ISSN:0975-9646

Enhanced Security for Mobile WiMAX through Secured Initial Ranging Process

[1]D. Roselin Selvarani, and [2]Dr. T. N. Ravi

[1]Department of Computer Science, Holy Cross College, Tiruchirappalli, Tamil Nadu 620002, India.
[2]Department of Computer Science, Periyar E.V.R. College, Tiruchirappalli, Tamil Nadu 620023, India.

Abstract - **WiMAX is expected to be a dominant technology for the Metropolitan Area Networks in near future as it has last mile coverage. It is a promising broadband wireless technology and possesses high data rates, quality of service, scalability, security, and mobility. Compared to fixed WiMAX, Mobile WiMAX has highly sophisticated authentication and encryption techniques but is still exposed to various kinds of attacks. This is due to the unencrypted MAC management messages used in the initial network entry of the mobile WiMAX network. Initial network entry process is an important process as it is the gate way to establish the connection between the Base Station and Mobile Station. The possible issues in this process are RNG-REQ and RNG-RSP vulnerability, Auth-Request and Invalid vulnerability and Rogue BS. In this paper, a new secured initial network entry is proposed to enhance the security of Mobile WiMAX environment. RNG-REQ attack encountered by Mobile WiMAX (IEEE 802.16e) is analyzed using NETSIM tool and experiments are conducted to analyze the impact of RNG-REQ attack in normal operations as well as under attack. The results are analyzed and it is found that secured ranging process produced better results in terms of access delay and retries. As the initial ranging parameters are highly critical, if they are not properly setup, it leads to DoS attack or poor system performance. Applications such as VoIP, Video streaming, FTP, Database etc. can be securely done using Mobile WiMAX through secured ranging process. Mobile database applications where the mobile workers / users want to synchronize the data after the completion of their task can also be done securely using this enhanced mobile WiMAX security.**

Keywords - **Mobile WiMAX, Secured Ranging, DoS attacks, RNG-REQ attack, Mobile database application, X.509 certificate.**

I. INTRODUCTION

Security is an essential requirement for the success of every communication technology. The main attempt of IEEE 802.16 is to offer more security in the network. It provides several features such as scalability, mobility, well-built security, access control, data confidentiality, robust user verification and strong Quality of Service. Many sophisticated authentication and encryption techniques have been set in IEEE 802.16 but still it is exposed to several attacks.

Worldwide Interoperability for Microwave Access (WiMAX) is a standard based technology enabling the delivery of last mile wireless broadband access as an alternative to cable or DSL. Basically it operates on two layers such as Physical layer (PHY) and Medium Access Control (MAC) layer. In WiMAX, security is implemented at the security sub layer of the MAC. Both the layers are susceptible to several attacks. The security sub layer of IEEE 802.16d standard defines the security mechanisms for fixed and IEEE 802.16e standard defines the security mechanisms for mobile network. The security sub layer supports to verify the user, authorize the user and provide encryption support for the key transfer and data traffic. IEEE 802.16e, the mobile WiMAX offers more enhancements over 802.16d. IEEE 802.16d standard security design is based on PKMv1 (Privacy and Key Management Version 1) protocol but it has major security problems. The authentication process in PKMv1 is one way process, in which BS authenticate MS but not vice versa. It leads to vulnerability and reason for many attacks. In PKMv2 protocol, it is modified as mutual authentication in which both MS and BS authenticate each other. IEEE 802.16e uses superior encryption methods and has more secure key management protocol. But still many security issues are yet to be solved.

Mobile WiMAX offers quality of services in different applications like VoIP, Video streaming, FTP, Database etc. A security enabled mobile WiMAX helps a mobile worker to gain safe network access in areas where it is traditionally not possible with wired networks. It also enables such services as wireless access for enterprise data, file and database synchronization, and convenient network access to corporate resources on the intranet. Therefore the network security becomes increasingly more vital for a successful mobile database application [1].

The remaining part of this paper is organized as follows. Section 2 reviews the WiMAX IEEE 802.16 and Mobile WiMAX IEEE 802.16e technologies. Section 3 explains the basic concepts of Mobile WiMAX. Section 4 describes the methodology of the proposed work. Section 5 analyses and discusses the results obtained and Section 6 concludes the paper.

II. REVIEW OF LITERATURE

In [2], the authors discussed the major security issues in PMP network such as DoS/Reply attacks during MS Initial network entry, Latency during handover and unsecured pre authentication, Downgrade attack, Cryptographic algorithm computational efficiency and Bandwidth spoofing. They

also focused on few other flaws such as Traffic Indication message (MOB_TRF-IND), Neighbor Advertisement message (MOB_NBR-ADV), Fast Power Control message (FPC), Multicast Assignment Request message (MSCREQ), Association Result Report (MOB_ASC-REP), Ranging Request (RNG-REQ) message.

