ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

A Review of WiMax / 802.16 Security Threats

Shikha[1], Vijender Kaushik[2]

Department of Computer Science, Mewar University, Mewar[1]

Department of Computer Science, IMT, Gaziabad[2]

Abstract: This paper reviews the various security threats at physical layer and MAC Layer in WiMax/802.16. The various masquerade attacks are discussed in this paper. the risk analysis is performed and problems still exists is discussed in the paper which help in further research work.

Keywords: IEEE 802.16, WiMAX, wireless network, threat analysis, vulnerabilities analysis, security, network security, PKM, PKMv2, authentication, encryption, man-in-the-middle attacks, DoS attacks, WiMAX attacks.

I. INTRODUCTION

The development of wireless communication arrangement is more rapidly than any of the communication technologies. Now days, people are in habit of using wireless network than wired network. The requirement of using network in public area is growing. For the wide area network range, Installation of wireless network is cost effective solution than wired technology.

In personal area network (PAN), the Infrared Data Association (IrDA) and the IEEE Standard 802.15, which are also called Bluetooth, technologies can replace the Universal Serial Bus (USB) and FireWire with limitation in speed and distance.

The IEEE 802.11 WLAN standard, also popular as Wi-Fi, has been established for wireless networks at local area. The IEEE Standard 802.11b is the broadly conventional standard and presently the leading standard for WLANs. It operates in 2.4 GHz band and supposedly supports up to 11 Mbps speed. Two other familiar standards in the IEEE Standard 802.11 family are 802.11a and 802.11g. Both of them provide a high-speed WLAN standard with a hypothetical maximum speed of 54 Mbps. The IEEE Standard 802.11a operates in the 5 GHz band, whereas the 802.11g does in the 2.4 GHz band. However, the area covered by the standard is still limited because of the standard aims to be used in LANs.

The popularity of wireless network is rising day by day. For the metro range wireless network, it has need of a many Wi-Fi access points. Then a new standard IEEE 802.16 has been shaped for metropolitan area networks (WMANs) which is popularly known as WiMAX [1]

The IEEE Standard 802.16 describe a medium access control (MAC) layer and physical layers. The medium access layer is divided into three sub layers namely convergence sub layer, common part sub layer and a privacy sub layer. The IEEE 802.16 standard functions in the frequency bands of 2.66 GHz. The standard defines two operation modes which are called as point-to-multipoint (PMP) and Mesh modes.

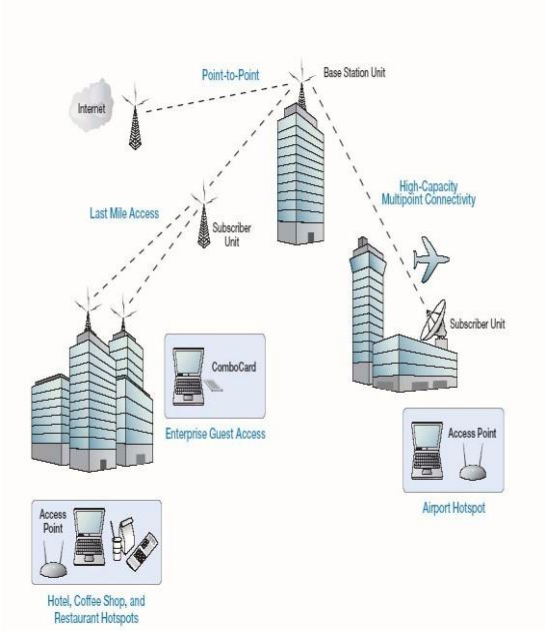

Figure 1: 802.16 standard WiMax comprehensive, secure and manageable wireless networks

II. RISK ANALYSIS

The peril of attack is evaluated by impact factor which specify the effects of an attack. This impact may be classified as Low, Medium or High. When there are reversible/repairable actions, the service trouble is tiny or the number of clients influences a minimal, then impact is defined as 'Low'. A 'Medium' impact has a considerable loss/trouble of usage over a period of time. In terms of users influence it can have an effect on only one user. The impact factor is medium in terms of system influence as the outage is controlled. A medium impact may origin some degree of financial hinder.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

