Global Journal of researches in engineering
Electrical and electronics engineering
Volume 12 Issue 5 Version 1.0 April 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Security Issues in Wireless Broadband Networks

By Dr. Gurjeet Singh & Dr. Jatinder Singh
Desh Bhagat Institute of Engineering & Management Moga

Abstract - In this paper, we would be discussing about major issues pertaining to security feature in broadband technology. To know different securities aspect which may hinder advancement of broadband technology. In this research paper taking up Wimax broadband technology working concepts and it's different security features, which needs to be taken up at a clear scale.

Keywords : *Security, Broadband Networks.*

GJRE- F Classification : *FOR Code: C.2,C.2.0,D.4.6*

Strictly as per the compliance and regulations of:

Security Issues in Wireless Broadband Networks

Dr. Gurjeet Singh [α] & Dr. Jatinder Singh [σ]

Abstract - In this paper, we would be discussing about major issues pertaining to security feature in broadband technology. To know different securities aspect which may hinder advancement of broadband technology. In this research paper taking up Wimax broadband technology working concepts and it's different security features, which needs to be taken up at a clear scale.

Keywords : *Security, Broadband Networks.*

I. Introduction

Broadband in the general term also referred as high-speed network connections. Broadband describes a medium that can carry signals from multiple independent network carriers on a single coaxial or fiber optic cable .While the benefits are compelling, there are still a number of challenges with moving to broadband Internet. Spotty geographic coverage and installation challenges are a significant impediment. As cable and DSL providers accelerate their deployment plans, this situation is improving, but there are still significant challenges. Network security is another very significant issue, and one that is becoming increasingly visible as hacker attacks on home PCs [1]

There are so many profits when we adapt a broadband network, this broadband network can spread through different geographic but installation is the major problem. Internet connections via cable modem and Digital Subscriber Line (DSL) are frequently known as broadband Internet connections. Cable and DSL providers speed up their operations plan and the conditions are improving, but network security is the major concern.

Security problems are increasing rapidly as hacker attacks on home PCs and major company websites such as government organizations. One of the most compelling uses of broadband connections is to allow enterprises to Connect branch offices and telecommuters into the corporate network with high-speed remote access. [2]

To come across the suggested subsequent security solutions:

1. **Firewall:** To access control policy connecting two networks firewall implemented. Firewalls might be dependent on the software like checkpoint, CA or hardware appliance similar to Net Screen, watch guard and Nokia etc. Personal firewalls solutions still give the impression of being for Home users resembling Network ICE etc.
2. **Anti-Virus:** Anti-Virus looks for patterns in the files or memory of your computer to specify possible occurrence of a recognized virus.
3. **Encryption:** To think about encrypting traffic at your PC communications are mostly responsive. The beginning of denial of service attacks from these computers VPN, SSL provide secure for e-commerce transactions the Firewall with VPN protection secures sensitive data to the remote site and prevent both U-turn attacks and products similar to Net Screen PGP and Cisco etc. The type of tracking appears the danger of cookies. [4]
4. Modem Security: In some cases modem configuration & authentication information would be stored on modem, in others, stored on your computer.
5. Shared Cable Modem Connection: Cable networks are shared among numerous subscribers in a given neighborhood. As a result, neighbors could monitor your transmission by using sniffer. Please ensure service provider upgraded networks and equipments to DOCSIS (Data over Cable Service Interface Specification).
6. **Content Inspection:** Since interactive technologies like Java, JavaScript, ActiveX are a big part of broadband content sites & emails, as well as potentially an emerging vehicle for hack attacks. It is recommended that disable mobile codes such as Java, JavaScript & ActiveX. Disable scripting features in e-mail programs. You may want to explore active content security products such as Trend Micro, CA, and Finjan etc.
7. **System Security:** It is recommended that you log off & power down your PC when you are not using your connection.

Commonly, security issues at home and small office installations involve are:

1. The Internet to your computer approaching in the form of Unauthorized Internet traffic.
2. AKA software home work to Unauthorized Information departing out from your Hard Drive to someone else web Server.
3. Sudden outflow in the firewall left disable, computer left in DMZ etc.

Suddenly home work Unauthorized Information departing out is mainly a function of spyware and programs. The sum of home work programs that are rising through the day. [5]

Author α :Deptt of CSE/IT, Desh Bhagat Institute of Engineering & Management, Moga.
Author σ : Principal, Golden College of Engg & Technology Gurdaspur.

To use Cable/DSL the most common solution is to share Broadband Internet connection. The Internet desires identify to which computer it belongs to utilize a small number of computers to share one Internet connection from the information that comes. The major function of Cable/DSL Router is to Route the Internet signal to the request computer. This function is called Network Address Translation (NAT). [6]

In this paper we would talk about subject concerning security mechanism can be worked out. In this study, we would decrease the converse various techniques pertaining to security tools and techniques.

II. Introduction to Wimax Technology

Worldwide Interoperability for Microwave Access (WiMax) is an emerging fixed broadband wireless technology that will deliver last mile broadband connectivity in a larger geographic area than Wi-Fi. It is expected to provide coverage anywhere from one to six miles wide. Such WiMax coverage range is expected to provide fixed and nomadic wireless broadband connectivity without necessarily having a line-of-site (LOS) with a base station. WiMax will also enable greater mobility, higher speed data applications, range and throughput than its counterpart, Wi-Fi.

