced security mechanisms to prevent any possible threats. Leaving aside the specific cryptographic suites that WiMAX uses, the protocol architecture can be characterized with two important features: (a) MAC has a connection-oriented architecture, assigning each slot to a certain connection, each one belonging to various services, like network management and data transport, all of which implement its own security parameters, (b) the stateful characteristic of the WiMAX MAC layer where MAC accepts messages only at certain times, rejecting thereby messages exceeding a defined period of time.

The aforementioned characteristics prevent many Denial of Service attacks, as described in the threat analysis section, make any connection exploitation and message injection extremely difficult. In addition to the sophisticated MAC operation, the WiMAX implemented security mechanisms enhance even more the network security. It is apparent from the detailed description of the WiMAX security mechanisms that user-authentication becomes secure with the X.509 certificates and the RSA asymmetric encryption, especially with PKM v.2 where mutual authentication is needed. Nevertheless, the 802.16 PKM authentication, as shown before, appears some flaws that could lead to some DoS attacks. The confidentiality and the integrity with WiMAX are well secured, although the TEK lifetime could be an issue when DES-CBC is used for data traffic encryption. Even if some management messages implement integrity mechanisms with HMAC of CMAC digests, and thus provide protection on modification attacks, the lack of the implementation to all management messages as shown could lead to serious DoS attacks. As a conclusion it can be stressed that WiMAX implements strong security mechanisms, much more enhanced from WiFi, especially with the 802.160e standard which is used for full mobility characteristics.

In the case of mobility though, an important issue should be determined that concerns the hand-over procedure of a mobile station. The hand-over mechanism is not defined in the 802.16e protocol and it is extremely important to be the fast, secure at the key exchange and the probable authentication procedure, and finally, seamless in real-time applications during the mobile station transfer from one Base Station to another.

6. Guidelines for Secure WiFi and WiMAX Networks

From the WiFi and WiMAX threat analysis, we concluded that WiMAX implements stronger security mechanisms and succeeds to block most of the threats in a wireless network. Nevertheless some weaknesses still exist in WiMAX as well; in the following, we will try to identify the recommendations for WiFi and WiMAX, on how specific mechanisms should be used, how specific security options shall be set and if new security mechanisms, additional to the ones available with WiFi and WiMAX, are needed in order for the network will operate more securely and robustly.

Passive attacks in any wireless network are unavoidable since all messages are transmitted freely in the air. If the network is to ensure the confidentiality of the data traffic by implementing strong encryption schemes as it is recommended later we could minimize the risks of passive attacks.

6.1. Guidelines for WiFi Networks

6.1.1. WEP Security. Threat analysis showed how insufficient is WEP security. The possibilities to enhance security are limited, and if WEP is the only available solution the only thing that can be done to enhance security is the constant key renewal is short periods of time (i.e., each day).

6.1.2. WPA Security. The usage of RC4 encryption faces the same important security issue as described in WEP, even if TKIP uses a different key for each MPDU encryption. Therefore, confidentiality and user shared-key authentication could be compromised as well. The only thing that can

be done, as well as in WEP, is the often key renewal in short periods of times.

In case where WPA can implement the AES-CCMP encryption-integrity security scheme, it is important to be the selected choice in order to provide secure confidentiality and integrity of the transmitted information.

With MIC (Michael) and the TSC operation, WPA succeeds to protect the integrity of MSDUs and the replay attack threat.

User authentication is well secured if the 802.1X authentication is to be used.

6.1.3. WPA2. As noted before, the implementation of the 802.11i protocol in WPA2 defines the Robust Security Network Association era where WiFi networks can be considered very safe. The confidentiality is totally guaranteed with AES encryption, while integrity is likewise secured with the CCMP implementation of the AES-CCMP scheme, where besides the MPDU, some additional authentication data (AAD) are protected as well. As mentioned with WPA, the 802.1X authentication ensures secured authentication procedure.

Nevertheless, as described in threat analysis, 802.1X can face a serious threat that could lead to a user-authentication breaching, and to a DoS attack with the transmission of a De_Auth message (Deauthentication attack). This attack appears in each WiFi security scheme and the reason is the lack of authentication in the De_Auth message.