In [3], the authors gave brief account of security issues that exist in IEEE 802.16e. They discussed the various threats that may occur at Physical and MAC layer in Mobile WiMAX. They focused on the solutions for the threats that have been proposed in various literature and shortcomings of these proposed solutions. They also proposed solution for the threat DoS. The following mobile WiMAX attacks are addressed in this paper: RNG-RSP vulnerability/DoS attack, Authorization Request and Invalid vulnerability, BS or MS Masquerading and Man in the Middle attack or eavesdropping.

In [4], the authors presented a detailed and exhaustive survey on the existing attacks and countermeasures on IEEE 802.16 technology. They classified the attacks according to the risk they imposed to the studied system such as Major, Moderate and Minor based on the likelihood of occurrence and impact upon the system. They also proposed the possible countermeasures and remedies for each category of attack. They evaluated the qualitative characteristics of each attack with reference to the specification. Seven types of attacks discussed in this paper are Ranging attacks, Power saving attacks, Handover attacks, Miscellaneous control message attacks, Attacks against WiMAX security mechanisms, Multicast/Broadcast attacks and Mesh mode attacks.

In [5], the authors discussed Privacy Key Management protocols focusing on PKMv2 which has been proposed after publication of IEEE 802.16e. They explained the attacks found in PKMv2 and the possible solution for these attacks. The main objective of this paper is to analyze the security mechanism in authentication protocol. They considered 3 attacks namely repeated attacks, Forgery and Juggle Attacks and man in the middle attack and made a comparative study between PKMv1 and PKMv2.

In [6], the authors investigated and provided a comparative study of existing security protocols over mobile WiMAX and discuss how they achieve better security against various types of security threats.

In [7], the authors provided solution to the initial network entry process by using elliptic curve Diffie-Hellman key exchange algorithm which is faster than the Diffie-Hellman key exchange algorithm. It improves the performance of IEEE 802.16. The authors also discussed the three possible threats in the initial network entry process such as RNG-RSP vulnerability, Auth-Request and Invalid vulnerability and Rogue BS. The proposed solution not only solves the RNG-RSP vulnerability but also authentication vulnerability.

III. BASIC CONCEPTS

A. Protocol Stack

The protocol stack of IEEE 802.16 standard contains two main layers such as Medium Access Control (MAC) layer and Physical (PHY) layer. The MAC layer is further subdivided into three sub layers, namely Convergence Sub layer (CS), Common Part Sub layer (CPS) and Security Sub layer (SS). The service specific CS communicates with higher layers and receives packets from them and then does some specific functions like packet/frame classification and header suppression. Next, it encapsulates these packets into MAC Service Data Unit (MAC SDU) format, and then distributes MAC SDUs to common part sub-layer. Asynchronous Transfer Mode (ATM) convergence and packet convergence sub-layers are two types of service specific convergence sub-layer. The ATM convergence sub-layer is used

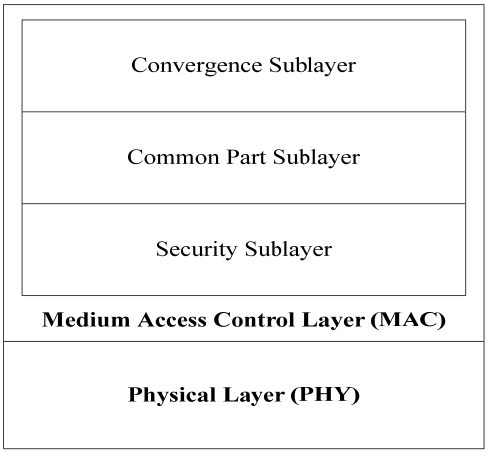

Fig.1. Protocol Stack of WiMAX

for ATM networks, and the packet convergence sub-layer is used for packet services like Ethernet, IPv4 and IPv6. The responsibilities of the CPS are bandwidth allocation, connection management, scheduling, connection control, automatic repeat request and QoS enforcement. The main purpose of security sub layer is to provide authentication, authorization and secured key exchange. It is also used for encryption and decryption of data from the MAC layer to PHY layer and vice versa. Encapsulation and PKM protocols are the two important protocols used in SS. Encapsulation Protocol is used for ciphering operations on data in the networks. PKM protocol is used for secure key distribution between BS and MSs. It also allows the BS to enforce conditional access to network services. The PHY layer receives MAC frames and then transmits them through coding and modulation of radio frequency signals. It supports Frequency Division Duplexing (FDD) and Time Division Multiplexing (TDM).

