Security Problems in Mobile Wimax Networks

Rajesh Yadav
Computer Science and Engineering
Mewar University
Chittorgarh, India
r_yadav2in@hotmail.com

Dr. S. Srinivasan
Master of Computer Applications
P.D.M. College of Engineering
Bahadurgarh, India
dss_dce@yahoo.com

Abstract—***Mobile Wimax is much anticipated broadband wireless mechanism because of its capability to provide high-speed connectivity over long distances thereby making it useful for telecommunications service providers and Internet users. As a Broadband Wireless standard it has security issues which must be addressed. This paper describes the security vulnerabities and attacks in Mobile wimax.***

Keywords- Mobile Station, Base Station, Wireless Networks.

I. INTRODUCTION

Mobile Wimax is a new technology which has all the feature in order to be used increasingly in the near future due to its high speed capabilities. Security for Mobile Wimax is an area that needs to be focused upon so as to protect its functionality. Mobile WiMAX systems are based on the IEEE 802.16e-2005 standards which involve a physical (PHY) layer and the medium access control (MAC) layer for broadband wireless access systems operating at frequencies below 11 GHz. A Mobile WiMax/802.16e wireless access network consists of two main entities i.e. base stations (BSs) and mobile Stations (MSs). The role of Base stations is to provide network attachment to the Mobile stations. While initiating the communication process, a MS selects that Base station which offers the strongest signal. In this approach, the subscriber plays the role of the user while a BS and a collection of served MSs play the role of system [1]. Section 2 gives the detailed information about the Security Vulnerabilities and their classification whereas Section 3 throws some light on attacks followed by the conclusion section.

II. SECURITY VULNERABILITY IN MOBILE WIMAX NETWORKS

A. Physical Vulnerabilities

In this case we consider (in public and hostile environments) link attacks ranging from passive eavesdropping to active interfering, Mobile Wimax network provides efficient functionality without any fixed infrastructure. It creates demand for developing those security protocols which are simply flexible and scalable [2].

1) Attacks on Secrecy and Authentication

a)Eavesdropping: Eavesdropping occurs when there is unauthorized interception of a communication which is private. Eavesdrop term is actually derived from the sense of standing under the eaves of a house, listening to conversations happening inside. Privacy is the area which faces it as a common attack. Communication information can be discovered by snooping to that data. Whenever control information about network configuration is being conveyed through traffic, the eavesdropping attack can act efficiently to affect the privacy protection [3].

b) *Replay:* This attack is being observed whenever a stream of messages is being copied by the attacker between two parties and the stream is being replayed to one or more of the parties.

c) Node Replication Attack: These attacks are those type of attacks in which a node is being compromised, its secret cryptographic key material is used by the attacker to create clones of it in order to populate the network. During this attack, packets can be wrongly routed or they can be corrupted, thereby leading to network disconnection. The attacker can easily manipulate a specific network segment by the process of disconnection [4].

d) *Traffic analysis:* During this process, the messages are intercepted and examined so as to deduce information from patterns in communication. It is being done even when the messages are encrypted and cannot be decrypted.

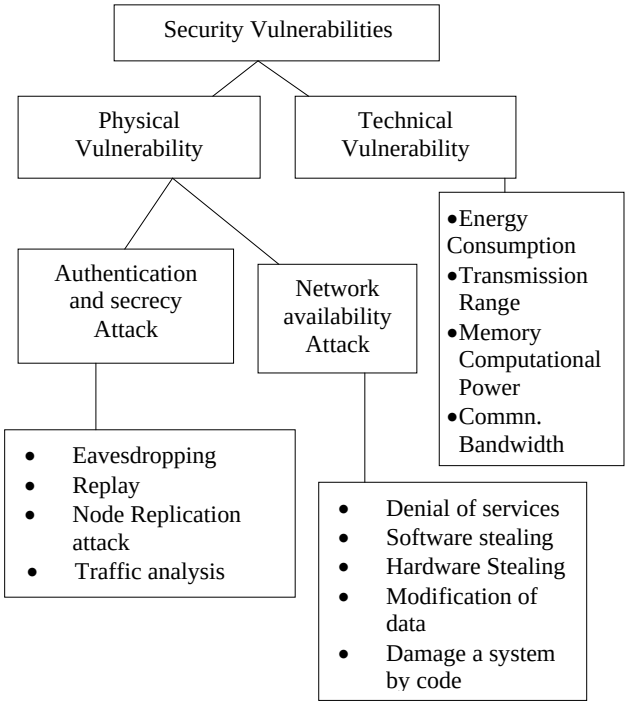

Fig 1: Security vulnerability in Mobile Wimax network

2) Attacks on network availability

These are referred to as denial-of-service (DoS) attacks. DoS attack refers to an attacker policy to disrupt, subvert, or destroy a network. Moreover, a DoS attack can turn into an event for eliminating capacity of network for doing it functions [5].These include Software Stealing, Hardware Stealing, Modification of data, Damage a system by code.

B. T echnological Vulnerabilities

Constraints like Energy Consumption, Transmission Range, Memory, Computational Power, Communication bandwidth must be focused upon in Mobile Wimax Network as technological vulnerabilities.

