ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering &Technology (IJARCET)
Volume 2, Issue 8, August 2013

A performance evaluation of various security assessments in WiMAX

Pankaj chouhan[1] & S.R. Mansore[2]

***ABSTRACT*- One of the technologies that can lay the foundation for the next generation (fourth generation [4G]) of mobile broadband networks is popularly known as WiMAX. WiMAX stands for worldwide interoperability for microwave access belongs to IEEE 802.16 standard family. WiMAX has many salient advantages over such as: high data rates, quality of service, scalability, security, and mobility. With the growing popularity of WiMAX security risk have increased in many folds. In this paper we study the WiMAX security architecture, physical Layer Threats, MAC Layer Threats, authentication, authorization and rough base station in WiMAX.**

***Keywords* - IEEE 802.16, WiMAX, wireless network, physical and MAC layer threats, security architecture, authentication, authorization.**

I. INTRODUCTION

WiMAX (Worldwide Inter-operability for Microwave Access) is designed to deliver next generation high speed mobile voice and data services and wireless “last mile” broadband services, backhaul connections that could potentially displace a great deal of existing radio air network (RAN) infrastructure. WiMAX can offer a large wireless access network footprint to subscribers (similar to data-enabled cellular services such as UMTS/CDMA), while at the same time providing higher throughputs that are similar to WLAN networks. WiMAX is an ideal access network for next-generation converged voice and data services and streaming wireless multimedia. [1]

The IEEE 802.16 standard was originally meant to specify a fixed wireless broadband access technique for point-to-point and point-to-multi point links. During its development, however, it was decided that mobility support should also be considered. WiMAX is the emerging broadband wireless technologies based on IEEE 802.16 standards. The security sub-layer of the IEEE 802.16d standard defines the security mechanism for fixed and the IEEE 802.16e standard defines the security mechanism for mobile networks. The security sub-layer supports are to: (1) authenticate the user when the users enter in to the network, (2) authorize the user if the user provisioned by the network service provider, and then (3) provide the necessary encryption support for the key transfer and data traffic.[2]

Mobile WiMAX adds significant enhancement. [3]

- It improves NLOS coverage by utilizing advance antenna diversity schemes and hybrid automatic repeat request (HARQ).
- It adopts dense sub channelizing, thus increasing system gain and improving indoor penetration.
- It use adaptive antenna system (AAS) and multiple input multiple output (MIMO) technologies to improve coverage
- It introduces a downlink sub-channelization scheme, enabling better coverage and capacity tradeoff.

II. WIMAX SECURITY

The WIMAX 802.16 provided architecture is classified into two main layers- first one is Medium Access Control (MAC) layer and second one is physical layer, as shown in figure. The figure presents the interfacing points where Service Access Point (SAPs) is formally defined by the standard. Common Part Sub-Layer is the central element of the layered architecture. In this layer, MAC Protocol Data Units (PDUs) construction, connections, establishment and bandwidth managing is done. The common part exchanges the MAC Service Data Units (SDUs) to the convergence layer. The security sub layer introduces the authentication, establishment of keys and encryption. The security sub-layer exchanges the MAC PDUs to the physical layer. Here we discuss the security threats at the physical layer and the MAC layer.

Service Specific Convergence Sub-layer	MAC Layer
MAC Common Part Sub-layer	
Security Sub-layer	
Physical Sub-layer	PHY Layer

Fig 1 Protocol Layer Architecture

- Physical Layer Threats:- At the physical layer, the flow of the bits is represented in equal length frame as shown in figure, which have two sub frame (A) downlink sub-frame & (B) an uplink sub-frame and have two operation modes (A) Frequency Division Duplex (FDD) & (B) Time Division Duplex (TDD).

  A downlink sub-frame consists of two main parts: The first part has control information and the second part has data. A Mobile Station (MS) receives only the bursts. WIMAX 802.16 is vulnerable to physical layer attacks like as jamming which is an example of interruption attack, is enough to reduce the channel capacity is produced by introducing a source of strong noise. Jammed segments of the bandwidth may also be ignored in a spread spectrum scheme and can be detected.
- MAC Layer Threats: - The MAC layer is basically based on connection oriented concept. Two types of connection are used, (A) management connection (B) data transport connections. We can classify management connections in to three types, basic, primary and secondary. A basic connection is developed for each Mobile Station when it connects the network. For short and urgent management messages, it is used. The primary connection is used for each Mobile Station at the network entry time, but it is used for delay tolerant management message. The secondary connection is used for IP encapsulated management message. A Security Association (SA) is a concept capturing the parameters of security. Table shows the five classes of attacks and their solution below.

