This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the ICC 2007 proceedings.

Security analysis of IEEE 802.16

Leonardo Maccari, Matteo Paoli, Romano Fantacci
Department of Electronics and Telecommunications - University of Florence
Telecommunication Network Lab
tel. : +390554796467 - fax : +390554796485 Florence, Italy
Email: {maccari, paoli, fantacci}@lart.det.unifi.it

Abstract— **This paper analyzes some critical security issues in the family of *IEEE 802.16* standard that has not been addressed so far. In particular two of the key features of the standard, the dynamic resources allocation and the mesh mode revealed to be vulnerable to attacks that represent serious threats to the robustness and privacy of the communications. In the first case the attacker is able to reduce bandwidth assigned to its neighbors, with the aim of obtaining more resources for himself; in the second case, we observed that there might be no real privacy in communications between two nodes of the mesh network. These vulnerabilities are still present even after the latest amendment to the standard, *IEEE 802.16e* that solved some previously addressed security flaws.**

I. Introduction

The family of IEEE 802.16 standards (also called Wimax) has produced high expectations from hardware vendors and Internet service providers. The main features that have been attracting a lot of attention are the possibility of having a broadband wireless access with an efficient resource allocation scheme combined with the possibility of having a mobile and mesh scenario. The first property perfectly fits the interest of an Internet service provider that wants to reach its clients directly at home or at a connection point serving a local area network, with great advantages in terms of flexibility and infrastructure costs compared to wired solutions. The second property can be seen as a more efficient and scalable alternative to *IEEE 802.11* [1] for creating mesh networks of mobile terminals, realizing a model of a pervasive network. Both these scenarios imply that the client terminals will be in direct possession of the final user, consequently some vendors already planned to include Wimax compatible devices in their laptop or mobile phones. The lesson learned with *IEEE 802.11*, that is highly vulnerable to several kind of attacks, should teach that the security features of a communication standard are highly stressed when the price of the devices lowers and they are shared among millions of users. The security protocols defined into the standard should be ready to face this scenario.

The authentication scheme used in Wimax, called *Privacy Key Management* (PKM) has already been criticized for insecurities revealed in the authentication protocol, some of which have been addressed in the latest *e* amendment that become *IEEE 802.16-2005* [2]. In this article we analyze two aspects of PKM that revealed to be insecure even after the last amendment of the standard, that are the resource allocation scheme and authentication in mesh mode. We observe that authentication for mesh mode presents some critical vulnerabilities that can lead to loss of privacy between the nodes of the mesh and that the resource allocation requests can be faked to change the medium availability for the terminal producing the attack. These two vulnerabilities hardly hit the security of two of the key features that the standard offers.

Section II will briefly give an overview of the present literature regarding security of *IEEE 802.16*, section III will describe the differences between authentication in PMP (Point Multipoint, centralized) mode and in mesh mode and will address some severe security problems that arisen in our analysis. Section IV will focus on some security problems we have observed in PMP mode, and in the last section we give conclusions and possible directions for improvement.

II. *IEEE 802.16* Security: State of the Art

The present literature regarding *IEEE 802.16* security is not particularly rich, only a few articles have been published since the standardization of the first version, in 2004. The most complete analysis of Wimax security can be found in [3], focused on the problems of *IEEE 802.16d*. The main problems addressed in that paper are the following ones:

- Lack of message integrity code (MIC) for data packets and authentication packets. Those frames can be easily replied since they contain no data to make them unique.
- Lack of authentication at the *base station* (BS) side. The BS never authenticates against the client station, so that a rogue BS can be used to perform a man in the middle attack in the same fashion as it was possible for WEP protocol in *IEEE 802.11*.
- Generation and lifetime of TEK and AK keys are insecure. The keys are generated by only one party of the authentication, so that all the trust is put on one side. Moreover, the lifetime of the TEK key can be too long and expose the algorithm to cryptanalysis. The chosen crypto algorithm is standard DES, which has proven to be outdated with respect to present needs.

