International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 30, Issue 01) and (Publishing Month: May 2016)
(An Indexed, Referred and Impact Factor Journal)
ISSN: 2319-6564
www.ijesonline.com

Security Issues in WiMAX and Solution

Algasim Min Allah Omer and Dr. Hala Eldaw Idris

**Department of communication, Faculty of Engineering,
Al-Neelain University, Khartoum, Sudan**

Publishing Date: May 28, 2016

Abstract

Security has become a primary issue to provide a communication, in wireless area we know the basic concept in communication the data sent from source to destination we talk here about a lot of data it can attack and vulnerability. WiMAX has a many advance like availability and scalability and quality and security but it has some vulnerability and threat, in this paper we discuss the security vulnerability network of WiMAX and threat and some solution for this vulnerability.

Keywords*: WiMAX vulnerability security, threat, IEEE 802.16e*

1. Introduction

The IEEE 802.16 family of standards. Based on the IEEE 802.16 standard, the WiMAX (Worldwide Inter-operability for Microwave Access) is "a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access". The WiMAX is supported By the WiMAX forum, which is a non-profit organization formed to promote the adoption of WiMAX compatible products and services [1].

WIMAX it involve a many application to many people to connect wireless backbone. It has high data rate and this application include voice calls, video transfer and other services, this application require security process it can divided into three steps: authentication, Data Key exchange and Data Encryption, Authentication for equipment and user is done by admission control process [2], [4].

2. Security Process in WiMAX

2.1 Authentication

Privacy & Key Management Protocol version 1(PKMV1) this is protocol Compatible WITH WIMAX standard [2].and it has three steps, the figure below shows PKM v1 the exhaustive operation of PKM v1found in [2], [5], [6].

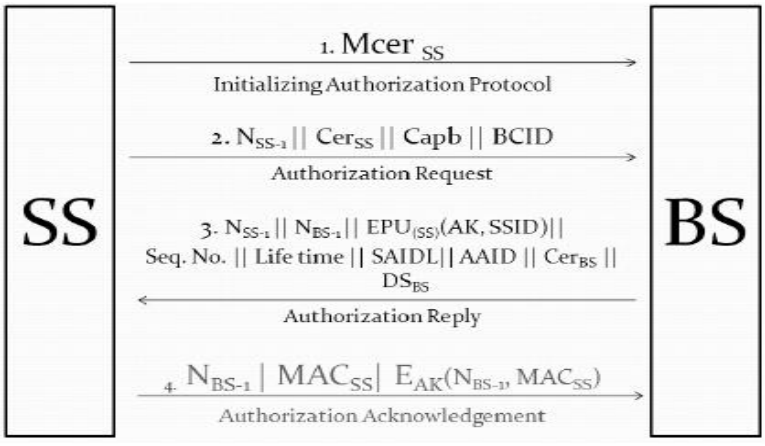

Figure 1: Privacy Key Management Protocol v1

When privacy user Make concessions the intruder attacks the network and this is describe attacks of authentication, and this attack it has a many kind like Interleaving Attack it as the enemy interleaves a communication session by preserve connection with subscriber station and base station, concern as BS to SS and conversely. And all information coming through the enemy [10], and Suppress Replay Attack This attack is capture message that is sent from receiver to transmitter this capture cause delay [7], this attack is difficult to detect, and Interception is a passive attack it can read information that is sent from receiver to transmitter , sniffer as example it can be gathering information like MAC address [4] and this attack it can be occur from outside of user's area for example from vendors [5], and Fabrication in this type The intruder demonstrate to be the source and this attack is active attack , imitate e-mail and spoofed ip are example for fabrication attack, any information sent from source it can sent to fabrication attack and he can doing anything like modified message, packets ip, [14] . And man in the middle attack this is another example for fabrication attack that mean he can be confident to the a another user [6], then Modification, Replay Attacks in this attack The intruder receive the information and can modified it and send to destination this attack is active attack for example for this attack is virus [7].replay attack is active attack it can take copy from message that send from source to destination [7].