B. Initial Network Entry Process

Initial Network entry is a procedure which is to be followed by MS to enter into the network and to get the network services. It consists of four processes such as (i) initial ranging process, (ii) MS basic capability negotiation process, (iii) PKM authentication process and (iv) registration process. The steps for initial network entry process are given below:

Step 1: When MS is powered on, it first scans the downlink channel to determine whether it is currently in the coverage of BS.

Step 2: Each MS stores a list of optional parameters, such as DL frequency. MS synchronizes with the stored DL frequency of most suitable BS.

Step 3: Once the DL synchronization is completed, MS can listen to the various control messages from which it obtains the UL parameters. Based on these UL parameters, MS decides whether the channel is suitable or not.

Step 4: If the channel is suitable MS performs 5^{th} step, otherwise it goes back to the step 1.

Step 5: *Ranging Process:* Ranging is the process to acquire timing and power level adjustment to maintain the UL connection with the BS. To perform initial ranging, MS send a RNG-REQ message to the BS with CID parameter.

Step 6: In response to this message, BS sends the RNG-RSP message to the MS with the basic and primary CID.

Step 7: *Basic Capability negotiation Process*: MS sends the SBC-REQ (Subscriber Basic Capability Request) message to the BS through which MS informs the BS about its basic capabilities in terms of PHY Parameters and Bandwidth Allocation.

Step 8: When BS receives this message, it responds with the SBC-RSP message consisting of the parameters required for the UL and DL transmission.

Step 9: After negotiating the basic capabilities, *authentication* and key exchange process will be performed.

Step 10: Once the key exchange process is completed, MS *registers* itself with the BS, for which it sends the RNG-REQ message to the BS.

Step 11: In response to this message, BS sends the RNG-RSP message to the MS. When MS receives this message, it can obtain the IP address.

Step 12: Finally the service flow will be established, which is either initiated by the MS or BS.

C. Attacks on IEEE 802.16 e Mobile WiMAX

Security issues occur only in 2 layers namely Physical and MAC layers in Mobile-WiMAX (IEEE 802.16e). Scrambling and Jamming are two threats at Physical layer. MAC layer encounters many threats, presented under review of literature, among which the initial network entry is the very important issue to be considered as it is the first step to create a connection between BS and MS. This paper focuses only on RNG-REQ attack.

1) *Ranging Attacks*

RNG-REQ message is sent from MS to BS in order to request the BS to permit the MS to join the network. RNG-RSP message is used to respond to the RNG-REQ message which contains basic and primary CID (Connection Identifier) for the MS, information about RF power level adjustment, offset frequency adjustment and timing offset corrections. These two ranging messages are not encrypted and hence the attacker can easily access it and modify it accordingly. In RNG-RSP attack, the attacker can modify this message and set the status as failed and then resend this message to the MS. Therefore the MS has to go again for initial ranging. If an attacker captures the RNG-RSP message again and again with the status providing as failed, the victim MS cannot join the network and it leads to the DoS (Denial of Service) attack.

A. RNG-REQ Attack

After obtaining UL and DL parameters, MS will try to get the correct timing offset and power adjustment through the process of ranging. To find the initial ranging interval, MS will use the information contained in UCD or UL-MAP message.BS allocates initial ranging interval consisting of many Transmission Opportunities (TO). For single carrier and OFDM PHY, the MS shall construct RNG-REQ message. Then MS can transmit the RNG-REQ message in one of the known TO. Typically, there are only 3 TO in a 5 ms frame. Therefore there is a high possibility of collision to occur. In order to reduce the collision, the 802.16 specification dictates that the nodes should pass a period of inactivity of random duration known as Backoff (BO). If the RNG-RSP message does not arrive to the device before the expiration of the timer T3, MS will understand that a collision occurs. By default, T3 is set to 200ms. After a random waiting time, the collided nodes will try to resend the RNG-REQ message. The waiting time interval will be doubled, until a maximum value is reached. As long as MS collides, this process will be repeated until the defined maximum number of retries. This process is called Truncated Binary Exponent Backoff (TBEB).