Therefore in order to prevent this threat, a modification in the WPA and the WPA security operation can be implemented when the 802.1X authentication is used. With 801.X and the EAPOL operation, both parties-Station and AP, possess the 128 bit EAPOL Key Confirmation Key (KCK). This key is used for data origin authenticity and it can be used in the De_Auth message authentication in order to determine that the message not only left from the AP with the specific MAC address that could be changed as shown before, but it must have a legitimate digest produced with the KCK key from the authentic AP, and only the Station can confirm it.

6.2. Guidelines for WiMAX Networks

6.2.1. General Guidelines. WiMAX has already shown some *cryptographic vulnerabilities*; some of them can be fixed if the following issues and specific cipher suites are followed.

(*i*) *Random Number Generation.* A random AK and TEK generation with the usage of a *uniform probability distribution* without any bias is needed. Such a generator must be explicitly defined by the implementation [12]. Additionally, the random number could be a concatenation of two random numbers created from the BS and the SS respectively. This would prevent any possible bias if the random generation is done only by the BS.

(*ii*) *The Lifetime of Keys (AK, TEK).* Since it is understood that short-time key generations will affect the network operation by keeping the BS busy more often with key renewals, the AK can be left at its default value (7 days) and below since the strong encryption (RSA—public key) is used and it cannot reveal the AK easily. Similarly TEK's lifetime should be set not more than its default value 12 hours. This is an acceptable lifetime to ensure that TEK's immunity to key-cracking is guaranteed. It should be noted that increasing the lifetime of keys, may have some (relatively small) positive impact on performance, it does though increase significantly the exposure to key attacks.

The WiMAX forum defines two system profiles; one based on the 802.16-2004 revision of the IEEE 802.16 standard and the other based on the 802.16e amendment. The first targets the requirements of the fixed and nomadic market, and is the first to be commercially available. The 802.16e version has been designed with portable and mobile access in mind, but it will also support fixed and nomadic access. Thereby, since the cryptographic suites for two system profiles are different, we will also differentiate the security planning guidelines.

6.2.2. Guidelines for the 802.16-2004 *Profile.* The following security mechanisms should be selected for the 802.16-2004 profile in order to ensure strong authentication, confidentiality and integrity.

(*i*) *Data Traffic Confidentiality and Authenticity.* the AES-CCM mode should be implemented with 128-bit TEKs, ensuring a strong encryption mechanism. Additionally CCM provides extra data origin authentication for some data outside the payload. If DES-CBC mode is to be implemented, though, it is important to generate an IV randomly with a uniform probability distribution for each packet to ensure secured encryption.

(*ii*) *TEK Confidentiality.* Either 3DES or preferably AES-ECB will provide strong security. RSA public key encryption is not recommended due to large computational costs. It can be implemented though if for some reason the KEK production or the usage is problematic.

(*iii*) *Integrity*. HMAC with SHA-1 is the only applicable management message integrity mechanism, but ensures message authenticity.

The following modifications could enhance the security offered by the 802.16-2004 profile.

(*i*) *Signature on the Third Message.* during authentication for integrity protection with the SS's RSA public key and SHA-1 or MD-5 hash algorithm for message modification prevention. Additionally, time-stamping in the second and the third message is required for replay attack protection. Nonce is not recommended as showed since that the SSNonce in the second message does not prevent a continuous replay attack. Even if the computational cost for the signatures and the time-stamping is increased, it is a onetime procedure for the whole session and it is imperative to be implemented to ensure secure authentication.

(*ii*) *Mutual Authentication.* solution prevents masquerading attacks. Therefore, the BS shall present its certificate within the third message as in RSA PKM v.2.

(*iii*) *Time-Stamping in SA-TEK 3-Way Handshake.* in a similar way with the authentication procedure, a time-stamping should be added in the messages to prevent replay attacks. With this feature, the SA-TEK 3-way handshake will be secured.

(*iv*) *Authenticated Management Messages.* In order to prevent DoS attacks, which cause obstruction in the normal operation of the management messages, all management messages should be authenticated.

6.2.3. Guidelines for the 802.16e Profile. The second system profile, the 802.16e includes all the security schemes that are implemented in the 802.16-2004 standard profile. Therefore, all the security enhancements discussed in the previous section should also be considered with the 802.16e profile in the case where PKM v.1 is to be used.