The authors suggest some changes, such as the introduction of EAP protocol to harden the authentication phase, that

This work is partially supported by National project Wireless 8O2.16 Multi-antenna mEsh Networks (WOMEN) under grant number 2005093248.

1-4244-0353-7/07/$25.00 ©2007 IEEE

have been applied later on in *IEEE 802.16e*, now become *IEEE 802.16-2005*. The analysis is focused only on the PMP mode of operation of the standard, so it doesn't consider the authentication in mesh mode.

More articles that cover the security of *IEEE 802.16* family of standards are: [4], that starting from the analysis done in [3] introduces the EAP-TLS and RADIUS protocols, in a similar way as *IEEE 802.11i* does; [5] where the introduction of nonces and timestamps is suggested to harden the PKM protocol, and a secure roaming algorithm is exposed. Lastly in [6] given the known insecurities of the standard a formal threat analysis is done to reveal the risks connected with the use of Wimax.

As a starting point for the analysis presented in this article we add two generic consideration to the ones contained in the cited articles:

- The standard seems to be quite unclear about critical race conditions. There is no specified behaviour to resolve situations in which a terminal receives several different valid answers to the same request, this may generate incoherences between different terminals. Under a security point of view this is a sensitive situation because it determines the reaction of the terminals when receiving packets from both a valid machine and the attacker.
- Even if *IEEE 802.16e* introduces new features increasing the security level of the standard there is no indication that these new methods should be preferred to the old insecure ones. Conversely, *IEEE 802.11i* [7] explicitly discourages the use of WEP protocol due to the vulnerability revealed so far and strongly suggests the use of WPA protocol. In *IEEE 802.16e* there is no such recommendation, and the old and new methods are described as equivalent.

III. New vulnerabilities in mesh mode

Authentication in mesh mode is a multi-hop version of the procedure defined for PMP mode, (refer to [3] for a detailed description of authentication and key generation) even in mesh mode there must be a unique node that plays the role of base station (BS) for the purposes of access control, so that each client has to perform authentication with a centralized server. If the BS is not directly reachable, the node entering the network will use a multi-hop connection to reach it. Let's consider the situation depicted in fig. 1 where a node A entering the network, will enter in contact with a certain number of nodes that already belong to the mesh, among these nodes it will select one that will play the role of *sponsor node* (node SP), that will behave as a proxy to the BS. The SP will include any MAC frame of type *Auth Info* and *Auth Request* received from A in an UDP frame to be sent to the BS over an IP channel, it will also receive from the BS the packets of type PKM-RSP (used for authentication response) over the same UDP channel to be forwarded as MAC frames to A. The authentication procedures are the same used for PMP networks but the packets are forwarded from SP to BS, even if this is transparent to A. Once A has obtained an *AK* from the base station (in mesh mode every node receives the same *AK* key, named Operator shared secret, *OSS*) then it will start a TEK exchange with one of its neighbors, most likely starting from the SP itself. Again the procedure is the same used in PMP mode, the only difference is that SP will cipher the *TEK* key using A's private key and not the *AK* as in PMP. This difference is due to the need of assuring privacy between couples of terminals, if the *TEK* key was ciphered with the *OSS* then any other node of the network would be able to intercept the communications.