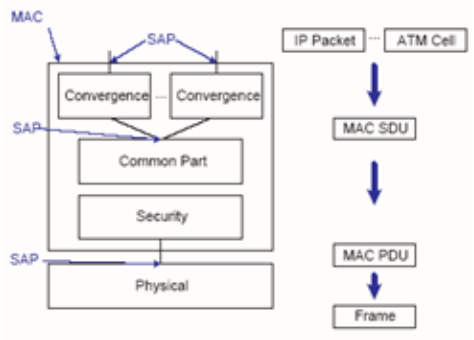

Figure 2: WiMax layered architecture

The impact is defined "High' when the loss of system usage is over a considerable length of time to a single user, defined as long to the organization. A long outage of the system is high also. There may be numerous unable to access the system, severe financial loss and/or illegal offences [2].
Risk values may vary according to the author of the analysis and information available to the author. Additional prominence could be focused on countermeasures/after effects for threats which require main concern. The MAC layer and Physical layer security threats are studied in this paper.

III. PHYSICAL LAYER THREATS

Ignores the bursts it cannot demodulate. Since the security sub-layer is above it, the physical layer is unsecured (as pictured in Figure 3). WiMax/802.16 is vulnerable to physical layer attacks such as jamming and scrambling [3].

Jamming is an interruption of the frequency such as intense noise. It can either be accidental or intended. Resistance to jamming can be increased by raising the signal frequency or intensifying the bandwidth using precise spreading techniques via sequence spread spectrum and frequency hopping. Increasing the power of the signal can be achieved easily by means of using a more powerful transmitter or a high gain transmission antenna and a high gain receiving antenna [4].

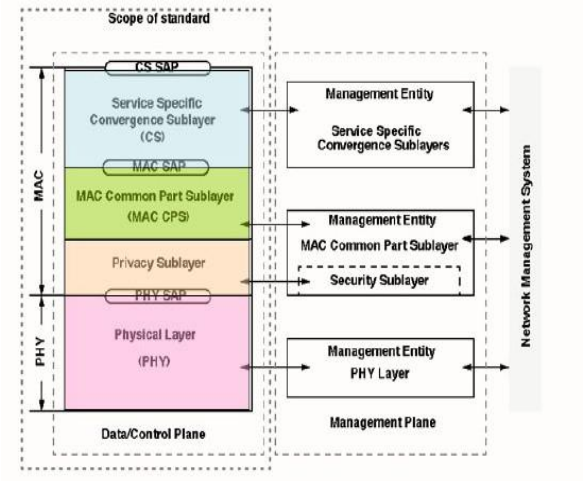

Figure 3:- IEEE 802.16 MAC and Physical layer.

Scrambling happens for small time period and is focused to certain frames or parts of frames. Scramblers is similar to jamming can intently effect control or management information with the rationale of disturbing the networks normal operation. This is of grave concern for time sensitive messages which do not have built in time delay. Examples of this are channel measurement reports requests or responses. Intentional scrambling of data traffic of particular users can cause them to retransmit. Though intended scrambling is more complex than jamming, the probability for scrambling to occur is possible due to natural noise interruption and the availability periods of the attack. These attacks can be unveiled by analyzing discrepancies in the systems performance [5].

The risk of scrambling is low in comparison to jamming because the attacker has to interpret control information and involves sending noise over the network at specific time interval. The impact of scrambling is low nevertheless results are reversible for example, by retransmission. Jamming is easier to detect, in comparison to scrambling, with the use of a radio spectrum monitoring equipment.

IV. MAC LAYER THREATS

We examine the MAC layer threats with respect to confidentiality and authentication. In eavesdropping, management messages (never encrypted) can provide valuable information to an attacker (e.g. to verify the presence of a victim at its location before perpetrating a crime). They can be intercepted by a passive listener within communication. There are no serious technical difficulties to resolve by an attacker. It is likely to occur. From the user perspective, eavesdropping of management messages may result in limited financial loss, if it results in the execution of a crime. From the point of view of a system, eavesdropping in itself may not create outages. Hence, eavesdropping of management messages is a critical threat for users and a major threat to a system. Eavesdropping of traffic is a minor threat and there is no need for countermeasures.