The 802.16e has stronger and more efficient security mechanisms and thereby the PKM v.2 protocol should be used wherever possible. In this case the security planning guidelines are the following.

(*i*) *RSA along with EAP.* authentication provides strong security with *mutual authentication.* The EAP scheme is not defined within the standard but the EAP-TLS or EAP-SIM should be implemented. It is recommended that even if the authentication procedure demands extra computational cost and time, it must be used because it ensures safe authentication.

(*ii*) *Data Traffic Confidentiality.* The AES-CCM or the AES-CBC mode with 128-bit TEK provides strong encryption. Additionally, CCM or CBC provides secure data integrity.

(*iii*) *TEK Confidentiality.* The AES Key Wrap is preferable because it is specifically designed to encrypt key data, and the algorithm accepts both the ciphertext and the ICV. If it cannot be implemented, either 3DES or preferably AES-ECB mode will provide secured TEKs.

(*iv*) *Message Authentication.* The hash AES-CMAC value is the strongest integrity mechanism because except the management message, it is calculated over additional fields like the 64-bit AKID, the 32-bit CMAC PN counter, and the 16-bit connection ID. Thereby it is the preferable solution for secure message authentication. Of course HMAC can be selected if AES-CMAC cannot be implemented.

Additional modifications in PKM v.2 are suggested in the following areas.

(i) Although RSA in PKM v.2 implements nonce for the second and the third message, as described in the section on WiMAX threat analysis, the second message remains exposed to replay attacks. Time-stamping must be used instead of nonce in order to ensure replay attack protection. In additionally, RSA signatures in authentication messages should be added to prevent message modifications.

(ii) All management messages should be authenticated.

Also, it is clear that the standard misses to define as secure seamless hand-off mechanism. In the following we describe such a mechanism which if implemented will enhance the security of mobility processes.

7. Open Issues and Conclusions

The first target of this work is to analyze and compare the WiFi and WiMAX wireless network security. An important conclusion from this comparison is the highly sophisticated design of the WiMAX networks. An important reason is the operational characteristics of the WiMAX networks, covering large areas and serving many more users than a WiFi network does. Nevertheless, the protection of the information cannot be relevant to the aforementioned characteristics and every security mechanism should guarantee it. Therefore, having WiMAX security as a pattern, it can be said that WPA2 implements similar strong security characteristics and it is the only secure solution in a WiFi network.

The second target of this work is the threat analysis of WiFi and WiMAX. The conclusions from this analysis present similar results as above. In WiFi an important number of threats can create serious problems, where in WiMAX most of these threats are prevented. The reason is the enhanced security mechanisms of WiMAX, along with the operational characteristics of MAC layer. Of course, some threats are still exist, especially in 802.16-2004 standard. In addition to the already defined possible threats, in this work we indicated a weak point in the 802.16 authentication procedure with the message modification attack in the third message sent from the BS and we propose the implementation of the 802.16e authentication mechanism in the guidelines to fix it.

The highest level of security is met in the 802.16e standard, where most of the 802.16-2004 standard security issues are fixed, and simultaneously, supports the mobility feature which is very important in the contemporary way of life. Nevertheless, it leaves two important matters open as far as security is concerned. The first is the implementation of the EAP mechanism. As noted, all EAP applications need to specify mandatory-to-implement algorithms to ensure security and mutual authentication. The second issue is the mechanism to ensure soft HO. Even if WiMAX Forum [7] expects that the initial products will support only simple mobility with hard HOs, which are less complex than soft HOs, but they have a high latency and increased energy consumption. The 802.16e will finally implement full mobility, mobile VoIP, and real-time applications. Security issues remain open for this implementation as pre-authentication procedure is out of the scope of the standard. Nevertheless, a seamless, fast and secure way of key management and transfer during pre-authentication with the aim to avoid a

full repeated authentication procedure, ensuring a smooth transcend from the serving BS to the target BS, remains an open matter.

The demand for wireless broadband access is growing fast and the success is highly dependent on the security it is provided. The implementation of the security guidelines for WiFi and WiMAX networks as described before will prevent any possible threats, enhance and fix indicated flaws, and form a safe environment where wireless communication shall be embraced from users.