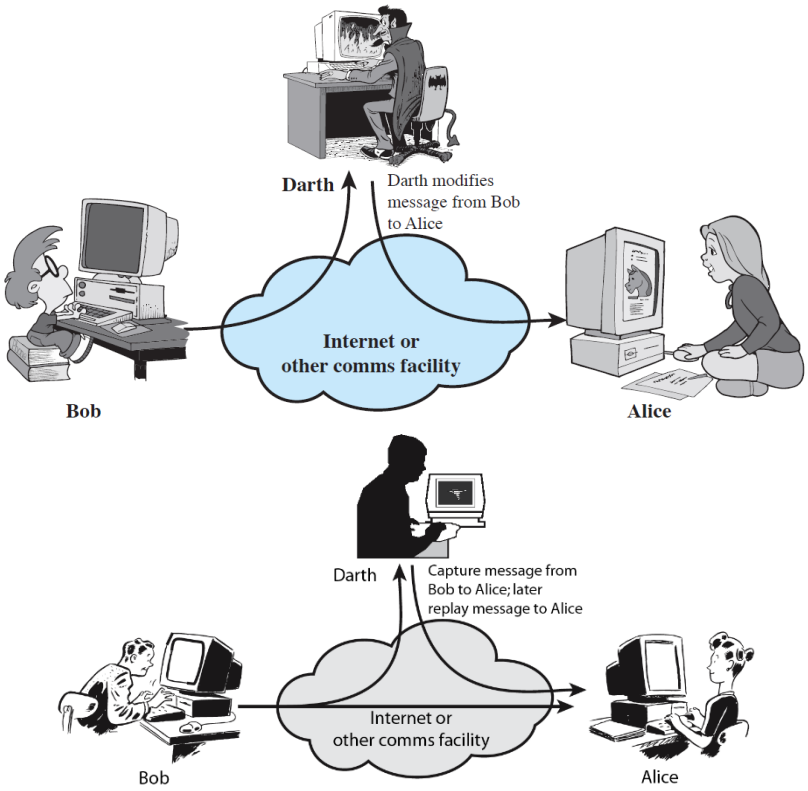

Figure 2: Active Attacks Modification of Messages and replay attack

And Interruption This attack it can block information that sent from source to destination, it is active attack examples are Denial of Service (DOS) [6] [3], finally Man In The Middle Attack It is active attack it can intercept information when the source sent information to destination or public key exchange and then retransmits to the destination [15].

2.2 Vulnerabilities in IEEE 802.16e

We here explain vulnerabilities that found in mobile WiMAX and analysis it, first unauthenticated messages the most management message sent integrity protect, it done by hash management authentication code (HMAC), but some of message is send without any authentication mechanism. like

broadcasting management message it include some vulnerabilities, then Unencrypted management communications here the hacker can listen to the traffic and collect information about BS and MS because the complete management communication is unencrypted, and Shared keys in the multi- and broadcast service here They are tow encryptions symmetric encryption and asymmetric encryption for Symmetric encryption the broadcast service in mobile WiMAX shares keys for all user group this is vulnerability because someone it can forge information .

One of Vulnerabilities in WiMAX is unauthenticated messages the most management message sent integrity protect, it done by hash management authentication code (HMAC) [11] or cipher based message authentication code (CMAC) [12], but some of message is send without any authentication mechanism. Like broadcasting management message it include some vulnerabilities, and they are many kind for unauthenticated messages.

- **MOB_TRF-IND:** Traffic Indication message (MOB_TRF-IND) this is type of broadcast and authentication management message, the BS send this message to MS to indicate to sleep MS that is traffic destined to it.. Sleep ID is content from 10 bit address for message process to be faster, the traffic message indication combine 32 sleep IDs in one sleep IDs group, that mean any sleep ID group it has 32 sleep ID, if the MS sleep the BS receive traffic for this MS and group ID for that MS sleep ID group is set true. The mobile station is wake up and receive the traffic when corresponding bit in traffic indication is set. And after verifying that the sleep indication for their group is set false, all other MS can continue sleeping. The hacker can product message to frequently MSs Wake up and can affect their battery.

- **MOB_NBR-ADV:** It is not authenticated the neighbor advertisement message (MOB_NBR-ADV). BS send message to show the feature of neighbor BS to MS for search handoff possibility. The hacker intersperse wrong data about the neighbor BS.