IV. THREATS AND VULNERABILITIES

WiMAX is a network that is based on the Internet Protocol and wireless or not, it is subject to the vulnerabilities of any IP network. A denial of service (DOS) attack by a malicious hacker can cripple any network, and precautions such as vigilant intrusion detection must be taken by IT professionals. Certain applications like VoIP come with their own vulnerabilities. VoIP security threats can take the form of eavesdropping, session hijacking, SPIT, and spoofing of IP addresses, each of which must be guarded against [5].

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

THREAT	ALGORITHM USED	PROBABILITY	IMPACT	RISK
Jamming Scrambling		3 2	1 1	3 2
Eavesdropping Management Message		3:3	2:1	6:3
Eavesdropping Traffic	DES – CBC AES – CCM			
BS or MS Masquerading	Device List X.509 certificate-based EAP	3 2:1 2:2	3 3:2 3:2	9 6:2 6:4
Management Message Modification	NO MAC SHA –1 MAC AES MAC	3 2 1	3 3 3	9 6 3
THREAT	**ALGORITHM USED**	**PROBABILITY**	**IMPACT**	**RISK**
Data Traffic Modification	Without AES With AES	3 1	1 1	3 1
DOS on BS or MS	EAP, SHA –1, AES, MAC	3:3	3:2	9:6

Table1 :- Different Type of Threats

WiMAX's enhanced MAC protocol offers higher QoS for low latency applications such as VoIP, it is expected that this service will comprise the bulk of bandwidth within the first few months of deployment. However, just as within a WiFi environment, there remain several vulnerabilities with VoIP in a WiMAX ecosystem. A VoIP system uses protocols like H.323, MGCP, Megaco and session initiation protocols (SIP) for signaling, and RTP/RTCP for media transport and control. Servers like media gateways, call agents, media gateway controllers, gatekeepers and proxies enable calling between the VoIP clients. SIP signaling protocols are exceptionally popular for their ease of implementation [6] interpretation and stateful analysis, but when left alone, are equally notorious for their vulnerability. Security risks remain within the signaling servers themselves, with hackers employing one of several methods to obtain unauthorized access. OEMs must address each of these methods individually, and as a whole, when developing an effective security infrastructure that can thwart against hackers.

A. Client impersonation: The SIP protocol can enable registration of multiple contacts for an individual user, with the "to" and "from" header fields unique per contact. By impersonating the client, a hacker can register his own contacts and make the coming and voice mail notification to the redirected contact addresses.

B. Server impersonation: After a client registers with a credentialed server, hackers can intercept session initiation requests from the client and reply with a spoofed response that directs the request to a new server. The calls from the client will either fail or connect to the hacker's defined endpoints, either way exposing the client. Similarly, hackers can intercept session requests in the registration process itself, redirecting the register requests to a fake server and exposing the server's credentials.

Attack	Likelihood	Impact	Risk
Device cloning	Likely (3)	Medium (2)	Critical (6)
Unauthorized access			
with device list-based auth.	Likely (3)	Medium (2)	Critical (6)
with manufacturer certificate-based auth.	Possible (2)	Medium (2)	Major (4)
with EAP-based auth.	Possible (2)	Medium (2)	Major (4)
Rogue base station			
without mutual auth.	Likely (3)	High (3)	Critical (9)
with EAP-based mutual auth.	Possible (2)	High (3)	Critical (6)
Replay			
without message auth.	Likely (3)	High (3)	Critical (9)
with HMAC	Possible (2)	High (3)	Critical (6)
with OMAC	Unlikely (1)	High (3)	Major (3)

Table 2:- Risk of Impersonation

C. Message tampering: Considered as trusted intermediaries, proxy servers are often employed by clients to exchange session initiation requests and stream media. Hackers may implement spoofed proxy servers and unbeknownst to the clients, intercept their media session encryption methods and associated keys. With this vital information, they may redirect the media streams to their device and decrypt the information, or prevent the media stream from reaching its actual destination, allowing for wiretapping and eavesdropping. An attacker injected the message that is able to overcome PHY layer synchronization issues and break any physical layer bulk encryption that might be present in a military system, there remain two issues that must be addressed that are Message Generation Issues, Timing of Injected Messages[7].

