WiMAX Security Threats And Their Counter Measures

Er.Kaushik Adhikary[1], Er.Vineet Mehan[2], Er.Amandeep Singh Bhatia[3]

Asst.Professor, C.S.E, Maharaja Agrassen University, Baddi, India[1]
Assoc.Professor, C.S.E, Maharaja Agrassen University, Baddi, India [2]
Asst.Professor, C.S.E, Maharaja Agrassen University, Baddi, India [3]

Abstract: WiMAX is a recent technology in wireless communication that is based on IEEE 802.16 standard.It is a Wireless Metropolitan Area Network. The WiMAX trademark was coined by WiMAX Forum.This Forum defines the precise content and scope of WiMAX technology through technical specification. WiMAX provides many advantages over previous technologies like high data rates, scalability, quality of service and security. WiMAX provides many security techniques but still it is vulnerable to various threats.This paper exposes those threats and their countermeasures.

Keywords: WiMAX, Security Threats, Vulnerabilities and countermeasure

I. INTRODUCTION

The standard used for broadband wireless access BWA is IEEE 802.16. To advance and certify compatibility and interoperability of broadband wireless product based on IEEE 802.16 family standards WiMAX forum has been on the mission. Under a line-of sight –condition, IEEE 802.16(e) which deals with mobility in WiMAX network is an amendment of WiMAX. Due to lack of physical boundary wireless system is less secure. In WiMAX the security layer is built into the protocol stack. The authentication and key exchange messages are defined as part of the medium access control layer. During the key exchange phase the MAC layer performs the encryption based on the keys negotiated in this phase. For fixed network security mechanism the IEEE 802.16 d has been defined. On the basis of the PKMv1 the security architecture of the IEEE 802.16d has been defined. For the mobile network the IEEE 802.16e [1] standard has been defined.

On compromising the radio links between WiMAX nodes the threats to the WiMAX wireless interface is focused. Both line-of-sight (LOS) and non-line-of-sight signal (NLOS) propagation is supported by these radio links. Because an adversary has to physically locate equipments between the transmitting nodes to compromise the confidentiality or integrity of the wireless links, links from LOS WiMAX systems are harder to attack than those from NLOS systems. The potential staging areas for both the client and adversaries are expanded as WiMAX NLOS system systems provide wireless coverage over large geographical regions. Organizations should implement some precautions to improve WiMAX system security [2]. For designing, implementing and maintaining properly the secured technologies, a security policy of the organization should be very strong. The design and operation of the technical infrastructure and the behavior of users should be addressed by a WMAN policy. WMAN policies such as disabling unneeded services and altering default configurations should be considered while configuring client devices. To stop or permit certain events to take place when definite conditions are met policy driven software solutions can be implemented on client devices. Policy driven software helps to ensure that with an organization’s defined policies client devices and users are complied. Federal Information Processing Standard (FIPS) validated cryptographic modules are employed in few WiMAX products. Many times with other security solutions that meet FIPS requirement vendor often integrate integrate their WiMAX product. These add-ons are not extended in WiMAX interoperability certifications. This can affect the security of the system and so organization should work closely with WiMAX vendors to gain a better understanding of potential system configuration constraints.

II.WIMAX ARCHITECTURE

Five basic architectural components are there in WiMAX networks:

A. Base Station (BS): The BS logically connects wireless subscriber devices to operator networks. Access to the operator networks and communications with the subscriber’s device is maintained by the BS. To enable wireless communications a BS consists of the infrastructure elements like antennas, transceivers and other electromagnetic wave transmitting equipments. B S can be used as part of mobile solutions though they are basically fixed nodes. For example, to provide communication with nearby WiMAX devices, a BS may be affixed to a vehicle. In the multihop relay topology, a BS serves as a Master Relay-Base Station.

B. Subscriber Station (SS): The SS is a WiMAX capable radio system that is stationary. It communicates with a base station. It can also connect to a relay station in a multi-hop relay network operation.

C. Mobile Station (MS): An MS is used when devices are in motion at upto vehicular speed. It is a mobile SS. MS are operated by battery and so employs enhanced power management in comparison to fixed SS. For Example, WiMAX radios which include MS are embedded in laptops and mobile phones.

D. Relay Station (RS): In a multi-hop Security Zone a RS are configured to forward traffic to other RS or SS. The configuration of RS is SS. Just as the air interface between a BS and SS, the air interface between RS and SS is same.

