ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Study and Analysis of Mutual Authentication Security Issues and Solution Schemes in WiMAX 802.16

Sher Singh [1], Gaurav Garg[2]

M. Tech, Dept. of CSE, Advanced Institute of Technology and Management, Palwal, India[1]

Assistant Professor, Dept. of CSE, Advanced Institute of Technology and Management, Palwal, India[2]

ABSTRACT: Wireless Technology are becoming more popular than wired network technology. In this paper we are introducing a technology called Worldwide Interoperability for microwave access (WiMAX).Every technology has some security issues aspects like authentication, authorization and encryption. Here we will discuss about mutual authentication problem and solution in WiMAX.The absence of proper authentication mechanism can lead to many threats like denial of service, masquerading and attacks on the authentication protocol. We will describe the BS authentication to improve the mutual authentication. Like other standards 802.11, WiMAX is also not free from vulnerability, threats and risks. This documentation will elaborate the possible attacks, transmission issue and their corresponding solutions.

KEYWORDS: Base Station authentication ; security; standards; WiMAX 802.16.

I. INTRODUCTION

The family of IEEE 802.16 standard is also known as WiMAX andhas produced high expectations from hardware vendors and internet service provider. Wireless network have brought about major development in the way, theinformation is shared between individual to individual, individual to business and business to business.

Wireless networks are convenient and popular, but the security issues in these networks are of major concern. Some of the security threats to wireless network are denial of service, masquerading, interception, theft of service etc. To prevent these threats use of security features such as authentication, authorization and encryption, becomes very important in any wireless network. Authentication is the ability of the network to ensure that the subscriber andsubscriber devices are original (legitimate)users and devices to be connected to the network. WiMAX (World wide Interoperability for Microwave Access) is a telecommunications technology that provides wireless andbroad band data transmission with high bandwidth and transmission rates between point-to-point links and fullmobile cellular access, as defined by IEEE standard as 802.16.

Adding mobility of stand is through IEEE 802.16 makes the attacker's life even easier. This need to maintain a secured state while a mobile SS moves between BSs introduces new vulnerabilities. An attacker could forge new frames and capture, modify and retransmit frames from authorized parties. The design must therefore also provide adata authenticity mechanism. Interference and distance could allow an attacker to communicate with two authorized parties who cannot communicate directly with each other, and reorder and selectivity forward frames. Thus, design must detect replayed frames. Can resend a valid, already send frames unmodified. Also provide a data authenticity mechanism.

Generally the Base Station (BS) uses the manufacturer certificate's public key to validate the Subscriber Station (SS) certificate, and therefore identify the device as genuine. This design assumes that the Subscriber Station (SS) keeps the private key related to its public key in a sealed storage, preventing attackers from easily compromise it. The major drawback of the WiMAX security design is the lack of a Base Station (BS) certificate. The only approach to defend the client against forgery or replay attack is to offer a scheme for mutual authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

II. RELATED WORK

A number of papers have been published regarding the security issues of WiMAX networks since IEEE 802.16 standard was developed.

In [9] Xu et al. give a detailed analysis on privacy and key management protocols of the standard. In [11]paper addressed the security issues of one-way authentication and rogue base station attack. In [13] the authentication issue is studied in types of wireless mesh networks.

In [10]Jin et al. propose an improved mutual authentication scheme in multihop WiMAX networks, in which they improve the X.509 certificate by using ECC algorithm instead of RSA, and modify the flow of mutual authentication to improve the security in multihop WiMAX networks.

In [4], Tie and Yi proposed a multihop ticket based handover authentication which adopted the idea from Kerberos and used a ticket to allow MS, RS, and BS to mutually authenticate each other. However, the authors in the aforementioned papers did not take rogue access node attack into consideration.

In [14]authors propose a design of hybrid authentication and key distribution scheme to support the IEEE 802.16j (part of current IEEE 802.16-2012 standard) MMR requirements. Although the authors claim that this hybrid design is robust enough to prevent rogue node attack, they only consider the case when a rogue RS tries to join the network at initial phase, and they do not take rogue BS attack into account. The latter case will cause more severe damage to the network since a rogue BS can take control of the whole area within its communication range if it successfully joins the network as a legitimate BS.

In another paper [15], the authors present a distributed scheme using decode and forward relays with localized authentication, which helps to authenticate MS and RS at initial network entry. However, this scheme still cannot solve the problem of rogue BS attack.