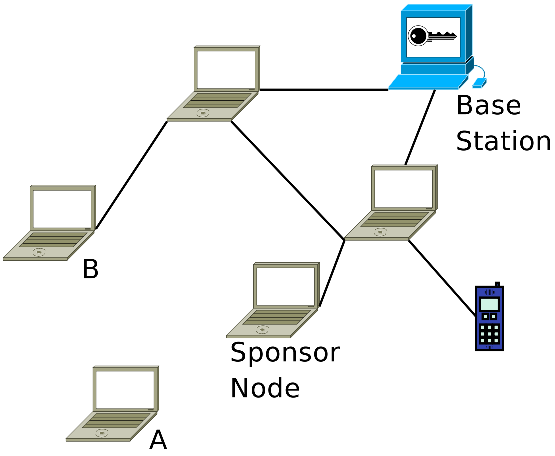

Fig. 1. Example mesh network

As in other access control protocols the phase of network entry is divided in two sub-phases: a first one in which A must show to an authentication server that it has the correct credentials to enter the network, this part ends when the machine acting as SP receives a packet from the BS that confirms the authentication; and a second one in which A will create a fresh key to communicate with its neighbors, normally starting with the SP itself. As an example (detailed later), in *IEEE 802.11i* the EAP handshake represents the first sub-phase and the WPA 4-way handshake the second one.

Since we are in mesh mode, A must be able to keep more than a single active link, the standard defines a three-way handshake aimed at *Neighbor Link Establishment* between A and another node B as follows:

```
A→B:HMAC{Operator Shared Secret,
    frame number, Node ID of node A,
    Node ID of node B}
A←B:HMAC{Operator Shared Secret,
    frame number, Node ID of node B,
    Node ID of node A}
A→B:Accept, Random unused link ID
```

Frame number is used to identify the frame in the flow of frames that has taken place between A and B before the link establishment begins. To verify its validity B will calculate multiple hashes using more recent frame numbers, in a range unspecified by the standard. Node ID's are identifiers of the terminals and the link ID is a fresh value that will identify the link after the establishment. HMAC{} is an authenticated hash algorithm.

This handshake should guarantee to A that machine B is part of the network, as well as the other way around. As we see, this handshake represents only the first sub-phase of access control, as illustrated before. Once correctly executed A and B have no private shared secret, so they have no way to communicate securely, but they share a link ID. Even if in the standard there is no explicit indication on how to secure the new link, it seems likely that a TEK exchange will follow the *Neighbor Link Establishment*.

Before going deeper in the analysis we introduce two scenarios that represent possible applications of mesh mode. If we consider a mesh network made up of fixed nodes with no mobility, the most common scenario is likely to be the backhaul network of a distribution system, in which each node of the mesh has two distinct interfaces, a first one serving with the role of access point a local area network and the second one for the core network. In such a scenario the nodes are normally belonging to the same administrator, and some logical trust relationships exist between them, that is, each node implicitly trusts each other. Once a node has shown to be an accredited member of the network it is considered trusted, so we expect no attacks from that node. If we introduce mobility, this scenario changes dramatically. The most interesting application is the creation of pervasive networks made of portable devices (smartphones, sub-laptop . . .) that create a joint ad-hoc cooperative network in a limited but scalable area. In this scenario each terminal of the network might belong to a different person or entity, so that there is no a-priori trust. Even if a node has shown the correct credentials to enter the network, it might still be a source of attacks, so the security protocols must put a very limited trust in each node of the network.

Under this point of view we should evaluate the security provided by the authentication algorithms of *IEEE 802.16*, starting from revision *d*. First of all it should be noted that there are no secret keys between any node of the mesh and the BS, there is only a unique shared key among all the nodes. This has the following consequences:

- The key can be spread to unauthorized machines to let them enter the network. This is hardly avoidable with any authentication system based on symmetric keys, still, if there exist a separate key bound to the single node and that node gives the key away, it is easy to find the culpable node. With a globally shared key this is impossible.
- It seems unclear how the *OSS* can be updated. If the lifetime of the key is the same for all the nodes, there will be a phase of overload in which all the nodes try to receive a new *OSS* from the BS, and a consequent loss of service. If the refresh method used in PMP mode will be used, in which the SS asks a new AK before the expiration of the old one, different nodes of the network might use different keys, both of them valid, according to when they asked for a refresh (the grace time for reautorization is configurable and not fixed and a node should always use the most recent key it owns). A *Neighbor Link Establishment* handshake might fail for this reason. If the *OSS* is never refreshed, the security of the system decreases with time.
- The *Auth Info* and *Auth Request* packets, and the PKM-RSP frames can be modified by the nodes over the UDP path from BS to the SP. This is an extremely serious threat that we will now explain in detail.