- **FPC:** The broadcasted Fast Power Control message (FPC) is not authentication. The power control message is sent by BS to MS or many MS to adjustment their transmitting power, if MS have low power it can tell it to increase its power and it has high power tell it to decrease its power. The adversary is set all transmitting power is maximum to all MS that effect in battery and cause some Disease for human.

- **MSC-REQ:** An unauthenticated unicast message is the Multicast Assignment Request message (MSC-REQ).when this message is sending the BS remove the MS from a multicast polling group. And any MS receive this message it can delete itself from multicast polling and send feedback to BS. It can misuse here.

- **DBPC-REQ:** The Downlink Burst Profile Change Request message (DBPC-REQ) it's not complete protect. The BS send this message to change the MSs Burst profile to more strong when the distance varies between MS and BS. It can be target for adversary misuse.

- **PMC-REQ:** Power control mode request (PMC-REQ) it send by MS itself to change it's power control mode. The BS response with power control response mode (PMC-RSP). This message can also send by BS, the PMC-REQ it can use by adversary to request a change of MSs power control mode.

- **RNG-REQ:** Range request message (RNG-REQ) must be protect by a digest when authentication key (AK) is available. Except they are another case non authentication message but a false of their carried information can be less dangerous.

- **MOB_ASC-REP:** Mobile association report (MOB-ASC-REP) this message is not authentication, BS is not straightly answer a ranging request, when BS and MS are keeping association level 2. Instead of it sending ranging request over the backbone to serving BS of requesting MS. all a ranging response of neighboring BSs are collect together by serving BS and collect together in one MOB-ASC-REP and this message is send to MS. in most case the ranging response message is protected but the MOB-ASC-REP is not. And it can happen misused by adversary he can change the information.

- **Unencrypted Management Communication:** When mobile is initial network entry it can happen conversation communication parameter and setting between MS and BS this conversation communication it can unencrypted and they are a much information exchange between MS and BS like security parameter and setting and user information etc. and adversary can listing to all this information is not encrypted.

- **Shared keys in Multi- and Broadcast Service:** Multi and broadcast service distribute message to many mobile with one signal message and economize the bandwidth and cost. Broadcast message in wimax are encrypted by one key share between all symmetrically, nd every subscriber in group have a key to decrypt message , this algorithm has a many vulnerability because any member can decrypt and verifying broadcast message and can also encrypt and authenticate message as they construct from real BS.

3. Solutions Suggested

The solution for unauthenticated message management messages it can be authentication by hash function Message Authentication Code (HMAC) or Cipher-Based Message Authentication Code (CMAC).and we can show HMAC below:

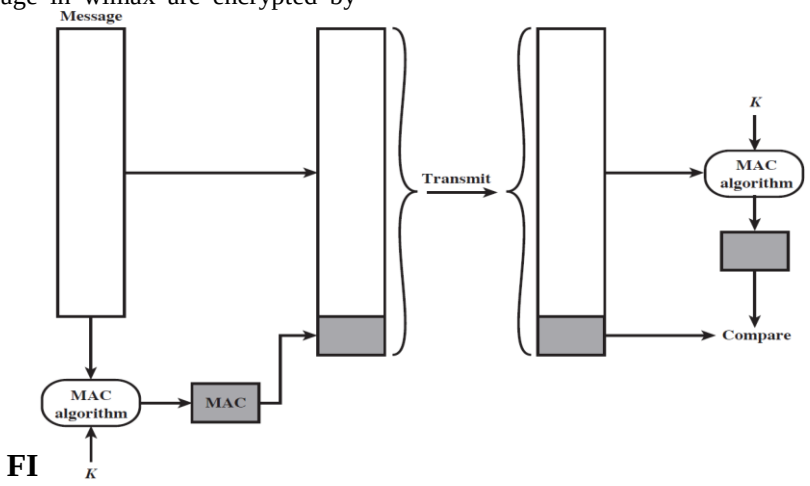

Figure 3: Message Authentication Code

Hash-based message authentication code (HMAC) provides sender and receiver each with a private and public key, but the private key is known only to that specific server and specific client. The client creates a unique HMAC, or hash, per request to the server by combing the request data and hashing that data, along with a private key and sending it as part of a request. The server receives the request and regenerates its own unique HMAC. The server compares the two HMACs, and, if they're equal, the client is trusted and the request is executed. This process is often called a secret handshake.