D. Session tampering/hijacking: After a call is established, messages are exchanged between the base station and CPE for session renewals and codec negotiations requests. However, during the call, it is possible for a hacker to tap into the stream and forge messages. When a client expects a session renewal message periodically, the session definition protocol (SDP) information is tampered with to divert the media stream, resulting in eavesdropped conversations.

E. Signaling requests resulting in DoS attacks: Proxy servers process registration and session initiation requests over a standard port number, through which hackers can instigate a flood of similar requests by spoofing multiple source IP addresses. Simultaneously barraging the server with multiple session initiation requests will result in server overload and denial of service. To protect against any of the aforementioned vulnerabilities, various 802.16-enabled devices within the WiMAX network, e.g. terminal adapters (TAs), integrated access devices (IADs), gateways, billing systems, voice mail servers and

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

unified messaging systems, must be equipped with software that can detect and prevent external infrastructure attacks before they take fruition. The complexity of this software varies with the type of the device, its usage, application and importance within the network.

The Ranging Request (RNG-REQ) message is the very first message sent by an SS seeking to join a network. The message announces the SS's presence and is a request for transmission timing, power, frequency and burst profile information. The message is also sent periodically to allow for adjustments on the part of the SS. The BS responds to the SS request using a Ranging Response (RNG-RSP) message. Early versions of the standard required an SS to make a RNG-REQ on a periodic basis. These requests would have been made during contention-based windows used for station maintenance. If an SS were unable to complete the periodic ranging process, it would be excluded from the network and ordered to re-initialize its MAC. This created a dangerous DoS vulnerability[3,13].The RNG-RSP message remains vulnerable to a potentially more serious type of exploitation. The problem is that the RNG-RSP message can do more than merely fine-tune SS transmission times. There are a variety of ways that the message may be misused. The most basic way to abuse the message is to spoof unsolicited RNG-RSP messages with the Ranging Status field set to a value of 2, which corresponds to "abort"[8].

V. ROUGH AP PROBLEMS

A rogue base station (or access point) is an attacker station that imitates a legitimate base station. The rogue base station confuses a set of subscribers (or clients) trying to get service through what they believe to be a legitimate base station. It may result in long disruptions of service. Attacks materializing this attack threat have high impact. The exact method of depends on the type of network. In a WiMax/802.16 network, this is more difficult to do because WiMax/802.16 uses time division multiple access. The attacker must transmit while the impersonated base station is transmitting. The signal of the attacker, however, must arrive at targeted receiver subscribers with more strength and must put the signal of the impersonated base station in the background, relatively speaking. Again, the attacker has to capture the identity of a legitimate base station. Then it builds messages using the stolen identity. The attacker has to wait until time slots allocated to the impersonated base station start and transmit during these time slots. The attacker must transmit while achieving a receive signal strength higher than the one of the impersonated base station. The receiver subscribers reduce their gain and decode the signal of the attacker instead of the one from the impersonated base station [9].

The rogue base station or access point attack is therefore a threat for which the risk is critical. Replay protection insures that messages are freshly generated and are not retransmissions by attackers of previously intercepted messages. For the sake of efficiency, replay protection is often combined with message authentication.

Common Approaches to Rogue AP Detection

The only way to reliably discover rogue APs [5] is to listen to the airwaves – the wireless side of your network – in combination with the wired side of your network. There are software and hardware products that make the former possible, but on their own they offer incomplete solutions.