E. Operator Network **:** To provide infrastructure network functions that provide radio access and IP connectivity services to WiMAX subscribers, the operator network is used. In the form of access service network (radio access) and the connectivity service network (IP connectivity) ,these functions are defined in WiMAX Forum. Using two wireless message types i.e. Management messages and data messages, WiMAX devices communicate. To transport data across the WiMAX network, data messages are used. To maintain the communication between an SS/MS and BS, management messages are used. For ex. Performing system registration events such as initial network entry, handoffs, etc.) , exchanging security settings and establishing communication parameters

III.VULNERABILITIES IN WIMAX

As WiMAX is wireless, it is susceptible to various vulnerabilities. The following discusses several major vulnerabilities:

A. *Need of BS to SS/MS authentication:*

There is authentication of SSs by BSs defined in PKMv1, but authenticating BS's by SSs/Mss is not provided [3]. A rogue BS may impersonate a legitimate BS due to lack of mutual authentication. The authenticity of protocol messages received from the BS is therefore not verified by the SS/MS. This would enable a rogue BS operator to take complete control of all traffic to and from the SS/MS, including capture of authentication credentials leading to a successful attack. Such an attack would also enable the rogue BS to impersonate name servers, allowing it to redirect user requests to computers with malware without easy detection. This vulnerability is mitigated in IEEE 802.16e-2005 and IEEE 802.16-2009 by the use of mutual authentication [4].

B. Feeble encryption algorithms: IEEE 802.16-2004 only supports the use of DES-CBC for encrypting communications which has well-documented weaknesses and is no longer approved for Federal agency use in protecting communications. IEEE 802.16e-2005 and IEEE 802.16-2009 support DES-CBC, but they also support multiple modes of AES that are approved for Federal government use.

C. Interpolation of reused TEKs: To determine which TEK is actively used to secure communications, IEEE 802.16-2004 TEKs employ a 2-bit encryption sequence identifier. Rendering the system vulnerable to replay attacks, a 2-bit identifier permits only four possible identifier values. The interjection of reused TEKs may lead to the disclosure of data and the TEK to unauthorized parties [5]. With the introduction of AES-CCM, this concern is resolved in IEEE 802.16e-2005 and IEEE 802.16-2009, which provides per packet randomization by adding a unique packet number to each data packet to protect the integrity of data and portions of the packet header.

D. Unencrypted management messages: Management messages are susceptible to eavesdropping attacks as they are not encrypted. To increase the efficiency of network operations, encryption is not applied to these messages. For management messages, IEEE 802.16-2004 does not provide any data authenticity protection. To protect against malicious replay or modification attacks, IEEE 802.16e-2005 and IEEE 802.16-2009 provide integrity protection for certain unicast management messages by appending a unique digest [6]. IEEE 802.16 multicast and initial network entry management messages do not add this digest. Digest integrity protection cannot be applied to management messages sent to multiple recipients (i.e., multicast transmissions), as with all wireless systems. Because nodes must first be authenticated to create the unique digest, initial network entry management messages cannot leverage integrity protection. An adversary may manipulate management messages to disrupt network communications in a man-in-the-middle attack by denial of service (DoS) attacks aimed at the WiMAX system, at specific network nodes, or both.

*E. Use of electromagnetic spectrum as a communications medium***:** Using RF to communicate inherently enables execution of a DoS attack by introducing a powerful RF source intended to overwhelm system radio spectrum. This vulnerability is associated with all wireless technologies [7]. The only defenses are either to locate and remove the source of RF interference or to move to another channel. Such actions can be challenging because of the large coverage areas of WMANs and the scarcity of alternative frequencies to support communications. It is recommended that organizations plan for out-of-band communications in the event of a DoS attack.

IV.THREATS

On compromising the radio links between WiMAX nodes, WiMAX network threats are focused. Compared with NLOS systems, LOS WiMAX systems pose a greater challenge to attack because an adversary would have to physically locate equipment between the transmitting nodes to compromise the confidentiality or integrity of the wireless link. NLOS systems provide wireless exposure over large geographic regions, which develop the potential staging areas for both clients and adversaries [8].

