Research Paper Engineering

Improving Mobile WiMAX EAP-TTLS Authentication with Minimum Downtime and Securing its Management Channel

Apostol Cristian-Gabriel — Electronic engineering and Telecommunications Department Military Technical Academy, Bucharest Romania

Ciprian Răcuciu — Computer Science Department, Titu Maiorescu University Bucharest, Romania

ABSTRACT

Increasing the level of security with minimum downtime in a wide area WiMAX network, with thousands of fixed and mobile subscribers will encounter practical problems. We refer mainly to increase authentication, protecting the management channel, the moment of changing AAA server policy, the x.509v3 digital certificates generation, the EAP.xml configuration and the CAs recognized by the network. Doing this with minimum downtime to the active services and with a limited number of system engineers is also a challenge. The approach presented in this paper is a solution for increasing the security level of a live geographically dispersed WiMAX network, independent from the vendor.

KEYWORDS authentication, management channel, EAP-TTLS, WiMAX, network security, x.509v3, minimum downtime.

1. Introduction

Nowadays for wireless networks, security represents a priority in order to assure protected communications. In IEEE 802.16, security has been considered as the main issue during the design of the protocol [1]. The Initial Network Entry procedure in an IEEE 802.16 (WiMAX) network has security defects which can be exploited by the Man-in-the-Middle (MITM) attack [2]. Improving network security in a live enterprise network with a large number of subscribers geographically dispersed should be done with minimum downtime, in order not to affect critical user data/voice services. Also the management channel should be strongly protected in order to prevent intrusion in the core network that contains all of the vital servers for network functionality.

Authentication is the validating process of a user identity and often includes validating which services a user may access and, typically involves a supplicant (that resides in the mobile station), an authenticator (that may reside in the base station or a gateway), and an authentication server [3]. EAP (Extensible Authentication Protocol) is a standard protocol (frequently used in wireless networks) for data transmission authentication, which is invoked by an 802.1X enabled NAS (Network Access Server) device such as an 802.11 a/b/g Wireless Access Point [4]. The EAP work group is developing algorithms of supporting many authentications like ID/Password, Certificates, SMART Card and methods of session key standardization using such authentication algorithms [5]. EAP (see figure 1) integrates different authentication methods (advised by IEEE) to match the nature of the communication channel, such as EAP-PKM, EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-SIM, EAP-AKA, and in addition a number of vendor specific methods and new proposals exist - commonly used methods capable of operating in wireless networks include EAP-TLS (Transport Layer Security), EAP-SIM (Subscriber Identity Module), EAP-AKA (Authentication and Key Agreement), PEAP (Protected Extensible Authentication Protocol), LEAP (Lightweight Extensible Authentication Protocol) and EAP-TTLS (Tunneled Transport Layer Security) [6].

Table 1. EAP Authentication Methods comparison

	EAP-TTLS	EAP-TLS	PEAP	LEAP	EAP-MD5
Mutual Authentication	Yes	Yes	Yes	Yes	Yes
Client Certificate	Optional	Yes	Optional	No	No
Server Certificate	Yes	Yes	Yes	No	No
Dynamic Key Exchange	Yes	Yes	Yes	Yes	No
Credential Integrity	Strong	Strong	Strong	Moderate	None
Client Identity Protection	Yes	No	Yes	No	No

EAP-TTLS supports dual authentication and represents a protocol that extends TLS. A secure TLS tunnel is established using the server digital certificate. The server can authenticate a client using a certificate or, if there is no certificate, using PAP/CHAP/MSCHAP v1, MSCHAP v2 or both phases of authentication, representing the strongest method. Phase 2 may still be required by setting a force-phase-2 parameter on the server, even if phase-1 digital certificate authentication has been successful. Over the established encrypted tunnel the client sends its username and password. For EAP-TTLS the second authentication method can be selected by the SS, but in PEAP the second authentication method is selected by the RADIUS server. The digital certificate authentication of network elements is an optional component of the Mobile WiMAX standard, and a security improvement.

