HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 9, May 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

A Review of Security Vulnerabilities and Threats in WiMax

***Vikesh Kumar**[*] **and Noor Mohammad**[†]*
vikesh.tomar@gmail.com

Abstract

The usual thought of communication is to send the details from source node to destination node but in my view the communication just isn't sent the knowledge even so the volume of secure information that's sent from source node to destination node. Security has developed into a main objective in order to provide protected communication in Wireless environment. The much anticipated technology for wireless broadband access, the WiMAX (Wireless Interoperability for Microwave Access) is finally getting to be available with to provide high data rates and provide interoperability of vendor devices at the same time. As being a promising broadband wireless technology, WiMAX has many salient advantages over for example: high data rates, service quality, scalability, security, and mobility. Many sophisticated authentication and encryption techniques are embedded into WiMAX but it still exposes to numerous

[*]M.Tech. Student, Department of Computer Science & Engineering, Graphic Era University - Dehradun, India.
[†]Assistant Professor, Department of Computer Science & Engineering, Graphic Era University - Dehradun, India. Email: noormohdcs@gmail.com

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 9, May 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

attacks in. This paper provides a brief survey of security vulnerabilities found in WiMAX network. Vulnerabilities and threats regarding both Physical and MAC layers in WiMAX.

Keywords

WiMAX, Security Threats, Review.

Introduction

The wireless method is less secure then wired system as a result of deficit of physical boundary. Wi-Max is the anticipated broadband wireless access mechanism for delivering high speed connectivity, making it attractive to internet and telecommunication service providers. In 802.16 networks is always that each subscriber station need to have a X.509 certificate that will uniquely identify the subscriber.

Basic Concept of WiMAX

WiMAX is usually shortly describe a telecommunication technology aimed towards providing wireless data over long distances in a variety of ways from examine point link to full mobile cellular type access. It can be according to IEEE 802.16 standard. In IEEE 802.16 here wide range of different protocol standard for WiMAX has been recently discussed [3].

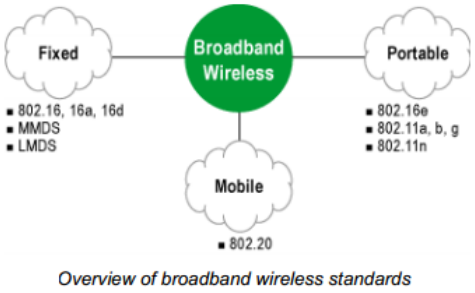


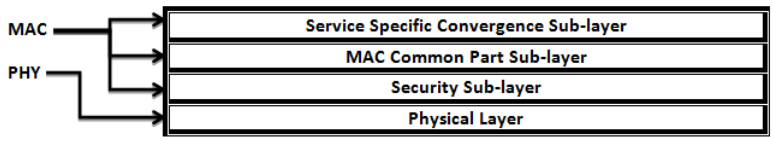
Figure 1: *Overview of boradband wireless standards*

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 9, May 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

WiMAX Protocol Architecture

The IEEE 802.16 protocol architecture is divided into two main layers:

1. The Medium Access Control (MAC), and
2. The Physical (PHY) layer



MAC layer consists of three sub-layers. The first sub-layer is Service Specific Convergence Sub-layer for higher data services, flow and connection to MAC layer. The second Sub-layer is Common Part Sub-layer its work with security sub-layer. For the system access CPS define the rule, mechanism, and bandwidth allocation and connection management. The third Sub-layer is the security Sub-layer which lies between the MAC CPS and the PHY layer, key establishment and exchange, addressing the authentication, encryption and decryption of data exchange [1].

The Physical layer (PHY) provides a two-way mapping between MAC protocol and Physical layer and transmitted with coding and modulation of radio frequency signals [2].

Threats at Physical Layer

1. Wireless network uses radio, anyone with the proper receiving end equipment can intercept the signal in air [1].
2. Jamming and scrambling are two most common attacks at PHY layer.
3. Jamming is about reducing the channel capacity.
4. Scrambling is incredibly identical to jamming, but it's about targeting particular timeslots or frames [2].