Since there is no authentication code in the authentication packets coming from the BS, there is the concrete possibility that a node in the IP path could modify or create new packets. Since the key is shared between all the nodes, it might decide to answer at the place of the BS, thus authorizing nodes that may not have the correct credentials. This is the major security flow that we encountered in the authentication protocol, since it completely bypasses the authority of the BS and gives to any authenticated or even external node the possibility to play that role. As a side effect, any node into the mesh could also prevent a correct authorization to be completed, sending an incorrect key that will be unusable for TEK handshake. For both the scenarios described before, the described insecurities are of high risk, since even in the less complex one they might introduce significant problems.

The second major problem we encountered is the vagueness used to define the *Neighbor Link Establishment* phase. As said, we interpreted this handshake as a way that A has to show to a neighbour B that it owns the *OSS*, so that it is an authorized station. This might be useful to create multiple links without repeating the multi-hop authentication performed the first time. As said, from this handshake no keying material is generated (no TEK is exchanged), so we suppose that as a following step a TEK exchange will be performed. Some problems arise:

- There is no way to identify different handshakes. A machine in possession of the *OSS* could repeat more then one handshake with a victim machine using a different Node ID. The victim would than be convinced of having links with more then one node while actually it is communicating with the same node; this kind of attack could be used to realize a man in the middle attack ensuring that the traffic from the victim will not take a different path on the mesh. Wimax associates a public key to each node, the usage of that public key could have prevented such an attack.
- There is no connection between *Neighbor Link Establishment* and *TEK* exchange. Since in *TEK* exchange for mesh mode, the *TEK* key is transmitted ciphered with the public key of A, B has no way to bound the Node ID obtained from the *Neighbor Link Establishment* to the public key used to cipher the *TEK*. The standard specifies that in the first frame of *TEK* exchange for mesh mode, A can include its public key (the *TEK* packets are signed with OSS key). The result is that there is no cryptographic connection between the two handshakes, B may have the two handshakes with two distinct machines both in possession of the OSS. This is the typical situation in which an insider attacker C can perform a man in the

middle attack answering at the place of B to the *TEK* request.

In the *Neighbor Link Establishment* algorithm a node creates a new link, this can be as a consequence of the loss of a previous link, performing an handover. Security considerations on handover procedures can be found in [8], as a general guideline, performing an handover without contacting the BS means that if the handover procedure is insecure, the BS looses access control over the whole network. In this case, it is clear that if a node is in possession of a valid *OSS*, it can enter the network even if it is not in possession of a valid certificate. Since the logic behind the PKM protocol is that a node should be identified by certificates installed in the physical device, this alternative procedure completely bypasses the certificate based authentication, making PKM procedure useless. Otherwise, if every TEK handshake must be preceded by an AK handshake then the function of the *Neighbor Link Establishment* is unclear. Moreover, since there is no security measure defined to protect the transmission of the OSS along the UDP path, and there are objective difficulties to refresh that key, an attacker can have some chances to obtain the OSS without possession of a valid certificate.

A. Changes in IEEE 802.16e

We briefly review how the introduction of *IEEE 802.16e* standard could influence this insecurities. The new standard lets untouched the legacy specifications relative to the mesh authentication, but introduces new packets and new authentication protocols (based on EAP [9] protocol) that can be used also in mesh mode. EAP itself, and EAP specific methods such as EAP-TLS (certificate based mutual authentication) are proven to be secure, but rely on the fact that the path between the authenticator (the role played by the SP in *IEEE 802.16e*) and the authentication server (the BS) must be secured by some AAA (Authentication Authorization Accounting) protocol such as RADIUS [10]. Strangely enough, there is no such requirement about the UDP tunnel used in Wimax, so that it is unclear how certain action required by EAP methods will be performed. As an example, using some password based EAP methods such as MS-CHAP that has been proven insecure if applied to an unciphered tunnel should be discouraged. The fact of having RADIUS protocol from BS to SP would also guarantee to A that SP is authenticated to the network, otherwise it would not be able to tunnel messages. Without this guarantee, any node can play the role of SP for the initial *OSS* exchange.