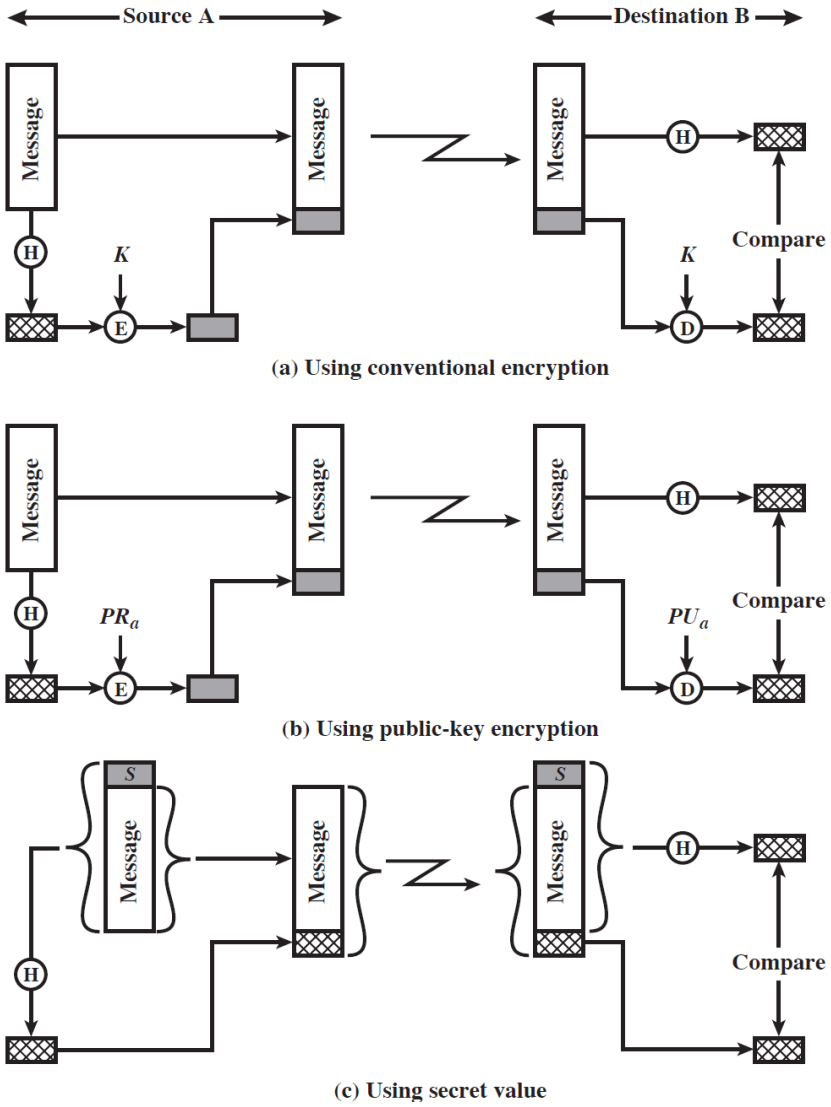

Figure 4: Encryption Methods

Consider two simple insecure hash functions bit-by-bit exclusive-OR (XOR) of every block $C_i = b_{i1}$ *xor* b_{i2} *xor . . . xor* b_{im} good for data integrity but useless for security.

Unencrypted management communication the management message it can be hack by adversary, to stop him must be encrypt the message .also authentication process using Digital Signature:
If someone want to send data to another it can encrypt by private key and the receiver can decrypt this data by public key, that mean the receiver know that data is trusted.