Threats at Security Sub-Layer

1. The results traffic is secured using strong encryption algorithms like DES and AES [2].

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

2. The attacker is going to be keen to fight the web link during authentication or key exchange process [1].

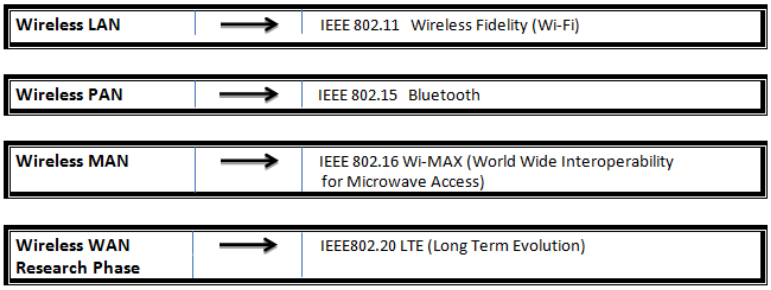


Figure 2: *Wireless Network Standards*

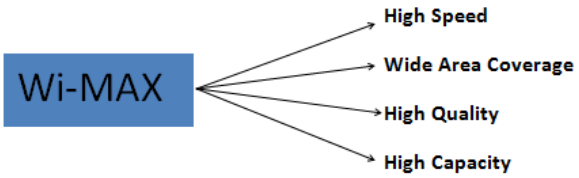


Figure 3: *Promising features of WiMax*

Security Threats in WiMax

In IEEE security is considered the most important part in the design of the protocol. However, security mechanism on the IEEE 802.16 still remains an issue. WiMAX is comparatively a different technology and it's not deployed widely to justify the data of threats [5].

Security in WiMAX is implemented in the Privacy Sub Layer. WiMAX provides a security architecture which basically secures the wireless transmission using different components. Some essential elements discussed are X.509 certificates, the security association, encryption method and the encapsulation protocol [7].

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 9, May 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

WiMAX Implementation on Hardware

Wimax system must meet a number of critical requirements such as processing speed, flexibility and time and energy to market, and it is these stringent requirements that ultimately drive selecting the hardware platform. Some of the major implementation challenges are further described below [6].

Implementation Challenges

Processing speed: broadband wireless system such as WiMAX have throughput and data rate requirement that are significantly higher than those in cellular system such as WCDMA. In order to able to support such high data rate, the underlying hardware platform must have significant processing capabilities.

Flexibility: WiMAX is relatively new market and it is currently studying the initial development and deployment process. 802.16 D has just been standardized while 802.16 e mobile version remains from the work.

Time to Market: Because WiMAX is definitely an emerging technology, time-to-marketplace is a key differentiator for OEMs trying to find early success in gaining market share. It's an effect on the development cycle and choice of hardware platform, with designers requiring easy-to-use development tools, software, boards, and off-the-shelf IP and reference designs to be able to accelerate the machine design.

Cost reduction path: last and important requirement to bear in mind choosing the hardware platform could be the use of a lasting cost reduction path. The evolving WiMAX standard is predicted to stabilize following the initial uncertainty surrounding it, leading to a scenario where expense of the ultimate product becomes a lot more important than retaining flexibility. A hardware platform that has this kind of clear cost reduction path and enables a seamless flexibility/cost tradeoff may be the need of the hour [9].

Wi-Fi vs WiMAX

WiMAX and Wi-Fi are wireless broadband technologies, but here difference between technical executions [6]. Wi-Fi was developed to be used for mobile computing device, such as laptop, in LANs, but in now increasingly used for more services, including internet and VoIP phone access, gaming and basic connectivity of consumer electronics such as televisions and DVD players,

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

or digital cameras on the other WiMAX was developed as standards based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL [4].

	802.16 WiMAX	**802.11 WiFi**	**802.20 Mobile-Fi**	**UMTS 3G**
Bandwidth	Share up to 70 MB/S	11-54 MB/S Shared	Up to 1.5 MB/S each	384 KB/S-2 MB/S
Range (LOS)	30-50 km	100 meters	3-8 km	Coverage is overlaid on wireless infrastructure
Range (NLOS)	2-5 km	30 meters	3-8 km	Coverage is overlaid on wireless infrastructure
Frequency/ Spectrum	2-11 GHz for 802.16a and 11-60 GHz for 802.16	2.4 GHz for 802.1 b/g and 5.2 GHz for 802.11a	<3.5 GHz	Existing wireless spectrum
Licensing	Both	Unlicensed	Licensed	Licensed
Standardization	802.16, 802.16a and 802.16 REVd, 802.16e	802.11a, b and g standardized	802.20 in development	Part of GSM standard
Mobility	Fixed (Mobile-16e)	Portable	Full mobility	Full mobility