2. Existing WiMAX network security

The WiMAX AAA Framework provides the following services [7]:

- Authentication Services - including device, user or combined device & user authentication;
- Authorization Services - including delivery of information to configure the session for access, mobility, QoS and other applications;
- Accounting Services - including delivery of information for the purpose of billing and information that can be used to audit session activity by both the home NSP and visited NSP.

For the initial network entry, the MS searches for a periodically broadcasted map message from the BS. This frame includes information about the connection identifier (CID) that is associated with a time slot where the initial ranging process can be carried. Access to this commonly used time slot

is defined as CSMA (Carrier Sense Multiple Access). The MS increases its transmission power until it receives a response from BS. The response includes ranging adjustments and the basic and primary management CIDs which reserve a particular time intervals for the MS to send and receive management messages [8]. After completing initial ranging, basic connection capabilities are negotiated, and after that the authentication procedure follows. Mobile WiMAX supports two types of authentication: EAP-based authentication or simple RSA-authentication. EAP-based authentication (see figure 2) can be considered more secure because it includes higher layer authentication. After the authentication process, the MS and the BS have a common authorization key (AK).

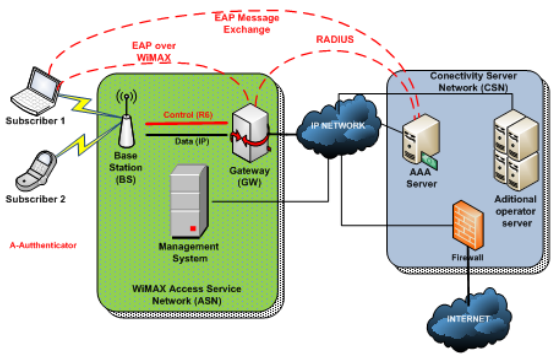

Figure 1: EAP Authentication

Derived from the AK is the key encryption key (KEK) which is used to secure future keys. Also derived from the AK are the keys used in the uplink (HMAC_Key_U) and downlink (HMAC_Key_D) message authentication [9]. After this for each data connection, the 3-way TEK-exchange is executed, obtaining the final keys which are used for data traffic encryption. The result is that the integrity of each message is protected using a MAC digest and the transferred traffic encryption key (TEK) is encrypted with the KEK. Each MS must register on the BS to be allowed to send and receive packets of data to the WiMAX based network. For managed MSs the registration process additionally sets up a secondary management CID which is needed to supervise and administer it.

Mobile WiMAX uses X.509, that is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI) and has been adopted by the Internet Engineering Task Force (IETF) as the PKI (see figure 3) for several IETF protocols [10]. As an integral part of the SSL and TLS protocol suites [11], X.509 certificates are, most often, used for server authentication in TLS/SSL, where the server presents its certificates to the client. Certificates are thus important for various protocols such as HTTPs, IMAPs, SMTPs and POP3s [12].

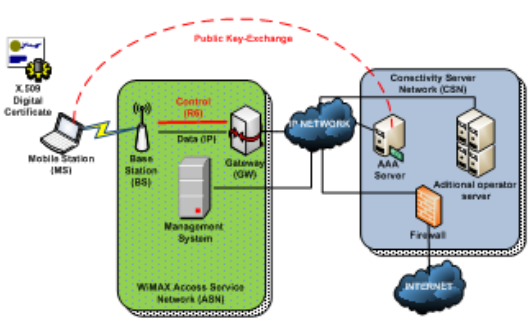

Figure 2: PKI in WiMAX

The 802.16 standard states that 802.16-compliant SSs must use X.509 Version 3 certificate formats, providing a public key infrastructure used for secure authentication. Each SS carries a unique X.509 digital certificate issued by the SS manufacturer, known as the SS X.509 certificate. More exactly, this certificate is issued (and signed) by a Certification Authority (CA) and installed by the manufacturer. This digital certificate contains the SS RSA public key and the SS MAC address. Each SS has a manufacturer-issued X.509 manufacturer CA certificate issued by the manufacturer or by an external authority. The manufacturer's public key is then placed in this X.509 manufacturer CA certificate, which in turn is signed by a higher-level CA. This higher level CA does not seem to be clearly defined in the present version of the standard. There are then two types of X.509 certificates: SS X.509 certificates and the X.509 manufacturer CA certificate. In the 802.16-2004 standards, there is an X.509 certificate for the BS [9].