III. SECURITY THREATS

- **DoS/Reply Attacks during MS Initial Network Entry: -**The initial network entry procedure is crucial since it is the first gate to establish a connection to Mobile WiMAX by performing several stepsincluding: Initial Ranging process, SS Basic Capability (SSBC) negotiation, PKMv2 authentication and registration process. When the SSenter into the network, it scans the downlink channel and synchronizes with it. In the downlink, BS announces the range of initial ranging code forSS. The SS selects any one of the ranging code and sends it to BS for initial ranging. The BS responds to the successful reception of ranging code by Ranging Response (RNG-RSP) message. The RNG-RSP message is used to nullify the offsets of frequency, time and power used by the SS. Thenthe SS goes for SBCREQ and other procedures. The message flows before SA-TEK are un-encryptednature. So the attacker can decode the MAC messages, modify and resend it to BS or SS. Thesecurity issues during initial network entry are: (i) RNG-RSP vulnerability (ii) Auth-Request and Invalid vulnerability and (iii) Rogue BS.
- **Latency During Handover and Unsecured Pre-Authentication:-** When handover occurs, the MS is re-authenticated and authorized by the target BS. The re-authentication and key exchange procedure increase the handover time, which affects the delay sensitive applications. In handover response message, BS informs the SS whether SS needs to do re-authentication with the target BS or not. If the SS is pre-authenticated by target BS before handover, then there is no need of device re-authentication but user authorization is still necessary.
- **Downgrade Attack: -**The first message of the authorization process is an unsecured message from SS telling BS what security capabilities it has. An attacker could send a spoofed message to BS containing weaker capabilities in order to convince the BS and the attack SS to agree on an insecure encryption algorithm. The standard doesn't specify a concrete solution for the situation that two valid answer received by BS.
- **Bandwidth Spoofing:-**In bandwidth spoofing the attacker grabs the available bandwidth by sending the unnecessary bandwidth request message to BS.
- **Key Space Vulnerability:-**In 802.16e a 4-bit sequence and 2-bit sequence number is issued to discriminate between successive generations of AKs. Also, a 2-bit key sequence number is used for the same reason with TEKs. The size of the key is inadequate to protect the keying material from attacks.
- **Man in Middle Attack: -**This form of WiMAX security issue occurs when a base station is set up to impersonate a base station in the network, either just to a subscriber, or a two way impersonation between the subscriber and the base station.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

IV. AUTHENTICATION SCHEMES

The purpose of authentication and authorization techniques mainly used in wireless systems are to prevent; snooping of the user ID, denial of service (DoS), man in-the-middle attack, offline dictionary attack, authentication method downgrading attacks, and also breaking a weak key. Adibi et.al [1] described EAP that offers an authentication scheme, which prevents the above mentioned problems. EAP allows for mutual authentication. It is basically a request-response protocol based on four different types of messages: EAP request, EAP response, EAP success, and EAP failure. In EAP protocol the different authentication methods are integrated to match the attributes of communication channel. This paper also described the authentication mechanism for WiMAX. Forend-to-end authentication, WiMAX uses PKM-EAP (Privacy Key Management-Extensible Authentication Protocol), which relies on the TLS (Transport Layer Security) standard which uses public key cryptography. There are two Privacy Key Management Protocols supported in 802.16e -PKMvl and PKMv2. In this paper the PKMv2 with more enhanced authentication features are discussed. The PKM-EAP of WiMAX has been introduced into the area of WLAN in a more robust and secured way. Mutual authentication is provided in PKMv2, which could avoid" Man in the Middle" attacks. Paper gives description ofX.509 certificate which is a digitally signed certificate, issued to each SS.The X.509certificate cannot be easily forged. Hence, each of the base station in WiMAX has high performance security processor which is dedicated and which provide us to implement a mutual authentication system in WiMAX.The two main goals of the WiMAX security are to provide privacy across the wireless network and to provide access control to the network.

The physical layer threat and MAC layer threat of WiMAX are studied by Lang Wei-min et.al [8] then it lists the security requirements of a WiMAX system which includes confidentiality, authenticity, integrity, and access control. Furthermore the security architecture of WiMAX is proposed which represent that the security sub layer of IEEE 802.16 provides subscribers with privacyacross the network and confidentiality. Paper also describe that the management messages are exchanged between the SS and BS for authentication and then advance to key management prior to transmission of data that is why authentication plays a critical role in securing connection in WiMAX and also in the transmission across WiMAX. In order to achieve the goal of authentication RSA authentication is described which with PKM uses X.509 digital certificates, and the RSA public-key encryption algorithm is used which is used to bind the public RSA encryption keys to the MAC addresses of SSs. X.509 certificates are used to allow the base station to identify subscriber stations. According to the 802.16 standard the 802.16-ompliant SSs must have to use the X.509 Version 3 certificate formats which provide a public key infrastructure that is used for the purposeof secure authentication. The paper also recommends the use of other critical techniques, such as EAP and HMAC.The subject of authentication within WiMAX (IEEE 802.16-2009) based wireless metropolitan networks is examined by Jacobs [6]. The two different WiMAX authentication mechanisms i.e. PKM v1 and PKM v2 are discussed. And a number of aspects which affect their authentication capabilities are presented. Managing digital certificates and the lack of multiple certificate authority support is studied. Due to the lack of multiple certificate authority support the interoperability of WiMAX devices produced by different manufactures is prevented. In this paper the recommendations are presented that should improve about the question that how WiMAX authentication operates and how to allow for mixed manufacturer device interoperability. This concluded RSA asymmetric encryption, when coupled with a PKI, provides highly reliable peer-entity authentication and non-repudiation. These security services are the result of a recipient of a message digitally signed by the sender's private key:• Having high assurance that the sender's private key has not been stolen or lost, or is still valid for use by the signer.• The message recipient possesses an authentic copy of the sender's public key.The first point is achieved by the recipient being able to verify that the certificate associated with the sender's private key has not been revoked prior to the certificate's not After date. The second point is achieved by the recipient being able to establish a chain of digital signatures on certificates starting from the sender's certificate to the certificate of the CA that issued the sender's certificate and continuing up a chain of CA certificates until a CA is identified that is within the hierarchy of CAs leading down to the CA that issued the recipient's Certificate. In the concern of increasing data security the network access control has become avery important part of network security system. Chiornita et.al [3] analysed different EAP authentication access methods that can be used with IEEE802.Ix standard as a means to protect the computer network against the unauthorized access from attackers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