Table 1: *Comparison with other Wireless Technologies*

Security in WiMAX

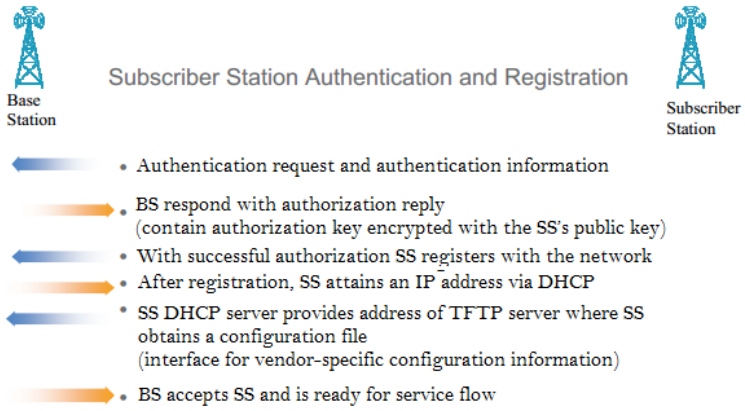


Figure 4: *Security in WiMax [7]*

Conclusion

In this particular paper, we offer an appraisal on authentication or authorization scheme on WiMAX. As being the utilization of WiMAX will increase the problem concerning the security is additionally likely to increase. The threats affect both layers of WiMAX. At PHY layer, jamming may very well be a serious threat. At MAC layer, critical threats include eavesdropping of management massages or DoS attacks. Ideas studied security vulnerability and threat and their solution. IEEE 802.16e provide better security compared to 802.16d in user authentication, access control data privacy and data integrity using sophisticated authentication and encryption technology.

References

[1] Saurabh Dubey, Sachin Kumar, Security Issues in WiMAX: A Critical Review, International Journal of Information and Computation Technology, Vol 3, No. 3, pp. 189-194, 2013.

[2] R. K. Jha and Dr. U. D. Dalal. A Journey on WiMAX and its Security Issues, International Journal of Computer Science and Information Technologies, Vol.1 (4), pp. 256-263, 2010.

[3] B. Sikkens, Security issues and proposed solution concerning authentication and authorization for WiMAX (IEEE 802.16e).

[4] H. Kaur and J. Saini, Review Paper on Performance Improvement of WiMAX using Coding Techniques, International Journal of Current Engineering and Technology, Vol. 3, No. 4, October 2013.

[5] A. Kumar, P. S. Sharma, V. K. Gupta, Review of Security Threat and Solution in WiMAX (802.16e), International Journal of Scientific and Engineering Research, Vol. 4, July 2013.

[6] T Han, N Zhang, K Liu, B Tang, Y Liu, Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, in 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005.

[7] A Deininger, S Kiyomoto, J Kurihara, T Tanaka, Security Vulnerabilities and Solutions in Mobile WiMAX, International Journal of Computer Science and Network Security, Volume 7 No.11, November 2007.

[8] T. Nguyen. (2009) A Survey of WiMAX Security Threats April 20, 2009.

[9] Taeshik Shon, Wook Choi: An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, First International Conference, NBiS 2007, LNCS, Vol. 4650, pp. 88-97, 2007.

[10] Service Document WiMAX, Available at http://www.aceindia.com/sites/default/files/documents/WiMAX_Service_Documentv1.pdf

[11] Sasan Adibi, Bin Lin, Pin-Han Ho, G.B. Agnew, Shervin Erfani, Authentication Authorization and Accounting (AAA) Schemes in WiMAX, Avaibale at: http://adela.utko.feec.vutbr.cz/mzsy/prednaska/Authentication%20Authorization%20and%20Accounting%20(AAA)%20Schemes%20in%20WiMAX.pdf

[12] Altera Corporation, White Paper: Accelerating WiMAX System Design with FPGAs, available at: http://www.altera.com/literature/wp/wp_wimax.pdf

[13] Arvind Kumar and Tanmay De, A Survey on Routing Protocols for Mobile Ad-hoc Networks (MANETs), HCTL Open International Journal of Technology Innovations and Research, Volume 5, Sept 2013, ISSN: 2321-1814, ISBN: 978-1-62840-986-4.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2 *References*

[14] Arpit Gupta and Gaurav Shrivastava, APDA with Data Collective: A Survey to Prevent Attacks in VANET, Edition on Wired and Wireless Networks: Advances and Applications, Volume 3 - November 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62951-015-6.

[15] Anil Kumar Khurana and Vishal Srivastava, QoS and Energy Efficient Routing Protocols in WSN, Edition on Wired and Wireless Networks: Advances and Applications, Volume 3 - November 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62951-015-6.

[16] Nitin Goel, Dr. Neetesh Purohit, Prof. B. R. Singh, Handover between Cellular Network to Wifi, Volume 4 of HCTL Open Science and Technology Letters (STL), February 2014, ISSN: 2321-6980, ISBN: 978-1-62951-212-9.