The WiMAX standard specifies the following security services: user/device authentication and data confidentiality. Authentication consists in verifying the identity claimed by a WiMAX SS/Server.

Confidentiality refers to protecting the WiMAX data messages so that only the authorized devices can decrypt them. The two standards, IEEE 802.16e-2005 known as Fixed WiMAX and the IEEE 802.16-2009 known as Mobile WiMAX have the same authentication and confidentiality mechanisms; they both support user authentication and device authentication. The security mechanisms for fixed network are defined by the security sub-layer of the IEEE 802.16d [13] standard and the security mechanisms for mobile network are defined by the security sub-layer of IEEE 802.16e [14] standard. The security sub-layer functions are to: (i) authenticate the user when the user tries to access the network, (ii) authorize the user, if the user is provisioned by the network service provider, and then (iii) provide the necessary encryption support for the key transfer and data traffic [15]. The security association (SA) is a shared set of parameters between the BS and MS/SS, similar in concept with IPsec, and it contains the algorithms and keys used in encryption [16]: x.509 certificates, authorization key (AK), key encryption key (KEK), message authentication keys, authorized data SA list, SA identifier, traffic encryption key (TEK), data encryption SA type indicator, group traffic encryption key (GTEK), group key encryption key (GKEK). X.509 digital certificates allow the system components of WiMAX to validate one another, and contain the public keys of the devices.

The authorization key provided during SS authorization is one of many types of keys used in 802.16 securities – the standard dictates use of the following keys [17]:

- Authorization Key (AK). Encrypted using the RSA public key scheme with the SS's public key in its X.509 certificate, this key is granted during initial SS authorization and is refreshed at the end of its lifetime as specified in the SA parameters.
- Key Encryption Key (KEK). Derived from the authorization key by the BS, this key is used to encrypt the traffic encryption key when it is transmitted to the SS.
- Traffic Encryption Key (TEK). Encrypted with the key encryption key, this key is used as the key to the encryption mechanism that will be used to secure the actual payload traffic between the SS and BS and vice-versa.

The BS uses the authorization protocol to authenticate and authorize network access to an SS - the protocol consists of three messages [18]:

- The first is an optional authentication information message, in which an SS sends its manufacturer's X.509 certificate to the BS.
- The second is an authorization request (Auth-REQ), in which the SS sends its certificate and information about its capabilities to the BS.
- The third message is an authorization response (Auth-RSP), in which the BS validates the requesting SS's identity, determines the encryption algorithms and protocols to share with the SS, generates an AK (authorization key), and sends it to the SS.

3. Improving WIMAX authentication and protecting the management channel

As we can see from the theoretical presentation in part two of the paper, the traffic encryption key (TEK) is derived from the authorization key (AK). This means that two security mechanisms, encryption and authentication, are strongly based on one another, thus concluding that strong authentication means strong encryption of WiMAX traffic.

Improving network authentication from the credential based MSCHAPv2 method included in EAP-TTLS to the optional digital certificates authentication, or even more robust the idea of using both types combined has to be done with minimum downtime. This involves taking into account different problems like the time needed to generate/upload digital certificates to the subscribers, to the AAA security server and to the other core servers like ASN, ASN-GW and NMS. It is important to note that changing the access policy on the AAA server requires a RADIUS restart. This restart stops all authentications that take place in the WiMAX Network at that time, but does not interrupt data and voice traffic. Choosing the time when the subscribers have minimum traffic rates is very important, and has to be done after a serious traffic peak and importance analysis.

It is also important to verify the eligibility of a user that wants to access the network, so this is why this method represents a practical approach. One of the strong points that we are trying to prove is that the certificates are not on a fixed time schedule until the AAA policy has to be changed to always require client certificates and vice versa. They can be done in a certain period of time agreed by the management of the telecommunications company provider.

The step by step process, for increasing authentication is described in figure 4.