V. CONCLUSION AND FUTURE WORK

As the popularity of WIMAX increases, so will the threats to it. Some of the issues have been dealt with and no longer pose a problem, but some still persist and need to be considered carefully as WiMAX becomes more prevalent. Malicious elements are working round the clock to break the security of the various networks. In a WIMAX system, data are transmitted via wireless link, so the security is becoming the hot topic of research.

In this Paper we also introduced various authentication schemes based on the Extensible Authentication Protocol i.e., EAP-TLS,EAPTTLS,PEAP, EAP-SIM, which extends the authentication to AAA server. AESCCM mode is a new data link cipher for data authenticity mechanism, which is specified by NIST (National Institute of Standards and Technology).The standard also, replaces Triple DES key wrapping in the PKM protocol with the AES ECB mode and facilitates low cost re-authentication during roaming. Further research is required to find out security threats and vulnerabilities in the IEEE 802.16e standard.

In the future work, we will perform a numerical analysis on the authentication performance of our protocols in terms of key processing time, response time, and total overhead of provisioning the dual authentication, the security zone key, and the license.

REFERENCES

1. Adibi, S.; Bin Lin; Pin-Han Ho; Agnew, G.B. Erfani,S.2006.Authentication, Authorization and Accounting(AAA) Schemes in WiMAX.IEEE InternationalConference on Electro/information Technology,210-215.
2. Kyle, "Intel Capital: WiMAX Is Not Dead," http://www.nibletz.com/international/intel-capital-wimax-is-not-dead/.
3. Chiornita, Alexandra; Gheorghe, Laura; Rosner, Daniel.2010.A Practical Analysis of EAP Authentication Method.9th Roedunet International Conference,31-35.
4. L. Tie and Y. Yi, "Extended security analysis of multi-hop ticket based handover authentication protocol in the 802.16j network," in Proceedings of the 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '12), pp. 1-10, Shanghai, China, September 2012.
5. IEEE Standard for Air Interface for Broadband Wireless Access Systems, "IEEE Std 802.16-2012 (Revision of IEEE Std 802.16-2009)," pp. 1–2542, August 17, 2012.
6. Jacobs, S. 2011.WiMAX subscriber and mobile station authentication challenges.IEEE Communications Magazine,166-172.
7. J. Huang and C.-T. Huang, "Secure mutual authentication protocols for mobile multi-hop relay WiMAX networks against Rogue base/relay stations," in Proceedings of the IEEE International Conference on Communications (ICC '11), pp. 1–5, IEEE, Kyoto, Japan, June 2011. · ·
8. Lang Wei-min; Zhong Jing-li; Li Jian-jun; Qi Xiang-yu.2008.Research on the Authentication Scheme of WiMAX .4th International Conference on Wireless Communications, Networking and Mobile Computing,1-4.
9. S. Xu, M. Matthews, and C.-T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16," in Proceedings of the 44th ACM Southeast Regional, pp. 113–118, Melbourne, Fla, USA, March 2006.
10. H. X. Jin, L. Tu, G. Yang, and Y. Yang, "An improved mutual authentication scheme in multi-hop WiMAX network," in Proceedings of the International Conference on Computer and Electrical Engineering (ICCEE '08), pp. 296–299, Phuket, Thailand, December 2008. · ·
11. D. Johnston and J. Walker, "Overview of IEEE 802.16 security," IEEE Security and Privacy, vol. 2, no. 3, pp. 40–48, 2004. · ·
12. F. Yang, H. Zhou, L. Zhang, and J. Feng, "An improved security scheme in WMAN based on IEEE standard 802.16," in Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1191–1194, September 2005.
13. K. Khan and M. Akbar, "Authentication in multi-hop wireless mesh networks," Transactions on Science, Engineering and Technology, vol. 16, pp. 178–183, 2006.
14. D. Zhu, N. Pang, and Z. Fan, "A self-testing approach defending against rogue base station hijacking of intelligent terminal," in Proceedings of the International Conference on Applied Science and Engineering Innovation, Zhengzhou, China, May 2015. ·
15. S. Khan, N. Fisal, S. Kamilah, and M. Abbas, "Efficient distributed authentication key scheme for multi-hop relay in IEEE 802.16j network," International Journal of Engineering Science and Technology, vol. 2, pp. 2192–2199, 2010.