Table 1 Five Class of Attack

Attack	On	Solved By
Interception	Confidentiality and Privacy	Encryption /Decryption
Fabrication	Authenticity	Authentication
Modification Replay Reaction	Integrity	Digital signatures on every Message.
Interruption	Availability	No effective solutions exist for interruption / Denial of Service attacks on availability.
Repudiation	No repudiation	Non-repudiation currently still suffers of cases of identity theft.

III. SECURITY ARCHITECTURE

The security sub layer performs three main functions: authentication, authorization and encryption. The security sub layer has two main component protocols. A data encapsulation protocol for securing packet data across fixed BWA network. A key management protocol (PKM) providing the secure distribution of keying data from the BS to the SS. The architecture of security sub layer is shown in figure 2.

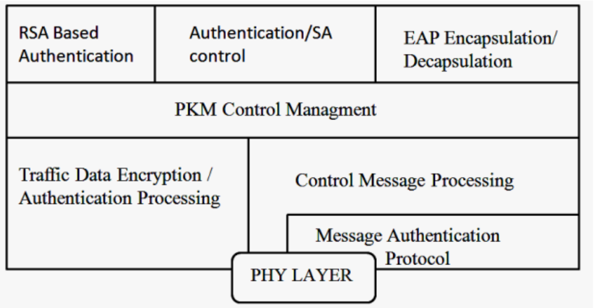
RSA Based Authentication
Authentication/SA control
EAP Encapsulation/ Decapsulation
PKM Control Managment
Traffic Data Encryption / Authentication Processing
Control Message Processing
Message Authentication Protocol
PHY LAYER

Fig 2 WiMAX Security Architecture

The main components of security architecture of IEEE 802.16 are as follows:

- Security associations: - a context to maintain the security state relevant to a connection between a base station (BS) and a subscriber station (SS).
- Certificate profile: - X.509 is used to identify communicating parties. These certificates are used by base station to identify the of subscriber stations.
- RSA authentication: - This protocol is based on X.509 certificates.
- EAP authentication: - The EAP uses particular kinds of credential (subscriber identity module, password, token-based, X.509 certificate or other) depending on the EAP method implemented.
- HMAC/CMAC authentication: - The 802.16 standard security includes the use of a Hashed message authentication and integrity control. IEEE 802.16e added the possibility of using CMAC as an alternative to HMAC.
- PKM authorization: - An authorization protocol to distribute an authorization token to an authorized SS.
- Privacy and key management: - A protocol to rekey the SA. Once authorized to the network, the SS can now establish a data SA between it and the BS, for that it again uses the PKM protocol.
- Encryption: - A payload field encryption using DSE-CBC in 802.16d, DSE-CBC and AES-CCM in 802.16e.

IV. SECURITY REQUIREMENTS

All computer system and communication channels face security threats that can compromise system, the services provided by the system, and/or the data stored on or transmitted between system. Well designed security architecture for a WiMAX and other wireless communication networks should support the following essential requirements:
:

- Privacy: - Provide protection from eavesdropping as the user data traverses the network from source to destination.
- Data integrity: - Ensure that user data and control/management message are protected from being tampered with while in transit.
- Authentication: - Have a mechanism to ensure that given user/device is the one it claims to be. Conversely, the user/device should also be able to verify the authenticity of the network that it is connecting to. Together, referred to as mutual authentication.
- Authorization: - Have a mechanism in place to verify that a given user is authorized to receive a particular service.
- Access control: - Ensure that only authorized users are allowed to get access to the offered services.

The main architectural components of a WiMAX network, including: -

- WiMAX Mobility Subscriber Station**:** - Mobile subscribers (MS) use mobile subscriber stations (MSS) generalized mobile equipment that provides connectivity between subscriber equipment and base station equipment.

- WiMAX Access Service Network**: -** Access Service Network (ASN) is defined as a complete set of network functions that provide radio access to a WiMAX subscriber, including a proxy AAA server, DHCP addressing function, and other IP-based resources, including network management.
- WiMAX Connectivity Service Network**: -** Connectivity Service Network (CSN) is defined as a set of network functions that provide IP connectivity services to the WiMAX subscribers through the ASN.