The following threats affect all WiMAX systems:

A.RF jamming: RF jamming attacks occurs in all wireless technologies. By introducing a powerful RF signal to overwhelm the spectrum being used by the system, the threat arises from an adversary. This denies service to all wireless nodes within range of the interference. RF jamming is classified as a DoS attack. The risk associated with this threat is identical for IEEE 802.16-2009, IEEE 802.16-2004 and IEEE 802.16e-2005 WiMAX systems.

B.Scrambling: Scrambling attacks affect all wireless systems are the precise injections of RF interference during the transmission of specific management messages. With the intent to degrade overall system performance, these attacks prevent proper network ranging and bandwidth allocations [Nas08]. Because they are engaged for short time periods and are not a constant source of interference scrambling attacks are more difficult to identify than jamming attacks. The threat related with this threat is identical for IEEE 802.16-2004, IEEE 802.16e-2005, and IEEE 802.16-2009.

C.Subtle management message manipulation:
Subtle DoS, replay, or misappropriation attacks that are difficult to detect are resulted due to exploitation of unauthenticated management messages . By allowing them to deny service to various nodes in the WiMAX system these attacks spoof management messages to make them appear as though they come from a legitimate SS/MS. An adversary drains a client node's battery by sending a constant series of management messages to the SS/MS in a *water torture* attack which is an example of subtle DoS. By following initial network registration with an appended integrity protection digest, IEEE 802.16e-2005 and IEEE 802.16-2009 provide integrity protection for certain unicast management messages. Attacks involving manipulation occurs in all other IEEE 802.16e-2005 and IEEE 802.16-2009 management messages, and all IEEE 802.16-2004 management messages,

D.Man-in-the-middle: When an adversary deceives an SS/MS to appear as a legitimate BS, Man-in-the-middle occurs and simultaneously deceiving a BS to appear as a legitimate SS/MS. During the initial network entry process, an adversary can perform a man-in-the-middle attack by exploiting unprotected management messages. This is because the management messages that negotiate SS's /MS's security capabilities are not protected. An adversary could send malicious management messages and negotiate weaker security protection between the SS/MS and BS if an adversary is able to impersonate a legitimate party to both the SS/MS and BS. An adversary can eavesdrop and corrupt data communications due to weaker security protection. The man-in-the-middle traffic relays between BS and SS/MS can be prevented by mandating the use of AES-CCM in IEEE 802.16e-2005 and IEEE 802.16-2009 since because it appends a unique value to each data packet. Adequate protection against man-in-the-middle attacks are not offered in IEEE 802.16-2004.

E.Eavesdropping: By using a WiMAX traffic analyzer within the range of a BS or SS/MS, an adversary can eavesdrop. Eavesdroppers are shielded from detection due to the large operating range of WiMAX networks. The confidentiality and integrity of communications are protected as eavesdropping mitigation relies heavily on technical controls. To identify encryption ciphers, determine the footprint of the network, or conduct traffic analysis regarding specific WiMAX nodes, management message traffic are monitored by the advisory. To decipher DES-CBC encryption, data messages collected during eavesdropping can also be used. Eavesdropping can be avoided using AES, since it provides robust data message confidentiality. IEEE 802.16-2004, IEEE 802.16e-2005, and IEEE 802.16-2009[9] have the same the risk associated with eavesdropping data messages.

V.COUNTERMEASURES

Countermeasures that may be used to reduce or mitigate the risks inherent to WiMAX systems are presented in the following sections. All possible attacks are not prevented by these countermeasures and they do not guarantee security. In response to technology the cost of countermeasures will change since the optimum security design is a dynamic intersection of threat risk and. With their acceptable level of risk organizations should implement countermeasures commensurate.

A. Management Countermeasures:

Management countermeasures assessment by an organization's management addresses any problem related to risk, system planning, or security. Organizations should develop a wireless security policy by addressing WiMAX technology. The security policy for an organization's foundation is designing, implementing, and maintaining properly secured technologies. WiMAX policy should address the design and operation of the technical infrastructure and the behavior of users

