International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 3 (2013), pp. 189-194

http://www. irphouse.com /ijict.htm

Security Issues in WiMAX: A Critical Review

Saurabh Dubey[1] and Sachin Kumar[2]

[1]School of Information and Communication Technology, Gautam Buddha University, Greater Noida -201308, India.
[2]School of Information and Communication Technology, Gautam Buddha University, Greater Noida -201308, India.

Abstract

WiMAX (World Wide Interoperability for Microwave Access) IEEE 802.16, WiMAX is the emerging technology of this generation. WiMax uses radio channel, which are open channel that's why security problem arises. In WiMAX air is used as a medium which connect Physical layer to MAC layer. Here is large probability of data getting destroyed by unauthorized users. In this paper we will have a detailed discussion on different security issues in WiMAX.

1. Introduction

WiMAX (Worldwide Interoperability for Microwave Access)IEEE802.16 is a technology which provide the facility of wireless broadband access with the high speed data rates across whole cities or countries. As the use of Wimax has increased the problem of security has also increased. The meaning of security in communication is how to save our data by the attackers and the main challenge is privacy, WiMax istransmitted from line of sight (LOS) and point to multipoint (PMP) with higher frequency (10-66GHz) and lower frequency (2-11GHz). WiMax uses air as a medium for the purpose of data transmission[1]. Since air is an open channel that's why there is large probability of the information getting affected by the attacker. For the transmission air is used as a medium which connect physical layer to MAC layer since it use air as a medium so there is large range for the attacker to move and affect the information.

2. Security Architecture

2.1 WiMax Protocol Structure

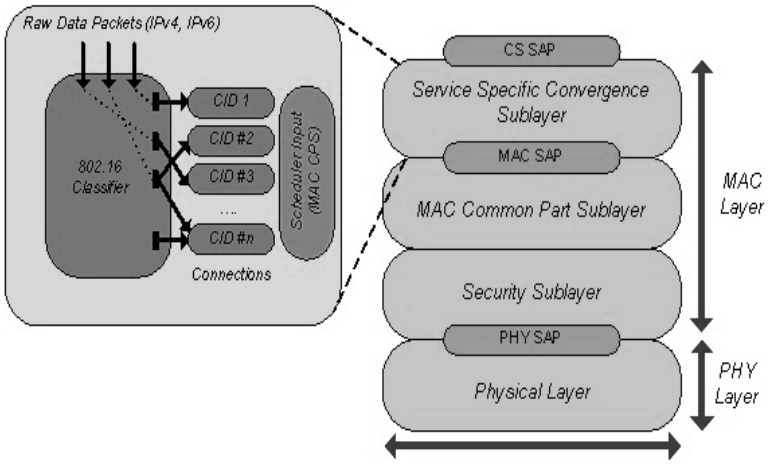
WiMAX protocol stacks have two layers. These are MAC layer & PHY layer. MAC layer is sub divided into three parts, namely Service specific convergence sub layer, MAC common part sub layer & Security sub layer. These are shown in fig. (1)

1-Service Specific Convergence Sub layer

This layer is used for mapping higher level data service to MAC layer service [1].

2- MAC common part sub layer

The common part sub layer (CPS) resides in the middle of MAC layer. It represents the core of MAC protocol and is responsible for bandwidth allocation, connection establishment & maintenance of the connection between two sides.



IEEE802.16 Protocol Stack

Fig. 1: Protocol of WiMAX.

3 Security Sub Layer

The security sub layer provides authentication, secure key exchange, encryption across the system.

2.2 Security Scheme of WiMAX

WiMAX security level is define in three parts these are [2] shown in fig. (2).

01. Authentication
02. Authorization
03. Data Encryption.

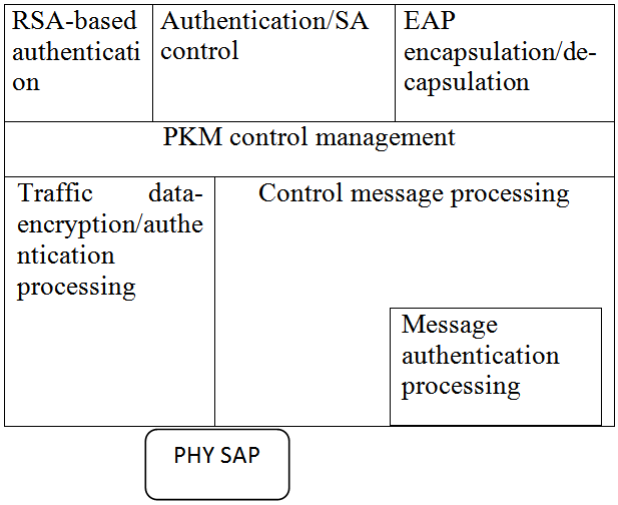


Fig. 2: WiMAX Security level.