Table 2- Example of WiMAX Threats and Countermeasures

Layers	**Threats**	**Countermeasures**	**Examples/comments**
Application	Worms, Trojans, Viruses	Antivirus, FW, IDP	Voice, instant messaging, email, enterprise network access, custom application, video, Web browsing, etc.
Service	SIP (Session Initiation Protocol), E-mail Denial of Service, DNS Attacks	DMZ,FW,SEL, Policy	SIP,SMPT/POP,HTTP, etc.
Infrastructure	EAP Throttling, Spoofing, DoS	EAP MAX Session Counter, Security Association, Secure Perimeter, FW, IDP	Air interface and mobile core network interface caring end-user data
	Flooding MS, RF Flooding	Over-the-air Encryptions, SSL VPN Tunneling	

Below are two primary issues for planning security of WiMAX network integration:

- AAA traffic: **-** To allow secure exchange of security, authorization and accounting material, an appropriate security and trust relationship should exist between the 3GPP AAA server and the WiMAX access network.
- Data Traffic: **-** appropriate security devices and tunnels should be deployed between the WiMAX access network and 3GPP gateway located on the border of 3GPP PS.

V. WIMAX SECURITY REFERENCE ARCHITECTURE

WiMAX security reference architecture provides a comprehensive view of vulnerabilities, identified threats and mitigations. This security reference architecture is the result of through security analysis of the WiMAX network environment, including:

- A security risk assessment from an operation network and customer requirement perspective
- Comprehensive WiMAX threat identification and analysis
- The impact of vulnerabilities within the network environment
- Suggested mitigations and recommendations for network design, network devices, procedures, policies, and related human factor issues.

The MSS WiMAX Security Reference Architecture is a unique guideline foe network service provider that are planning countermeasure and security enhancements to mitigate /reduce threats to an acceptable risk level. At key points in the WiMAX network, appropriate security controls are selected based on defense-in-depth layering along with people, process, policies and technology enforcement.

The architecture analyses WiMAX threat and protections using these logical and functional networks areas.

- WiMAX user plan: **-** The end user security plane address security of access and use of the service provider network by customers, including actual and user data flows.

- WiMAX Control/signaling/plane:- the signaling and control data across WiMAX networks are transferred by ASN gateway, BTS, FA/ROUTER, switches and AAA using protocols according to the type of signaling messages and networks elements involved.
- WiMAX management plane (Operation, Administration, Maintenance and Provisioning OAM&P):- This plane address security of management data across the WiMAX network and the elements that perform OAM&P, such as network management systems and network elements that have visibility on the management plane, radius server, base station, routers and etc.

VI. ROUGH BASE STATION IN WIMAX

The rough BS (base station) makes the SS (subscriber station) believing that they are connected to the legitimate BS, thus it can intercept SS's whole information. SS can be compromised by a forget BS which imitates a legitimate BS. They are also known as masquerade attack in which one system assumes the identity of another. A rough BS is a malicious station that impersonates or duplicates legitimate base station. The rough base station puzzles a set of subscribers who try to get service which they believe to be a legitimate base station. The attacker generates his own Authorization Reply Message containing its own self generated AK. Hence attacker can register himself as a BS with victim SS. The attacker has to capture the identity of legitimate BS. Then it builds messages using the stolen identity. The attacker must transmit while achieving a RSS (receive signal strength) higher than the one of the fake base station.

WiMAX 802.16 supports two models of authentication at network entry: unilateral (MS only) and mutual (BS and MS). The lack of mutual authentication between the SS and BS is the main reason behind this kind of attack. There are two types of certificate are categorize by WIMAX standard" one is for subscriber station (SS) certificates and other is for manufacture certificate but there is no provision for Base Station (BS) certificates. A manufacture certificate identifies manufacture of WIMAX device. It can be self signed certificate or subjected to any third party. The SS certificate is used by BS to determine whether the SS is legitimate or not. Manufacture normally create and sign Subscriber Station certificates. The major drawback of the WiMAX security design is the lack of Base Station (BS) certificate.