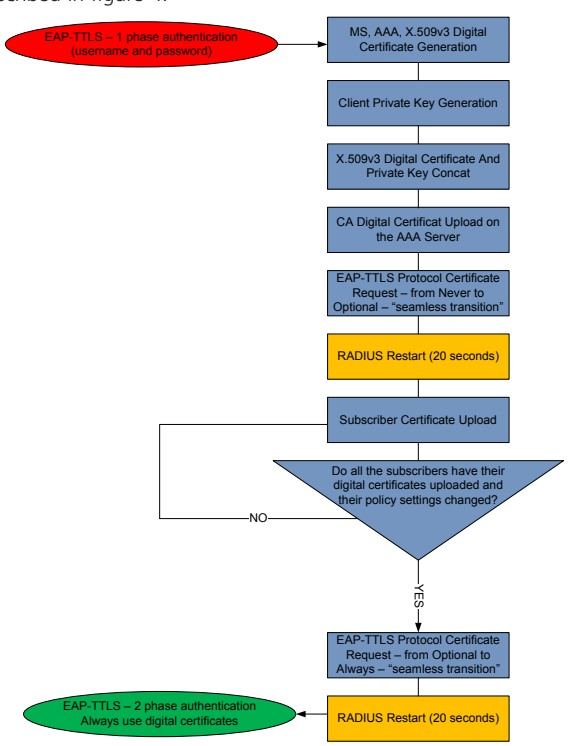

Figure 4: The proposed method for increasing security with digital certificates over credential based EAP-TTLS WiMAX Network

The software present on the terminal stations, depending on the vendor usually has a separate zone to upload the private key. There are some types of WiMAX terminals that accept only the digital certificates. In this case the practical solution for this problem is to upload the digital certificate and the private key in the same memory field, by concatenating them, but securing the private key with a chosen password.

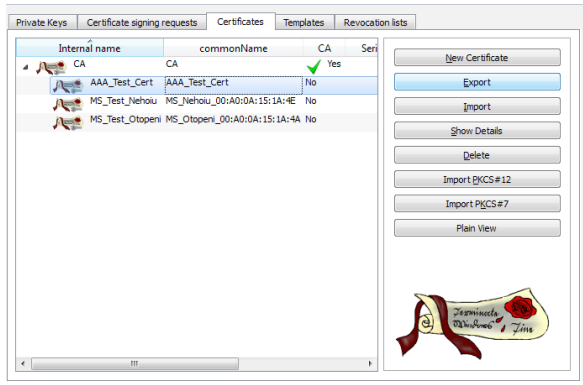

Figure 5: Simulated certificate client/server/CA database

The client certificates have to be signed by the same CA. The private key of the CA, used in the testing is type RSA with a key size of 2048 bits. End-entity certificate type should be chosen for MS and the valid period for the digital certificates chosen for this application is 2 years, but the valid period of the certificates can be customized depending on the security requirement of the network.

A client certificate has been generated in 1-2 minutes. Depending on the scale of the network, this process is directly proportional with the number of mobile/fixed subscribers. By changing the validation of these security certificates to optional, by coding the EAP method on the AAA server, the process can be done step by step with maximum attention for every user.

The practical generation of digital certificates can be done with Open SSL or with XCA, which are free online downloadable applications. In figure 4 it can be seen that the x.509v3 certificates for all the system components are issued by the same CA, generated on a workstation in the core network with the following attributes: Intel Core i5, 2.5 GHz processor, 4GB RAM Memory, 32-bit Windows 7 operating system.

The private key (see figure 5 and 6) can be used for digital signing, key encipherment and data encipherment. After their generation, the digital certificates and the private keys have to be exported from the local PKI Infrastructure and uploaded in the WiMAX network.