Acknowledgments

The author acknowledges that this article reflects personal opinion and it does not in any way represent the opinion of ENISA or any other person or an ENISA body in any way whatsoever.

References

[1] L.M.S.C. of the IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band," ANSI/IEEE Standard 802.11-1999™.

[2] L.M.S.C. of the IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Standard 802.11b™-1999.

[3] L.M.S.C. of the IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Standard 802.11g™-2003.

[4] L.M.S.C. of the IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Standard 802.11i™-2004.

[5] L.M.S.C. of the IEEE Computer Society, "Air Interface for Fixed Broadband Access Systems," IEEE Standard 802.16™-2004.

[6] L.M.S.C. of the IEEE Computer Society, "Air Interface for Fixed Broadband Access Systems. Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," IEEE Standard 802.16e™-2005 and IEEE Standard 802.16™-2004/Cor1-2005.

[7] WiMAX Forum, "Fixed, nomadic, portable and mobile applications for 802.16-2004 and 802.16e WiMAX networks," November 2005.

[8] S. Fluhrer, I. Martin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," in *Proceedings of the 8th Annual Workshop on Selected Areas in Cryptography*, Toronto, Canada, August 2001.

[9] B. Aboba and D. Simon, "PPP EAP TLS authentication protocol," *RFC 2716*, October 1999.

[10] C. He and J. C. Mitchell, "Security analysis and improvements for IEEE 802.11i," in *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS '05)*, pp. 90–110, February 2005.

[11] D. Halasz, "IEEE 802.11i and wireless security," August 2004, http://www.embedded.com/.

[12] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," *IEEE Security and Privacy*, vol. 2, no. 3, pp. 40–48, 2004.

[13] W. Stallings, *Cryptography and Network Security*, Pearson Education, 4th edition, 2006.

[14] C. Adams and S. Lloyd, *Understanding PKI*, Addison-Wesley, Reading, Mass, USA, 2nd edition, 2003.

[15] M. Barbeau, "WiMax/802.16 threat analysis," in *Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05)*, pp. 8–15, Montreal, Canada, October 2005.

[16] B. Aboba, "EAP-only security review on 802.16," IETF Liaison to IEEE 802.

[17] T. Karagiannis and L. Owens, "Recommendations of the National Institute of Standards and Technology, Wireless Network Security—802.11, Bluetooth and Handheld Devices," NIST Special Publication 800-48, November 2002.

[18] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MOBICOM '01)*, pp. 180–188, Rome, Italy, July 2001.

[19] A. Stubblefield, J. Ionannidis, and A. D. Rubin, "Using the Fluhrer, Mantin, and Shamir attack to break WEP," in *Proceedings of ISOC Symposium on Network and Distributed System Security*, February 2002.

[20] D. D. Boom, *Denial of service vulnerabilities in IEEE 802.16 wireless networks*, M.S. thesis, Naval Postgraduate School, Monterey, Calif, USA, September 2004.

[21] A. Mishra and W. Arbaugh, *An Initial Analysis of the IEEE 802.1X Standard*, Department of Computer Science, University of Maryland, 2002.

[22] K. Scarfone, L. Owens, B. Eydt, and S. Frankel, "Establishing Wireless Robust Security Networks to IEEE 802.11i," NIST Special Publications 800-97. February 2007.

[23] C. Wullems, K. Tham, J. Smith, and M. Looi, "A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs," in *Proceedings of Wireless Telecommunications Symposium (WTS '04)*, pp. 129–136, Pomana, Calif, USA, May 2004.

[24] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practice Solutions," Department of Computer Science and Engineering, University of California at San Diego.

[25] Electronic Frontier Foundation, *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*, O'Reilly, Sebastopol, Calif, USA, 1998.

[26] The Register, Intel: WiMAX in notebooks by 2006, September 2004, http://www.theregister.co.uk/2004/07/02/intel_wimax/.

[27] S. Xu and C.-T. Huang, "Attacks on PKM protocols of IEEE 802.16 and its later versions," in *Proceedings of the 3rd International Symposium on Wireless Communication Systems (ISWCS '06)*, pp. 185–189, Valencia, Spain, September 2006.