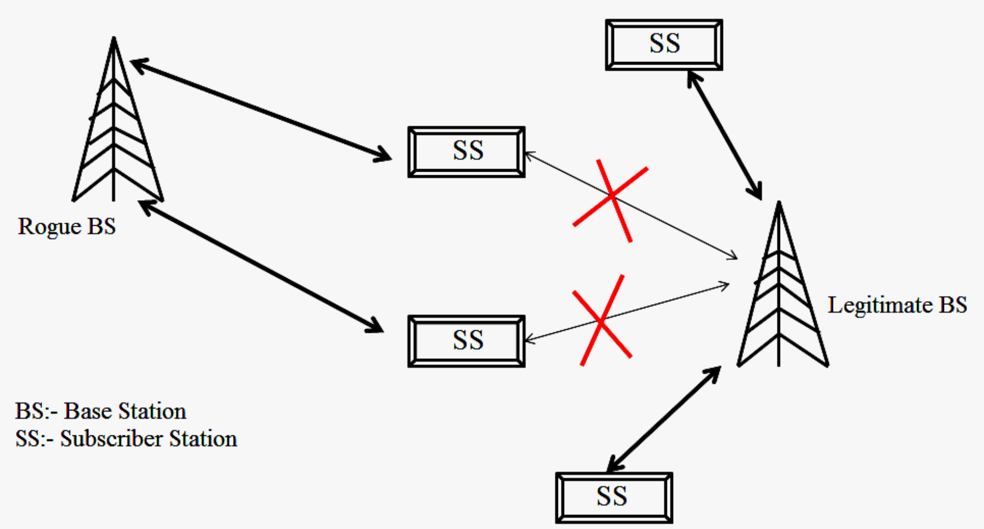

Fig 3 Working of Rough Base Station

VII. CONCLUSION

WiMAX is a powerful wireless services access platform that will increasingly support a wide range of revenue-generating voice and data applications for network service providers around the globe. The MSS provides a specialized security service focused on understanding and satisfying the unique business and technical needs of leading network service providers. MSS can benefit provides in the development stages of WiMAX, as well as in cases where WiMAX has already been implemented. Hacking, fraud, virus attacks, identity theft, denial of services attacks and data pirating can lead to WiMAX services interruption and revenue loss. The more a service provider relies on data services and data-driven applications, the more it needs to have an advance network security design. MSS security design and integration services are uniquely able to protect WiMAX network infrastructure. MSS helps service providers proactively manage their WiMAX networks, reducing vulnerabilities and safeguarding performance. Our main aim to write this paper is to discuss the security assessments in WiMAX and then find out the possible solution. Our study can provide a guideline to the WiMAX for the design of a more secure and practical network.

REFERENCES

[1] WiMAX End-to-End Network Systems Architecture - 3GPP/ WiMAX Interworking, Release 1; 2006; WiMAX Forum

[2] IEEE TIC 2009, Information Asseurance in Security and Privacy, September 27-29, 2009 Toronto, Ontario, Canada

[3] IEEE802.16 working group htpp://www.IEEE802.16.org.

[4] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," IEEE Sec. & Privacy, vol. 02, no. May-June 2004, pp. 40-48.

[5] Randall Nichols, and Panos Lekkas, "Wireless Security Models, Threats, and Solutions," McGraw-Hill 2002.

[6] Benjamin M. Lail, "Broadband Network and Device Security," McGraw-Hill 2002.

[7] Michel Barbenu, "WIMAX 802.16 Threat analysis," 2005.

[8] Hao Yang, Fabio Ricciao, Songwu Lu, and Lixia Zhang, "securing Wireless World." 2008.

[9] "Broadband Wireless Access with WIMAX/802.16: Current Performance Benchmarks and Future Potential", GHOSH (A.), WOLTER (D.R.), ANDREWS (J.G.), CHEN (R.), IEEE Communication Magazine, 43, no. 2, pp 129-136, February 2005.

[10] "IEEE Standard for Local and Metropolitan Area Network. Air Interface for Fixed and Mobile Broadband Wireless Access System" IEEE Std 802.16e. New York: IEEE Press , 2006.

[11] "Securing a Wireless World", IEEE Comm. Mag. vol. 94, Hao Yang, Fabio Ricciato, Songwu Lu, and Lxia Zhang, no. 2, pp 442-454, Feb 2006.

[12] "WIMAX/802.16 threat analysis", M. Barbeau, Proceedings of the 1st ACM International Workshop on Quality of Service &Security in Wireless and Mobile Networks, pp. 8-15, October 2007.

[13] "Rough Base Station Detection in WiMAX/802.16 Wireless Access Networks" La detection de faussed station de base dans les reseaux d'accessans fil WIMAX/802.16 Michel Barbeau School of Computer Science, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada KIS 5B6 Jean-Mare Robert1 Alcatel, CTO Security Research and Competence Center, 600 March Rd., Ottawa, 2006.

[14] www.wimaxforum.org/resorces/featured-research

[15] www.wimax industry.com/wimaxwhitepapers.html

[16] www.freewimax.com

[17] http://4g-wirelessevolutio.tmcnet.com