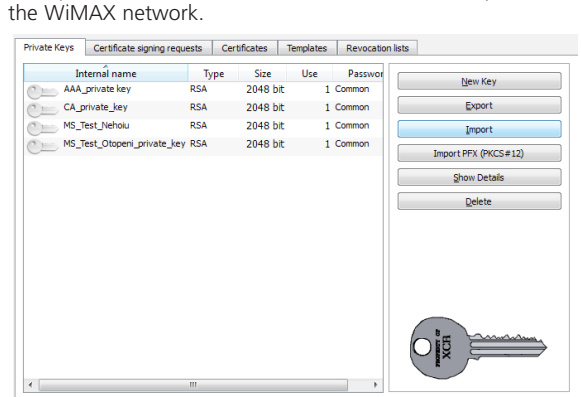

Figure 6: Private keys of the CA, AAA server, and the subscribers used in testing, corresponding to their digital certificates

Testing and experiments have shown that the digital certificates can be in the PEM (privacy enhancement mail) format or in the CRT (certificate) format. From this point all subscribers will be authenticated in 2 steps: digital certificates and authentication credentials generated on the AAA Server. Thus achieving an upgrade in the overall security of the network by

robust authentication, independent indoor digital certificate generation, thus reducing costs near to zero for this upgrade, minimum downtime achieved – between 40 seconds and 1 minute.

In this time, the services are not stopped. The limited downtime is for the subscribers that are trying to reauthentcate in this period of time. For our test network it is set at 72 hours, and during this period 3 out of 3320 subscribers had to wait between 40 seconds and 1 minute in order to be reauthenticated, untill the RADIUS server had restarted. Thus achieving a downtime result of 40 seconds to 1 minute for less of 0.1% of the network users.

```
<eap-ttls>
    tls-setting REQUIRED
        Reference to the setting-name of a tls-setting element.
    session-resumption-timeout CDATA "0"
        Stores the session resumption timeout value, in seconds. It shall have a range
        of values between 0 - 86,400 seconds (1 day)
    authentication-policy CDATA #IMPLIED
        Optional identifier for the name of a policy file, to determine whether the
        client authentication shall occur locally or remotely.
    force-phase-2 OPTIONAL (default = 'N')
        Forces phase 2 authentication to proceed even if a client certificate was
        presented and successfully verified during phase 1. Use require-client-
        certificate=y in conjunction with this parameter to force authentications
        during both phase 1 and phase 2.
        'N' => If client certificate is received, phase 2 will not proceed.|
               If client certificate is not received, phase 2 will proceed.
        'Y' => If client certificate is received, phase 2 will proceed.
               If client certificate is not received, phase 2 will proceed.
</eap-ttls>
```

Figure 7: The authentication code uploaded in the AAA server for eap-ttls optional certificate authentication

The force phase 2 parameter is changed to "optional" when migrating from credential-based authentication in RADIUS to digital certificates authentication. It will function this way untill the engineers upload digital certificates on all of the subscribers, and set them to authenticate the server also, thus achieving mutual authentication that is considered in [3] as robust against Man-in-the-middle attacks.

After all the subscribers have been programmed and uploaded with digital certificates that have been generated from the CA, the force phase 2 parameter is set to "always". This means that from this moment all the certificates are going to be required from the clients, and the users will have to possess, in a mandatory way from the AAA server, a valid digital certificate in order to acces the WiMAX network. In this manner we achieve mutual authentication between the user-terminals and the network, enforcing security against possible man-in-the-middle attacks.

Management in WiMAX is done via a management VLAN ID in ETH-CS and from the AAA and ASN-GW in IP-CS. For the first part we will describe our approach on securing ETH-CS management, and using the same principles we will present the method for securing IP-CS management.

In order for this channel to be protected, it is important to program the subscriber station in such a way so that the management VLAN is stopped in the WiMAX terminal equipment and not bridged in the local area network connected to it. When selecting a certain management VLAN tag, this network has to be inaccessible from the LAN of the terminal.

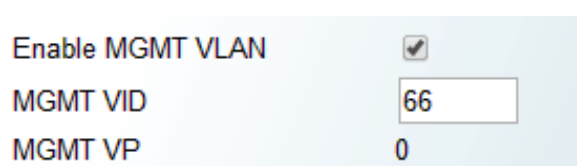

Figure 8: Stoping the management VLAN in the terminal equipment

Another principle that can be applied to protect the management channel is the filtering of the MAC address that can access the core network via the management channel. These equipments should be only the WiMAX terminals. The proposed idea is to allow only the WiMAX terminal to access the base station via the management channel for network updates, and no other equipment connected to it. In this way, even if a local third party manages to enter the management VLAN, it will not be granted service by the base station because it's physical address is not in it's database.