III. SECURITY ATTACKS IN MOBILE WIMAX NETWORKS

In comparison to any other wireless network, Mobile Wimax network faces many different attacks, which can be categorized as Layer wise and Type wise.

1) Layer Wise

In case of layer wise working, frequency selection, carrier frequency generation, signal detection, modulation, data encryption are the responsibilities of physical layer [6]. Data link layer performs Data streams multiplexing, data framing, medium access control, error control [7]. The network layer performs the job of routing. The transport layer does data delivery to application process on host machines. The application layer is basically responsible for communicating applications between different machines. Layer wise attacks are shown in fig. 2.

<table>
<tr><th colspan="2">Layer Wise</th></tr>
<tr><td>Physical:
• Jamming
• Interception
• Eavesdropping</td><td>Data Link:
• Traffic Analysis
• WEP weakness
• Sybil</td></tr>
<tr><td rowspan="2">Network:
• Wormhole
• Sinkhole
• Black hole
• Flooding
• Node capture
• Spoofing/misdirection</td><td>Transport:
• Session Hijacking
• Syn. Flooding</td></tr>
<tr><td>Application:
• Overwhelm
• Repudiation</td></tr>
</table>

Fig 2: Layer wise attacks

a) Physical layer attacks

Jamming:

In this case the actual traffic is jammed by overwhelming frequencies of illegitimate traffic thereby denying service to authorized users.

Interception:

These are the attacks which works against the network availability by overloading the server so that it stops responding. Moreover service access is also blocked in this case because the intermediate network or network device can be overloaded.

Eavesdropping:

It is also known as sniffing attack and it is the one in which the attacker has the objective of getting entered into communication which is private using network monitor or dsniff utility.

b) Data Link layer attacks

Traffic analysis:

During this process, the messages are intercepted and examined so as to deduce information from patterns in communication. It is being done even when the messages are encrypted and cannot be decrypted.

WEP Weakness

Changing keys periodically is sometimes forgotten by users when they use WEP thereby making it easy for attackers to get access to the information.

Sybil attack:

In this type of attack identities are being forged and an unknown station claims multiple identities. The attacker can use the network to act maliciously by disrupting network communication or simply stealing the information.

c) Network layer attacks

The network layer in Mobile Wimax network faces different attacks like Wormhole, Sinkhole, Black hole, Flooding, Node Capture, and Spoofing/Misdirection.

d) Transport layer attacks

Session hijacking:

It is a type of attack in which a user session is hijacked in case of a protected network. It commonly happens through IP spoofing in which source routed IP packets are used for inserting commands between communications of two stations and presenting an image of itself as an authenticated user.

Sync flooding:

It actually belongs to the family of DOS attack. It involves sending SYN packets in repetition using IP addresses which are fake. The server sends SYN-ACK message. The station sends SYN requests, but does not send any ACK messages thereby making the server slow or unresponsive.

e) Application layers attacks

Overwhelm:

In the situation of Overwhelm attack, stations are being overwhelmed by the attacker which causes the network to forward large traffic volume to base station. As a result Station energy and network bandwidth are consumed very fastly.

Repudiation Attacks:

When this attack happens, the information looks invalid or misleading. Through this attack the attacker can change the authoring information so as to log wrong data to log files.

2)Type Wise

It includes active network attacks, insider exploitation, passive communication monitoring, close-in attacks, and attacks which comes because of service provider. Type wise attack is shown in fig. 3. It is categorized as Active attack and Passive attack.

Type Wise:	
Active: • Sinkhole • Flooding • Jamming • Wormhole • Fabrication • Hello flood • Impersonation • MITM • Selective forwarding	Passive: • Traffic Monitoring • Eavesdropping • Traffic Analysis

Fig 3: Type wise attacks

a) Active Attack

In such an attack, secured systems are being bypassed or breached by attacker. This is made possible using Trojan horse, worms, viruses. The objective of this attack is to enter malicious code in order to steal information by breaking into protection features.

Sinkhole:

It is an attack in which the base station is prevented from having correct and complete information about transmission with mobile stations. In a Sinkhole attack [8] a compromised station attempts to have complete or maximum traffic from a specific area, by creating an attractive image of itself to nearby stations. Due to this all traffic that was supposed to have base station as it destination is attracted by attacker.

Flooding:

In this attack network traffic is flooded to affect service. Requests are being flooded in to the network making the server unable to deal with genuine requests also. Memory buffer of server is filled so that further connections cannot be made thereby resulting into denial of service. Flooding attack can be achieved either by using RREQ or Data flooding [9].

Jamming:

In case of jamming attack, the legitimate traffic is jammed by overwhelming frequencies of illegitimate traffic thereby authorized users are denied.

Wormhole:

It is such type of attack in which attacker follow a strategy to let them into the network with the purpose of hearing the network information and can also go for wireless data recording [10].

Fabrication:

Through fabrication fake routing messages are generated. It is not easy to detect this attack as they appear as correct routing constructs majorly in the situation of fabricated routing error messages claiming that neighboring stations are unreachable [11].