A. Sniffers

One way to find a rogue access point is to search your facility from the wireless side. Sniffer software (such as AirSnort or NetStumbler) allows you to carry a laptop or PDA around your facility scanning all radio frequency (RF) channels for connections with any and all access points within range. While this software allows you to capture valuable information about the access points in your environment, it can be very time consuming to walk through all of your facilities in search of rogues. and data captured this way is only a sample snapshot – only valid when it is captured[10].

Further, you must determine whether the unrecognized access points you discover are rogue (within your facility whether connected to your network or not) or simply foreign (operating within range of your airspace, but connected to some other network, i.e. a neighboring business).
While this type of RF audit is often worthwhile, it is costly, incomplete, and too intermittent to continuously protect your wired network from rogues. And if your network covers many geographically dispersed locations, this method of rogue detection may be unworkable.

Probes

To ensure continuous vigilance for rogue APs, you can install full-time probes – electronic devices that continuously monitor all traffic within their range. This can be an expensive proposition. Not just in the cost of the probes (typically $500 to $1000 per device), but also in terms of pulling Ethernet cable and providing electrical power.

The rogue base station is likely to occur as there are no technical difficulties to resolve. EAP supports mutual authentication, i.e. the base station also authenticates itself to the subscriber. When EAP mutual authentication is used, the likelihood of the threat is mitigated, but not totally and remains possible for reasons similar to the ones aforementioned for EAP-based authorization[11].

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

VI. SECURITY INFRASTRUCTURE

In addition to encrypting network traffic beyond the default PKI authentication [5], OEMs must implement several additional features with in networking equipment to ensure against sniffing of the data packets originating from the signaling servers, which direct traffic to their destination.

A. Firewall and NAT traversal, topology hiding*:* The firewall provides access to authorized devices for registering and making calls through VoIP servers, dynamically opening and closing multiple ports for signaling, while handling unsolicited incoming sessions. A NAT traversal enables both signaling and media streaming from devices with cloaked IP addresses[12].

B. ***DoS and flood attack detection****:* The session border controller (SBC) shall detect the DoS attacks, UDP, ICMP and TCP flood attacksdiscussed above in vulnerabilty.

C. ***Signaling and media security, theft of service prevention:*** Signaling security is based on MD-5 authentication and TLS/IPsec.'Media security is based on secure RTP/IPsec. The type of security is negotiable through SIP signaling or through a provisioning process.

D. ***Granular access control:*** Stateful with granular access control policies provides a facility for the administrator to create application-specific policies.

E. ***Session admission control, rogue RTP detection, policing and shaping:*** The SBC shall allow the media traffic to go through valid sessions and apply traffic management rules and police the traffic to avoid excess traffic. Similarly, the SBC shall provide the desired QoS by shaping the traffic in the egress [13].

F. ***Firewalls specially designed for application-specific gateways:*** These firewalls have higher capabilities over conventional firewalls because they are part of the VoIP gateways/ IP PBX systems. The firewall can provide security to these elements and detect frauds realtime in the distributed networks, which is not possible in legacy PSTN systems that adopt centralized fraud management systems.

G. ***Intrusion detection and prevention systems:*** An intrusion detection system is vital in detecting signature-based attacks and intrusion. This system shall not pose delays and jitter in VoIP signaling and voice traffic flowing through the network. To accelerate their product deployment cycles and maintains a competitive edge in terms of product innovation, OEMs will turn to third-party software original design manufacturers (ODMs) to incorporate comprehensive converged software platforms comprising support for the aforementioned security features[14].

These platforms are:

1. Comprehensive enough to accommodate the demanding enterprise's convergence needs;
2. Thoroughly tested and approved by industry consortiums and security groups, enabling OEMs to bypass often rigorous certification standards; and
3. Fully interoperable with legacy (i.e.802.16)and future (e.g. 802.16e) standards, assuring products remain future-proof.

Additionally, these software platforms are mature enough for turnkey integration into any WiMAX CPE device, enabling OEMs to design and deploy their solutions to market at a cost-benefit to the end-user or enterprise.
Security risks remain within the signaling servers themselves, with hackers employing one of several methods to obtain unauthorized access. OEMs must address each of these methods individually, and as a whole, when developing an effective security infrastructure that can thwart against hackers[15].