Policy considerations should include the following for WiMAX systems:

i. Roles and responsibilities
ii. Which users or groups of users are authorized to use the WiMAX system
iii. Which office or officer provides the strategic oversight and planning for all WiMAX technology programs
iv. Which parties are authorized and responsible for installing and configuring WiMAX equipment
v. Which individual or entity tracks the progress of WiMAX security standards, features, threats, and vulnerabilities to help ensure continued secure implementation of WiMAX technology
vi. Which individual or entity is responsible for incorporating WiMAX technology risk into the organization's risk management framework32
vii. WiMAX infrastructure
viii. Physical security requirements for WiMAX assets
ix. The use of standards-based WiMAX system technologies
x. Types of information permitted over the WiMAX system, including acceptable use guidelines
xi. How WiMAX transmissions should be protected, including requirements for the use of encryption and for cryptographic key management
xii. A mitigation plan or transition plan for legacy or WiMAX systems that are not compliant with Federal security standards
xiii. Inventory of IEEE 802.16 BSs, SSs/MSs, and other devices
xiv. WiMAX client device security
xv. Conditions under which WiMAX client devices are allowed to be used and operated
xvi. Standard hardware and software configurations that must be implemented on WiMAX devices to ensure the appropriate level of security

xvii. Standard operating procedures (SOP) for reporting lost or stolen WiMAX client devices

xviii. WiMAX security assessments

xix. Frequency and scope of WiMAX security assessments

xx. Standardized approach to vulnerability assessment, risk statements, risk levels, and corrective actions

B. Operational Countermeasures

In operational countermeasures controls that are executed by people are included. Configuration management, security awareness and training, incident response, personnel security and physical environment protection are their examples. In a system security plan (SSP) all parties involved with WiMAX system operations should maintain controls that are documented. SSPs provide an overview of the security requirements of a system are living documents which should be maintained and describe the controls in place to meet those requirements. This includes all system hardware and software, policies, roles and responsibilities, and other documentation materials. Documentation formalizes security and operational procedures to a given system are a security control. Only authorized personnel should have access to WiMAX equipment which is the physical security is fundamental to ensuring. Physical access control systems, personnel security and identification, and external boundary protection are the measures included. For example, integrating Federal personal identity verification (PIV) into physical access controls can reduce the risk of unauthorized access to WiMAX systems. To address the specific challenges and threats to wireless technologies training should be given to WiMAX system administrators and users. Because of its expansive coverage area it is difficult to prevent unauthorized users from attempting to access a WiMAX system, the use of additional security mechanisms may help prevent the theft, alteration, or misuse of WiMAX infrastructure components. The most prevalent spectrum used to accommodate WiMAX is the 2.5 GHz licensed range, but WiMAX solutions are also viable across several unlicensed spectrum ranges. Organizations should understand the implications of spectrum allocation as it impacts system availability. Due to the proliferation of unlicensed wireless technologies, interference may become an implementation obstacle when operating in unlicensed spectrum. Regardless of which spectrum frequency is used, organizations should use counter-interference technologies37 in addition to site surveys to ensure system availability.

VI.CONCLUSION

This paper described the security mechanisms present in the WiMAX. We identified and analyze the security issues ignored by the current mobile wireless standard. However, through this review, we can see that WiMAX does offer much more strong security solutions in comparison with other wireless technologies such as Bluetooth or Wireless Fidelity (WiFi). WiMAX is still under development and need more research on its securities vulnerabilities. In the near future, when WiMAX achieves a maturity level, it would have a great opportunity to be a successful wireless communication technology.

REFERENCES

[1] S. Frankel et al, NIST Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, NIST, 2007. http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[2] Tao Han et al, Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, Key Lab of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, 2007.

[3] Dong, H., and Yan, W. 2008. Secure Authentication on WiMAX with Neural Cryptography. In International Conference on Information Security and Assurance, 2008. ISA 2008, pp. 366-369**.**

[4] Yang, Y., and Li, R. 2009. Toward Wimax Security. In Proceedings of Computational Intelligence and Software Engineering, Wuhan, China, pp. 1-5.

[5] Sikkens, B., 2008. Security Issues and Proposed Solutions Concerning Authentication and Authorization for WiMAX. In Proceedings of 8th Twente Student Confereence on IT,Enschede.

[6] Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu, Anand Srinivasan," Analysis on Mobile WiMAX Security", IEEE TIC-STH 2009.

[7] Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking", Chapter 9: MAC Layer of WiMAX, Pearson Education Prentice Hall, 2007. ISBN (PDF) 0-13-222552-2

[8] Yang, Y., and Li, R. 2009. Toward Wimax Security. In Proceedings of Computational Intelligence and Software Engineering, Wuhan, China, pp. 1-5.

[9] Dong, H., and Yan, W. 2008. Secure Authentication on WiMAX with Neural Cryptography. In International Conference on Information Security and Assurance, 2008. ISA 2008, pp. 366-369