In RNG-REQ attack, an attacker may produce a large number of forged RNG-REQ messages with different values each time and concurrently transmit them to the target-BS in order to waste its resources. To respond to these fake messages, BS did a multi-step process which contains the allocation of Basic and Primary management CIDs, deciding whether the signal is good enough or any adjustments are necessary, constructing a RNG-RSP message etc. This unnecessary task creates much stress on BS. When many attackers join together and do this attack, it causes maximum burden to the BS which in turn results in lower quality of service or even Distributed DoS for all legitimate MSs connected to this BS. When the attacker attempts this type of attack, he/she may affect the system in many ways such as (i) artificially increases the number of collisions in the network, (ii) imposes burden on the BS by forcing it to conduct the ranging process for a large number of virtually non-existing MSs, and (iii) tricks the BS into ranging and then committing bandwidth and CIDs to MSs.

IV. METHODOLOGY

A. Secured Ranging process using X. 509 certificate

The RNG-REQ message is the first message sent by a MS to BS requesting transmission time, power, frequency and burst profile information before joining the network. This initial message is neither encrypted nor verified for authentication which makes it vulnerable to interception and modification to the least effective settings for the MS leading to degrading or denying the service to the MS. In order to solve this problem, a new secured ranging process using X.509 certificate is designed.

1. BS → MS: UL-MAP(Initial ranging Interval)
2. MS→BS:RNG-REQ(Enc(Cert MS, selected ranging codes) PKBS)
3. BS → MS: Enc (RNG-RSP) PKMS

The MSs should be installed with X.509 certificate of the required Base station (Cert BS). MS sends the selected ranging codes and Cert MS encrypted with Public key of the BS, retrieved from Cert BS. Then the BS sends the subsequent messages encrypted with Public key of the MS. If MS moves from one station to another station by means of soft handover and identifying the BS through GPS, the corresponding BS's X.509 certificate can be updated automatically, as the communication is done through a secured channel. This secured ranging process is incorporated with Authorization key and Key Generation Key and Traffic Encryption key right from the management messages.

To implement this concept, software is designed using VC++. NETSIM is used to create a mobile WiMAX environment to understand the behaviour of the network during the normal mode (a situation where there is no attack), and under attacks.

The following scenario is considered to evaluate the impact of RNG-REQ attack: A number of MSs that have been arrived during the Uplink Channel Descriptor (UCD) interval are cleared to enter contention for initial ranging process. The simulation is conducted for a time frame of 5 sec but the attacker attacks only during the first second of the ranging process. As the Back Off (BO) window size is very small and the probability of collision is large, this interval is taken in real attack conditions. During this interval the attacker is transmitting an RNG-REQ message on every single transmission opportunity of every frame. In this simulation environment the initial ranging process is evaluated in Normal mode and Under attack. The behavior of the network in terms of access delay and number of retries is considered under different number of contenting mobile nodes.

TABLE 1 PARAMETERS USED IN SIMULATION

Parameter	Value
Frame duration	5 ms
Initial BO window	8
Final (Max) BO window	1024
UCD interval	5 ms
Timer (T3)	200ms
Simulation duration	5 Sec

As a result of this attack all contending MSs are collided and progressively set their BO window to a very high interval. This has an immediate effect in the access delay subsequently. The total number of RNG-REQ messages transmitted by the attacker in 1 sec period of attack is not more than 600 messages with total traffic about 96 Kbps.

V. RESULTS AND DISCUSSIONS

TABLE 2 ACCESS DELAY VS NO. OF NODES

No. of Nodes	Average Access Delay Normal Mode(mS)	Average Access Delay Under Attack (ms)	
		Initial Ranging process	Secured initial Ranging process
5	112	205	115
10	201	298	206
15	307	410	315
20	416	536	426
25	515	645	530
30	628	736	646