Hellow Flood:

This attack smartly makes use of HELLO packets as a tool for dealing with stations in mobile wimax network. High processing power and high radio range capable attacker transmits HELLO packets to different Mobile stations thereby convincing the neighboring stations that it is not an attacker, it is actually their neighbor. As a result the victim stations can route the information through the attacker which was supposed to be sent to base station, so they are spoofed by the attacker [12].

Impersonation :

No authentication mechanism is so much capable of protecting the mobile wimax network from malicious entities. In order to possess identity and hiding into the network, the attacker makes use of MAC and IP spoofing. It is also known as spoofing attack [13].

Man in middle Attack:

An attacker lets itself between the communicating parties i.e. sender and receiver and it starts sniffing every information content which is being shared between the two. Moreover the attacker can also masquerade sender for communication with receiver or masquerade receiver to reply to sender.

Selective Forwarding:

In this category of attack, malicious stations can simply refuse for packet forwarding or they can also drop packets in order to ensure that they are not propagated further. So as to avoid any detection the attacker can drop selected packets coming from some selected nodes and remaining packets will be forwarded [14].

b) Passive Attack

This category of attack tries to explore unencrypted traffic and finds clear-text passwords, sensitive information so as to use the same in other attack types. Information or data files will be disclosed to the attacker without letting the user know about it through passive attacks.

Traffic Monitoring:

It can be done with clear objective of knowing about communicating parties and to be aware about their functionalities, such information can be utilized for happening of further attacks.

Eavesdropping:

In this type of attack, unknown receiver intercepts and read the message conversation. Wireless communication majorly uses RF spectrum and its broadcasting nature makes it easy to eavesdrop transmitted messages and fake message can be put into the Mobile wimax network.

Traffic Analysis:

This attack serves the objective of gaining network information on which mobile stations communicate and also to have an idea of finding out the volume of data to be processed.

CONCLUSION

The deployment of Mobile Wimax becomes difficult as it comes with different vulnerabilities and attacks and proper attention is to be given to this network environment. In this paper, we have analyzed security vulnerabities and attacks in Mobile wimax network. As there are different category of attacks so it is required to have proper solution which works against each category of attack.

REFERENCES

[1] Gaurav Soni, Sandeep Kaushal," Analysis Of Security Issues Of Mobile Wimax 802.16e And Their Solutions", International Journal of Computing and Corporate Research, Volume 1 Issue 3 Manuscripts 3 November 2011.
[2] Deepali Gawali, Shweta Bagul, Omkar Kulkarni, Dr.B.B.Meshram, "Survey on Vulnerabilities in Wimax", International Journal of Computer Application, Issue2, Volume 2 (April 2012).
[3] Deepti, Deepika Khokhar Satinder Pal Ahuja," A Survey of Rogue Base Station Attacks in Wimax/Ieee802.16", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 1, January 2012.
[4] Pfitzmann, M. Kohntopp, Anonymity, unobservability and pseudonymity – a proposal for terminology, in: Hannes Federath(Ed.), Designing Privacy Enhancing Technologies, Lecture Notes in Computer Science (LNCS), vol. 2009, Springer-Verlag, 2001.
[5] Tao Han, Ning Zhang, Kaiming Liu; Bihua Tang, Yuanan Liu,"Analysis of mobile WiMAX security: Vulnerabilities and solutions, Mobile Ad Hoc and Sensor Systems", 5th IEEE International Conference, Sept. 29 2008-Oct. 2, 2008.
[6] Sanjay P. Ahuja, Nicole Collier," An Assessment of WiMax Security", Journal of Scientific research, May 2010.
[7] D. David NeelsPon Kumar, Praveen David, S.Rimlon Shibi, K.Arun Kumar, "Security Enhancement for Mobile WiMAX Network" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
[8] Jin Cao, Maode Ma, Ariff,"Security enhancements in WiMAX mesh networks", Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on 28-30 Oct. 2011.

[9] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy,"A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks", Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[10] Sharanbeer Kaur ,Shivani Khurana,"WiMAX -WLAN Interface using TORA, DSR and OLSR protocols with their evaluation under Wormhole Attack on Voice and HTTP Applications", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, Volume 16, Issue 3, Ver. IX (May-Jun. 2014), PP 80-86 www.iosrjournals.org.

[11] A.K.M. Nazmus Sakib,"Security Enhancement & Solution for Authentication Frame work in IEEE 802.16",International Journal of Computer Science & Information Technology (IJCSIT), Vol 2, No 6, December 2010.

[12] Biswas and Md. Liaqat Ali,"Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology? Sweden, 22nd March 2007.

[13] Mitko Bogdanoski, Pero Latkoski, Aleksandra Risteski, Borislav Popovski," IEEE 802.16 Security Issues: A Survey", 16th Telecommunications forum, Telfor 2008, Serbia, Belgrade, Nov. 25-27, 2008.

[14] Gharge D. M., Dr.Halse S. V. Dr.Jagtap S. B.," Forward Selection Call Admission Control with Intrusion Detection System in IEEE 802.16E WiMAX Network", International Journal of Computer Science and Communication Engineering Volume 2 issue 4(November 2013 issue).