The *Neighbor Link Establishment* phase is unchanged, so that the introduction of EAP in mesh mode can be useless given the outlined vulnerabilities of the *TEK* exchange. Last, if EAP is used it is not quite clear how the same OSS can be generated for every machine.

B. 802.11i ad-hoc mode

To have a comparison with another widely used standard we briefly review the ad-hoc mode of *IEEE 802.11i*, which uses the *IEEE 802.1X* standard for access control, using EAP and RADIUS. Whenever a machine A enters the network it is authenticated with an EAP method (the standard doesn't specify a single method but mandates that it must give mutual authentication and fresh key material generation, as EAP-TLS does), the link between the authenticator and the authentication server is secured with an AAA protocol, such as RADIUS. The result of the authentication is the generation between the supplicant and the authentication server of a shared secret called *PMK*. The *PMK* is then moved on the RADIUS link to the authenticator, the *PMK* is different for every link. After this phase a 4-way handshake is performed. The requirement to complete the handshake is possession of *PMK* and the result is another key named *PTK* that will be used for encryption. For every new link the supplicant wants to activate it should repeat the whole authentication. Some key features are:

- *PMK* are different for every EAP authentication, and bound to the MAC address of the authenticator, to refresh a *PMK* a new EAP authentication must be performed.
- *PTK* are generated with keying material given by both the authenticator and supplicant.
- each data packet is ciphered and authenticated, also, it contains a sequence number which makes it unrepeatable, thus resolving problems of race conditions and reply attacks.
- authentication is always mutual.
- the use of WEP is strongly discouraged in favour of new algorithms.

As we see, even if the proposed solution is quite complicate to deploy in the most challenging scenarios, the standard offers a wide range of solutions keeping a high level of security.

IV. Miscellaneous vulnerabilies of PMP mode

In PMP mode a BS is the central node that dynamically allocates radio resources for the client stations (called SS, subscriber stations). Downlink and uplink are separated resources mapped to different frequencies or time slots depending on the chosen physical layer. The BS is the only node that can use the downlink channel while the SS can only transmit in uplink channel. The BS periodically communicates the scheduled allocation to the clients with a message of type DL-MAP and UL-MAP for downlink and uplink channels.

The BS may generate UL-MAP and DL-MAP at intervals specified into the particular PHY specification, this management messages are sent in broadcast in the downlink channel and are not authenticated by the BS.

We identified three criticalities in PMP mode:

- Incorrect application of the cryptographic primitives
- Possibility of sending *spoofed* (faked) resource requests
- Miscellaneous denial of service attacks

A. Cryptographic primitives problems

In fig. 2 is represented the CBC (Cipher Block Chaining) application of the DES encryption algorithm as used in *IEEE 802.16d*. The IV (initialization vector) value should change at each transmitted packet, its role is essential to assure that if the same packet is sent twice, it won't be ciphered in

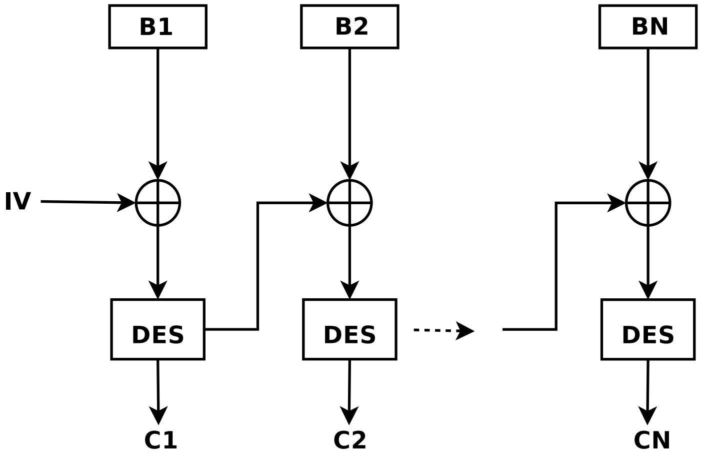

Fig. 2. Scheme of the DES *Cipher Block Chaining* mode, data are divided in blocks then the IV is XORed with the first block of plaintext. The result of every DES block is XORed with the following plaintext before encryption