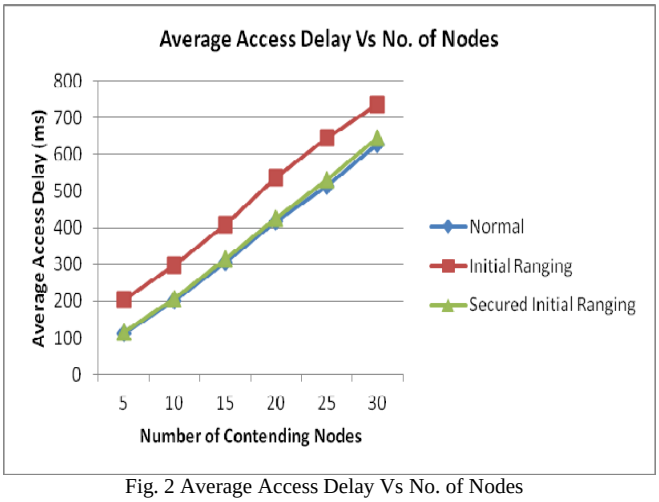

Fig. 2 Average Access Delay Vs No. of Nodes

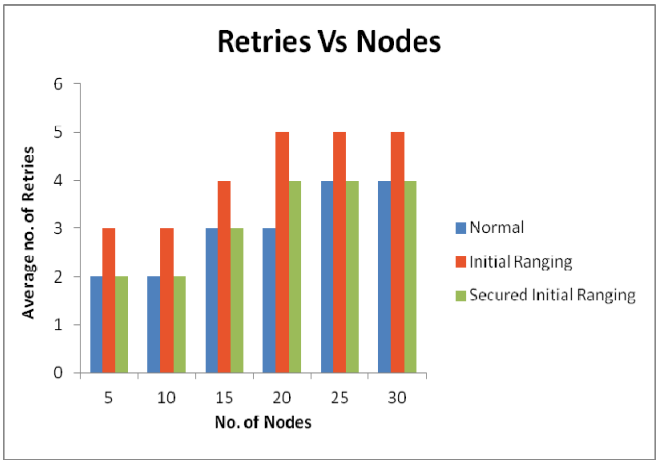

Fig. 3 Average no. of Retries Vs No. of Nodes

Fig. 2 and Fig. 3 illustrate that the average access delay and the average number of contention retries against the different number of contending nodes in both scenarios. This type of attacks will force many MSs to disconnect simultaneously and after that this large number of MSs will attempt to reconnect performing initial network entry. Ultimately, this will result in a large number of MSs contending for a small number of TO in the Initial Ranging step, which is actually the bottleneck of the whole initial network entry process.

From the result obtained in table 2, it is clear that the average access delay by different number of contending mobile nodes under attack is much higher than the average access delay by different number of contending mobile nodes under Normal operation. It is observed that average access delay using Secured initial ranging process is lesser compared to the general initial ranging process where the messages are transmitted in plain text.

TABLE 3 RETRIES VS NO. OF NODES

No. of Nodes	Average No. of Retries Normal Mode	Average No. of Retries Under Attack	
		Initial Ranging Process	Secured Initial Ranging Process
5	2	3	2
10	2	3	2
15	3	4	3
20	3	5	4
25	4	5	4
30	4	5	4

From table 2, it is clear that the average number of contention retries against the different number of contending nodes under attack is more than the average number of contention retries against the different number of contending nodes under Normal operation. It is observed that average number of contention retries using secured initial ranging process is lesser than the initial ranging process with plain text.

VI. CONCLUSION

WiMAX has sophisticated features compared to other wireless technologies. With all the advantages it holds, if it has security issues, it cannot be used reliably. So the attacks on Mobile WiMAX are focused in this paper and RNG-REQ DDoS attack is analyzed. Further X.509 certificate based secured ranging process is designed and implemented to check the effect of RNG-REQ attack using NETSIM. It is found that the Secured ranging process produced better result. The impact of RNG-REQ attack in terms of access delay and retries is reduced to an extent and thus security is enhanced in Mobile WiMAX.

REFERENCES

1. Sanket Dash, Malaya Jena, “In the Annals of Mobile Database Security”, CPMR Interntional Journal of Technology, Volume 1, No. 1, December 2011.
2. Gaurav Soni, Sandeep Kaushal, “Analysis of Security Issues of Mobile Wimax 802.16e and their Solutions”, IJCCR, Vol.1, Issue 3, Manuscript 3, November 2011.
3. Reena Dadhich, Geetika Narang, D.M.Yadav, “Analysis and Literature Review of IEEE 802.16e (Mobile WiMAX) Security”, International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-3, Page No. 167 – 173, February 2012. ISSN: 2249 – 8958.
4. Constantinos Kolias, Georgios Kambourakis and Stefanos Gritzalis, “Attacks and Countermeasures on 802.16: Analysis and Assessment”, IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, Pages 487-514, First Quarter 2013.
5. Kamran Sameni, Nasser Yazdani, Ali Payandeh, “Analysis of Attacks in Authentication Protocol of IEEE 802.16e”, International Journal of Computing and Network Technology, No. 1, PP. 33-44, 2013.
6. Rajesh Yadav, Dr. S. Srinivasan, “Analysis of Security Protocols in Mobile Wimax”, International Journal of Engineering Research & Technology, Vol. 3 Issue 12, December-2014, ISSN: 2278-0181,
7. Pranita K. Gandhewar, Prasad P. Lokulwar, “Improving Security In Initial Network Entry Process Of IEEE 802.16”, International Journal on Computer Science and Engineering (IJCSE), Vol. 3, No. 9, September 2011, pp 3327-3331, ISSN : 0975-3397.