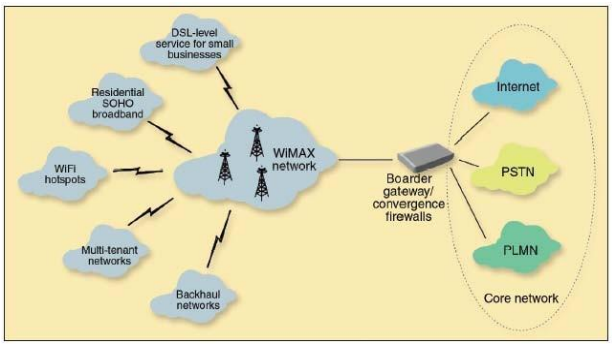

Figure 4. Several complimentary features are highlighted in Context of VoIP, each of which should be addressed by OEMs in developing a converged network platform.

VII. PROBLEM STILL EXISTS

- Hard Physical attacks are not solved to solve due to the nature of wireless signals
- Only messages above the security sub-layer are protected, while the MAC (media access control) layer are not protected.
- Connection can be distinguished using the MAC header, which violates identity privacy.
- DoS attacks on SS or BS are possible due to the complicate authentication and key derivation procedures

VII. CONCLUSION

An analysis on various threats on WiMax security has been considered. Countermeasures need to be devised for networks using the security options with critical or major risks like jamming eavesdropping of management message modification and scrambling. Using simple risk analysis, it can be demonstrated that existing authentication schemes cannot fully protect hosts in a wireless network from various attacks.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

REFERENCES

[1] WiMaxForum.www.wimaxforum.org/home, 2005.

[2] WiMax/802.16 Threat Analysis, Michel Barbeau School of Computer Science Carleton University 1125 Colonel By Drive, Ottawa, Ontario, Canada

[3] Security Issues of IEEE 802.16 (WiMAX**)** Jamshed Hasan School of Computer and Information Science ,Edith Cowan University, Australia

[4] R. Poisel. Modern Communications Jamming Principles and Techniques. Artech House Publishers, 2003.

[5] D. Johnston, and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security & Privacy, 2004.

[6] G. Lowe, "A Family of Attacks upon Authentication Protocols", Technical Report 1997/5, University of Leicester, 1997.

[7] W. Stalling, Cryptography and Network Security: Principles and Practices, 3rd edition. Pearson Education, Prentice Hall PTR, 2003.

[8] An assessment of threats of the Physical and MAC Address Layers in WiMAX/802.16, Krishnun Sansurooah School of Computer and Information Science (SCIS) Edith Cowan University Perth,Western Australia, 5.Barbeau, M. (2005).

[9] Ernst and Young, (2004). The necessity of rogue wireless device detection. White Paper,Schindler, E. (2006). The WiMAX Evolution: Bring in the Standards Suspects.

[10] Detecting Impersonation Attacks in Future Wireless and MobileNetworks Michel Barbeau1,Jyanthi Hall1, and Evangelos Kranakis1 School of Computer Science,Carleton University, Ottawa, K1S 5B6, Canada..

[11] Denial of ServiceVulnerabilities in IEEE 802. WIRELESS NETWORKS, by Derrick D. Boom September 2004, Rex Buddenberg, Brian Steckler.

[12] Frank Adelstein, Prasanth Alla, Rob Joyce, and Golden G. Richard III. Physically locating wireless intruders. In Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), pages 482– 489, 2004.

[13] R. Boshonek. Advanced Denial of Service Techniques in IEEE 802.11b. The Register. "Intel: WiMAX in notebooks by 2006."

[14] Potter, "Wireless security's future,". Security & Privacy Magazine, IEEE Volume 1, Issue 4, July-Aug. 2003.

[15] B. Aboba. The uno_cial 802.11 security web page - security vulnerabilities in EAP Methods.