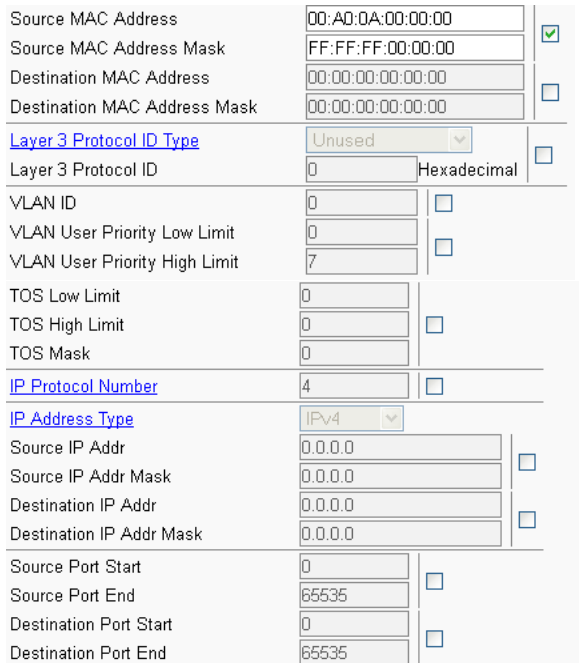

Figure 9: Proposed SS parameters for L2 and L3 rules for the management protection

For Layer 2 subscribers, that can assure network services via VLAN, we propose to set the source MAC address to correspond to the physical address of the WiMAX device that can access the network's management. The Source MAC address mask in this case should be set to FF:FF:FF:FF:FF:FF, in order to let only this subscriber to access the core, and no other similar MAC.

If the network has only devices from a certain manufacturer, the source can be set with the first three groups of the MAC that represent the company that produces the equipments. In this case only the terminals produced by a certain company can access the network, but this represents a lower level of protection.

In case of the terminals that operate in the Layer 3 mode, in a similar way we will set the Source IP Address of the terminal that is approved for management in the network, and the destination of the Core gateway that will allow its connection.

4. CONCLUSIONS

Improving the network security with minimum downtime is a priority in todays and future perspectives. This involves solving different problems like the time needed to upload digital certificates to the subscribers and to the server; this has to be done in a seamless way for the services that are running, with minimum interruption. The first part of the paper discusses the improvement of EAP-TTLS authentication based only on MSCHAPv2, to the authentication using both methods based x.509v3 digital certificates and the existing credential based authentication, in a mandatory way for the fulfillment of both checks by the AAA server.

The RADIUS restart stops all authentications that take place at that moment in the WiMAX Network, but does not interrupt traffic between network entities. The RADIUS restart for a Mobile WiMAX network should be done at night, when subscriber traffic is at minimum rates. Choosing the time when the subscribers have minimum traffic rates is very important, and has to be done by network statistics and by traffic importance.

The paper shows that the security increase can be done inside the organization, with minimum costs, thus independent from the vendor, and with secrecy because only the system engi-

neers of the institution know and chose the parameters of the digital certificates, the private keys and the AAA security policy. The method proposed discusses minimum downtime and achieving security in a live WiMAX Network with 0.1% of the users having actual downtime for maximum 40 seconds to 1 minute.

A client certificate has been generated in 1-2 minutes manually, but this process can be done automatically. Depending on the scale of the network, the time needed for this process is directly proportional with the number of mobile/fixed subscribers. Changing the validation of these security certificates to optional, by coding the EAP method on the AAA server, the process can be done step by step with maximum attention for every group of user, and only after that, the network engineers can set the digital certificates check to mandatory. The security policy is changed after all of the subscribers have been dealt with.

The paper also discusses protection of the management channel that is linked to the core network. An attack here can have critical consequences to the network, and this is why we take into account its security. After a primary authentication of the user terminal, two more security mechanisms are implemented to enforce the robustness of this virtual network by applying a VLAN tag stop in the terminal and by filtering the MAC addresses of the equipment's by the Base Station, so that no unauthorized third party has access.