the same way, avoiding traffic analysis and cryptanalysis. In donwlink the CBC IV for DES is calculated as the result of the XOR between the IV parameters of the TEK key information (initialized during the TEK exchange and transmitted in plaintext) and the content of the *PHY Synchronization* field of latest valid DL-MAP message. This procedure should assure that the IV is changed at least at every transmission of DL-MAP. The first issue about IV emerges observing that if the chosen physical medium is WirelessMan-OFDM the PHY Synchronization field is empty, so that the IV Vector will be build only by the IV parameters of TEK Key and will never change during TEK lifetime. This makes the IV useless.

General security issues connected with the generation of sequences of IV are discussed in [11]. Depending on the type of security associations the need of randomicity and secrecy for the IV might be strict or more relaxable but for any kind of application an attacker should not be able to forge valid packets with chosen IV. In *IEEE 802.16d*, since the DL-MAP frames are not authenticated an attacker could possibly inject into the network a faked DL-MAP, containing a different vector $\overline{IV}$. From that moment on, until the reception of another DL-MAP a SS will decipher the received data using $\overline{IV}$ and will send packets ciphered with $\overline{IV}$.

Decryption is done as follows:

$$\begin{cases} P_1 = D[C_1] \oplus IV \\ P_2 = D[C_2] \oplus C_1 \\ \dots \\ P_n = D[C_n] \oplus C_{n-1} \end{cases} \tag{1}$$

with *D[]* we refer to the operation of DES decryption, while C_i and P_i are respectively corresponding cipher text and plaintext blocks. Note that if the attacker is able to change the IV, he can interfere with the decryption of the first block (8 bytes) of the packets *flipping* some bits while leaving the decryption of the rest of the packet unchanged. Further analysis is needed to evaluate the impact of this design defect and verify if, depending on the upper layer protocol used, this might have consequences similar to the ones described in [12] for *bit flipping* attacks to WEP.

B. Spoofing of Bandwidth Request messages

An SS may ask and obtain channel resources using Bandwidth Request messages, requests can be aggregate (containing an absolute value) or differential (containing the difference from current assignment). Aggregate requests are sent in the unscheduled time period where each SS can transmit using a contention technique; bandwidth Requests are included into unauthenticated frames, so they might be forged by an attacker. The attacker can send false aggregate requests pretending to be some other station and requesting very limited channel resources, thus, the BS will update the schedule and communicate it with the following UL-MAP and DL-MAP.

As said, one of the most interesting features that distinguishes *IEEE 802.16* from *IEEE 802.11* is the possibility of having a centralized resource allocation to distinguish several service class, according to the credentials of the user. With this attack an authorized SS of the network can reduce the resources allocated to its neighbors with the aim of having more resources disposable to itself. If the attack is repeated at every time interval, then the victim stations will not have the chance to issue some new valid requests.

C. Miscellaneous Attacks

Other possible attacks have emerged during the analysis of the protocol, we briefly cite them in this subsection:

- A downgrade attack is possible on the initial TEK authentication. The security capabilities are sent by SS to BS over an insecure connection, before negotiating the encryption keys, these include the kind of crypto functions to be used to cipher the data packets. Since there is no authentication (neither *a posteriori*) an attacker could send a spoofed message containing weaker capabilities in order to convince the BS and the attacked SS to agree on an insecure crypto algorithm. Since the standard doesn't specify a correct behaviour for the BS upon reception of two valid answers for the same request, it is unclear how this race condition may be solved.
- In *IEEE 802.16e* SS can authenticate with BS with the new PKMv2 RSA authentication, in this new authentication type the BS has to sign the reply messages with its public key. Public key encryption and signature is a computationally heavy operation, so if flooded with false requests, the BS may be victim of a denial of service attack, using all its resources to evaluate digital signatures.
- In *IEEE 802.16e*, to support mobile limited resource devices, a power save mode is introduced. A SS can enter sleep mode and communicate it to the BS, that will buffer messages for the SS. The SS can set the sleep mode in the Bandwidth request and uplink sleep control messages that are not authenticated. The attacker can send the Bandwidth request and uplink sleep control

message with the identifier of victim SS and the BS will stop transmitting messages to that SS, so performing a denial of service attack. As a test, we performed this attack against an *IEEE 802.11* network (we observed the same security issues also on *IEEE 802.11* networks) and the result was of a lack of connectivity for the victim client.
- More management frames are sent in clear, unauthenticated, that could be used by an attacker to produce denial of service attacks, as an example, CMP-CLK messages, Auth Invalid messages or RNG-RSP messages can be used to desichronize clocks or to force the SS to repeat network entry or authentication.

V. Conclusions

IEEE 802.16 is an emerging standard for broadband wireless communications that is receiving a lot of attention from service provider and hardware producers as an alternative to wired broadband access or as an efficient wireless LAN medium. In this article we discussed some of the security features of the standard, and revealed some critical vulnerabilities that can be used by an attacker to achieve two goals:

- In mesh mode, an insider attacker can fool other nodes of the mesh to create man in the middle attacks, invade their privacy, or to let other nodes enter the network in an uncontrolled manner.
- In PMP mode any node can send faked resources requests with the aim of having the *base station* to allocate less resources for its neighbors.
- Various denial of service attacks and misuse of cryptographic functions have been identified.

As further developments of the standard some security policies are to be evaluated:

- Full integration of *IEEE 802.1X*, for PMP and mesh mode.
- Evaluation of secure handover strategies to substitute the *Neighbor Link Establishment*.
- Introduction of authentication for certain sensitive management messages, as it is planned for wifi with IEEE 802.11w [13].

References

[1] Institute of Electrical and Electronic Engineers, Inc., *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std., 2004.

[2] ——, *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*, IEEE Std., 2005.

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

[4] F. Yang, H. Zhou, L. Zhang, and J. Feng, "An improved security scheme in wman based on ieee standard 802.16," in *2005 International Conference on Wireless Communications, Networking and Mobile Computing*, 2005.

[5] S. Xu, M. M. Matthews, and C.-T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16," in *ACM Southeast Regional Conference*, R. Menezes, Ed. ACM, 2006, pp. 113–118. [Online]. Available: http://doi.acm.org/10.1145/1185448.1185474

[6] M. Barbeau, "Wimax/802.16 threat analysis," in *Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*. New York, NY, USA: ACM Press, 2005, pp. 8–15.

[7] Institute of Electrical and Electronic Engineers, Inc., *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Std., 2004.

[8] L. Maccari, R. Fantacci, T. Pecorella, and F. Frosali, "A secure and performant token-based authentication for infrastructure and mesh 802.1x networks," in *IEEE Conference on Computer Communications*, 2006.

[9] B. Aboba and L. Blunk, "Extensible authentication protocol (eap)," RFC 3748, 2004.

[10] C. Rigney and A. Rubens, "Remote authentication dial in user service (radius)," RFC 2138, 1997.

[11] V. L. Voydock and S. T. Kent, "Security mechanisms in a transport layer protocol," *Computer Networks*, vol. 8, pp. 433–450, 1984.

[12] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MOBICOM-01)*. New York: ACM Press, 2001, pp. 180–188.

[13] Ieee 802.11 task group w. [Online]. Available: http://grouper.ieee.org/groups/802/11/Reports/tgw_update.htm