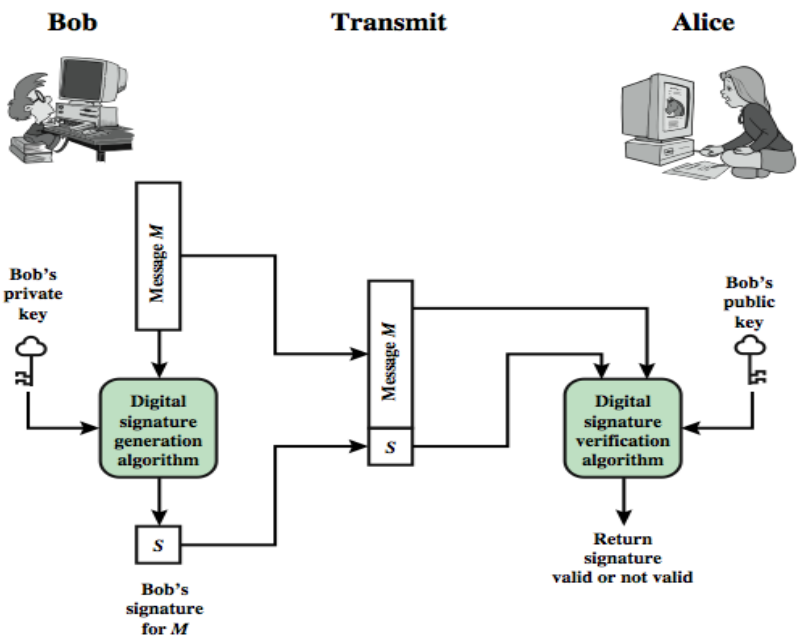

Figure 5: Digital Signature

4. Conclusion

In this paper, we showed different security vulnerabilities found in IEEE 802.16e and gave possible solutions to eliminate them. When all proposed changes are applied, the security of Mobile WiMAX can be significantly increased. Encrypting the management communication solves the Vulnerability which existed since the first version of the standard. With applied encryption an adversary is no longer able to collect management information about Mobile devices. Some messages were found which carry sensitive information without any authentication. If they are forged this can be dangerous for system operation. If the message authentication is extended to these messages as proposed, they are protected against forgery. To prevent a key misuse in the multi- and broadcast rekeying algorithm three different solutions were presented based on unicasting, asymmetric cryptography and hash function, digital signature. Generating traffic encryption keys in a hash function is a fast solution that does not introduce much Overhead. Unfortunately it has a long period without forward secrecy. Thus if forward secrecy is important one of the other algorithms might be appropriate.

References

[1] M. Barbeau, "WiMAX/802.16 threat analysis," in Proceedings of the 1st ACM international workshop on Quality of service security in wireless and mobile networks, Quebec, June 2005

[2] IEEE Computer Society and the IEEE Microwave Theory and Techniques Society," 802.16TM IEEE Standard for local and metropolitan area networks," Part 16: "Air Interface for Fixed Broadband Wireless Access Systems", June 2004.

[3] IEEE Std. 802.16e/D12, "IEEE Standard for Local and Metropolitan Area Networks", part 16:" Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE Press, 2005.

[4] 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

[5] R. M. Hashmi et, "Improved Secure Network Authentication Protocol (ISNAP) for IEEE 802.16", Proceedings of 3rd IEEE International Conference on Information and Communication Technologies, August 2009.
[6] Sen Xu,Manton Matthews, Chin-Tser Huang. "Security issues in privacy and key management protocols of IEEE 802.16",44th annual Southeast regional conference, pp. 113-118, ISBN 1-59593-315-8, 2006.
[7] Ayesha Altaf, M. Younus Javed, Attiq Ahmed, "Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005", 9th ACIS International Conference on software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp. 335-339, 2008.
[8] Sen Xu,Chin-Tser Huang,"Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions", Computer Science and Engineering Department, University of South Carolina, Columbia, September, 2006.
[9] Michel Barbeau, "WiMax/802.16 Threat Analysis", School of Computer Science Carleton University, Ontario, Canada, October 2005.
[10] Krawczyk H., Ballare M., Canetti R.: HMAC: Key-Hashing for Message Authentication, RFC 2104, http://www.ietf.org/rfc/rfc2104.txt, IETF, 1997.
[11] Dworkin M.: Recommendation for Block Cipher Modes of Operation: The CMAC mode for authentication, NIST special publication 800-38B, National Institute of Standards and Technology (NIST), MD, USA, 2005.
[12] 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
[13] Figure 2 network security essentials application and standards fourth edition for William Stallings
[14] IETF RFC 1994. PPP Challenge Handshake Authentication Protocol (CHAP) 1996.