The paper also discusses the protection of the management channel in both cases of subscriber functionality, Ethernet Convergence Sub-layer and IP Convergence Sub-layer. Even if filtering of the IP parameters are not strong for robustness used as a standalone principle, combining this theory with strong device authentication via full EAP-TTLS can assure a higher level of security for subscribers and for the core network protection. Testing has shown that no other terminals than the ones with the specified parameters and digital certificates are allowed to access the network.

The proposed method represents a contribution on improving WiMAX security with a limited number of engineers, small downtime and with no cost on behalf of the network operator or to the clients. The paper also takes into account the security of the management's virtual network, for both IP-CS and ETH-CS subscriber functionalities and proposes a practical security increase of the two operating modes.

REFERENCES

[1] Z. You, X. Xie and W. Zheng, "Verification and research of a Wimax authentication protocol based on SSM", Education Technology and Computer (ICETC), 2nd International Conference on, Shanghai, vol. 5, pp. 234-238, 2010. | [2] B. N. Komu, M. Mzyece and K. Djouani, "SPIN-Based Verification of Authentication Protocols in WiMAX Networks", Vehicular Technology Conference (VTC Fall), Quebec City, pp. 1-5, 2012. | [3] M. Bogdanoski, P. Latkoski, A. Risteski and B. Popovski, "IEEE 802.16 Security Issues: A Survey", 16th Telecommunications Forum - TELFOR, Belgrade, pp. 199-202, 2008. | [4] L. Blunk and J. Vollbrecht., PPP Extensible Authentication Protocol (EAP). IETF RFC 2284, Mar. 1998. | [5] H. Hwang, G. Jung, K. Sohn and S. Park, "A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP", Proc. Int'l Conf. Inf. Systems Security, Seul, Korea, pp. 164-170, 2008. | [6] S. Adibi, L. Bin, H. Pin-Han, G. B. Agnew and S. Erfani, "Authentication Authorization and Accounting (AAA) Schemes in WiMAX", IEEE International Conference on Electro/information Technology, East Lansing, MI, pp. 210-215 , 2006. | [7] S. M. Rosu and G. Dragoi, "Virtual Enterprise Network Solutions and Monitoring as Support for Geographically Dispersed Business", Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions, chapter 3, M.M. Cruz-Cunha et al. (Eds.), IGI Global, Hershey, PA, USA, pp. 34-62, 2012. | [8] A. Deininger, S. Kiyomoto, J. Kurihara and T. Tanaka, "Security Vulnerabilities and Solutions in Mobile WiMAX", IJCSNS International Journal of Computer Science and Network Security, vol. 7, no. 11, pp. 7-15, 2007. | [9] L. Nuaymi, WiMAX Technology for Broadband Wireless Access. John Wiley & Sons Ltd, 2007. | [10] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," RFC 5280 (Proposed Standard), May 2008. | [11] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol version 1.2," RFC 5246 (Proposed Standard), Aug. 2008, updated by RFCs 5746, 5878, 6176. | [12] R. Holz, L. Braun , N. Kammenhuber and G. Carle, "The SSL landscape: a thorough analysis of the x.509 PKI using active and passive measurements", Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, Berlin, pp. 427-444, 2011. | [13] IEEE 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed Broadband Wireless Access Systems", IEEE Press, 2004. | [14] IEEE 802.16-2005, "IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE Press, 2005. | [15] P. Rengaraju, L. Chung-Horng, Q. Yi and A. Srinivasan, "Analysis on mobile WiMAX security", IEEE TIC-STH 2009, Information Assurance in Security and Privacy, Toronto, 2009. | [16] K. Scarfone, C. Tibbs and M. Sexton, "Guide to securing WiMAX wireless communications", National Institute of Standards and Technology Special Publication, pp. 800–127, 2010. | [17] R. Dantu, G. Clothier and A. Atri, "EAP methods for wireless networks", Computer Standard and Interfaces, vol. 29, pp. 289-301, 2007. | [18] C. T. Huang and J. M. Chang, "Responding to Security Issues in WiMAX Networks", IT Professional, vol. 10, issue 5, pp.15 -21, 2008. |