1. Authentication

The first level of security authentication is MAC authentication & WiMAX support this. Authentication is done by Public Key Interchange Protocol. It ensures the establishment of encryption key. WiMAX defines the Privacy Key Management (PKM) protocol in security sub layer. It permits three type of authentication. One of them is based on RSA, it use the X.509 certificate with RSA encryption, X.509 certificate basically finds the identity of Base Station (BS)with the help of Subscriber Station (SS) [3], which is shown in fig.(3)

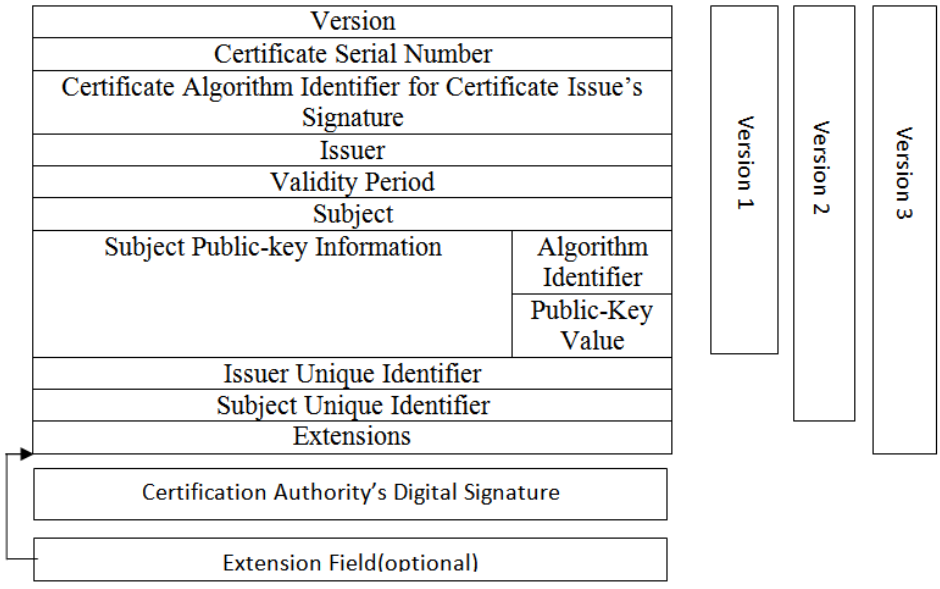


Fig. 3: X.509 certificate.

2. Authorization
AK & security access are requested by SS, the authorization request message SS's X.509 certificate, encryption algorithms & cryptographic ID. The network BS interacts with AAA(Authentication, authorization& accounting) server to carry out necessary validation & send back an authorization reply that contains the AK encrypted with the SS's public key, a lifetime key and an SAID.

3. Encryption
Data traffic is encrypted by the Traffic Encryption Key (TEK)[4].

Privacy Key Management
For the normal authorization of the SS, periodic re-authorization and reception/renewal of key material the privacy key management protocol is responsible. The PKM protocol is comparable to client/server model where the SS request key material form base station. Which work as PKM server[5].

3. Vulnerabilities

3.1 Physical layer Threats

In WiMAX there are only 2 types of threats in physical layer.

- Jamming arises by introducing a strong noise to reduce the capacity of the channel, it may be unintentional or malicious [6].Resilience jamming can be increased by increasing the power or bandwidth of the signal. It is fairly easy to detect & address.
- Scrambling is a sort of jamming but for short interval of time & target is specific WiMAX frames [6]. Scrambler can reduce the effective bandwidth of the victims& increase the processing of own data by selectivescrambling.

3.2 MAC Layer Threats

MAC layer is connection oriented. There are two types of connections. These are Management connection & data transport connection.Management connections are divided into three types:

1. Basic connection

When MS joints the network, a basic connection is created used for short & urgent management message.

2. Primary connection

At the time of network entry, a primary connection is created for MS. It is used for delay tolerant management message.

3. Secondary connection

It is used for IP encapsulation management message.(E.g. DHCP, SNMP, TFP).Security parameter of a connection is captured by security association (SA), security association is of three type primary, static & dynamic all these have their own SAID's which contain information like cryptographic suite identifier, TEK's &

initialization vector. There is one primary SA for each MS.Maximum part are the X.509 certificate, TEK, AK & the HMAC key. The MS already have X.509, it contains the PK of MS. PK is basically used for authentication of MS with the BS. Requirement of remaining keys are fulfilled during the process of authorization[1][7].

4. Security Requirments

The biggest security issues in WiMAX areprivacy & access control to the network. The issue of privacy is resolve by encrypting the connection in between BS & SS. For the access control purpose a keying protocol is used by the base station.

5. Conclusion

In this paper, we provided a review on security issues in WiMAX / IEEE 802.16(wireless broadband network). As the use of WiMAX will increase the problem regarding the security is also going to increase. Here we have discussed the different threats layers.

References

[1] Syed Shabih Hasan, Mohammed Abdul Qadeer, “Security concerns in WiMAX”, International Conference on Digital Object Identifier, 2009.

[2] Muhammad Sakibur Rahman, Mir Md. Saki Kowsar, “WiMAX security analysis and enhancement”, 12th International Conference on Digital Object Identifier, 2009.

[3] Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, Yuan'an Liu, “Analysis of Mobile WiMAX Security”,Mobile Ad Hoc and Sensor Systems, 2008.MASS 2008. 5th IEEE International Conference on Digital Object Identifier,2008.

[4] Lang Wei-min, Wu Rung-shen, Wang, Jian-qiu, “A Simple Key Management Scheme Bsaed on WiMAX”, International Symposium on Computer Science and Computational Technology, 2008.

[5] Eren, Erven“WiMAX Security Architecture – analysis and assessment”, Intelligent Data Acquisition and advanced Computing System; technology and Application,4th IEEE Workshop on Digital Object Identifier,2007.

[6] Hu, Dong ; Wang, YuYan, “Security Research on WiMAX with Neural Cryptography”,Information Security and Assurance,Internationa lConference on Digital Object Identifier,2008.

[7] Michel Barbeau, “WiMax/802.16 Threat analysis”, Carleton University, 2005.