WiMax uses the IEEE 802.16 standards specifications (802.16d and g). The IEEE 802.16d specification is primarily tailored to wireless wide area networks (WWANs). The recently approved IEEE 802.16e specification, the mobile version of WiMax, on the other hand is primarily used for mobile wireless metropolitan networks (WMANs). These two specifications render WiMax architecturally ideal for the last mile, the backhaul, Internet Service Providers, cellular base stations that bypass PSTN's, hotspots, and enterprise networks.

Abilities such as a high bandwidth frequencies between 2 GHz and 11GHz, makes WiMax ideal for data transport. WiMax has a total range of up to 30 miles. This ability is enhanced by WiMax's cell radius of 4-6 miles. More so, WiMax has the ability to support various data transmitting rates of up to 75Mbps. WiMax is gaining tremendous popularity each day. In the recent 3GSM Congress, dozens in the field touted WiMax, the way forward. In fact, on August 8, 2006 Sprint, the number three ranked mobile operator in the US announced that it has selected WiMax technology for its 4G initiatives.

There are several advantages that can be derived from the deployment of WiMax. Firstly, it supports higher throughput rates, higher data speed rates, and wider operating range. These make the technology very useful for deployment in bad terrain areas or in environments with limited wired infrastructure. Moreover, WiMax supports and interfaces easily to other wired and wireless technologies such as Ethernet, ATM, VLANs, and Wi-Fi. Furthermore, WiMax provides network connectivity that explores multipath signals without the stringent requirement of a direct line of sight. Finally, WiMax provides a better Quality of Service (QoS) by taking advantage of smart antenna technology that utilizes the spectrum more efficiently.

The main drawback to the deployment of WiMax is proprietary equipment. WiMax equipment must be able to utilize power efficiently in order to deliver optimum functionality. For WiMax, the output power usage is based on a ranging process that determines the correct timing offset and power settings. Therefore, the transmissions for each subscriber station are supposed to be such that they arrive at the base station at the proper time and at the same power level. When WiMax is deployed outdoors, in non-line of sight environments it may encounter delay, which can cause potential intersymbol interference. Though the use of scalable orthogonal frequency division multiplexing (SOFDM) is meant to try and alleviate this problem, OFDM usage has the problem of generating phase noise, which Broadband introduces two new security challenges:

a. Increased vulnerability to hacker attacks
b. Establishing secure connections to other networks across a public IP network.

III. Research Methodology

As our research is mainly concentrating on security issues and different work mechanism of security tools and techniques through which, we can overcome those. This section discusses the security mechanisms included in IEEE 802.16-2004, IEEE 802.16e-2005, IEEE 802.16-2009, and IEEE 802.16j-200912 to illustrate their functions and provide a foundation for the security recommendations in Section 5. The IEEE 802.16 standards specify two basic security services:

- Authentication
- Confidentiality

Authentication involves the process of verifying the identity claimed by a WiMAX device. IEEE 802.16e-2005 and IEEE 802.16-2009 share the same authentication and confidentiality mechanisms. They both support user authentication in addition to device authentication. Confidentiality involves preventing the disclosure of information by ensuring that only authorized devices can view the contents of WiMAX data messages. The IEEE 802.16 standards do not provide any capability to encrypt management messages.

The IEEE 802.16 standards do not address other security services such as availability and confidentiality protection for management messages; if such services are needed, they must be provided through additional means. Also, IEEE 802.16 security protects communications over the WMAN link between an SS/MS and a BS, but not communications on the wired operator network behind the BS. End-to-end

security is not possible without applying additional security controls not specified by the IEEE standards.

The latest development in wireless metropolitan area networks is IEEE 802.16, also known as WiMAX (Worldwide Interoperability for Microwave Access) [IEEE04] [IEEE06] [Hos06]. This new standard brings us higher range and speeds compared to 802.11 (WLAN, wireless local area network). The standard is still evolving these days and many problems are not solved yet. One major issue of WiMAX is security. Several scientific papers call this is a big problem. For example [YZZ+05] tells us: "But the security problems in its original protocol may be becoming the most serious obstacle in its marketable producing process." [LL06] states: "As the mobile services supported in the standard, new security problems may be coming and becoming a serious obstacle to develop the WMAN (Wireless Metropolitan Access Network)."The latest standard for WiMAX, IEEE 802.16e [IEEE06], already offers significant security improvements over 802.16-2004 [IEEE04]. It uses better encryption methods and has a more secure key management protocol. Also a new authentication method based on EAP (extensible authentication protocol) [DCA06] [Man03] was added. But still a lot of security issues remain to be solved. Security, and especially authentication and authorization, is crucial to every wireless technology, because without good security the technology is not usable at all. Several researchers have published solutions on the security issues of WiMAX, but are these solutions satisfactory? In this research we will answer that question with a focus on the authentication and authorization part for 802.16e. This paper gives a state of the art on security solutions for WiMAX and it provides a comparison of hese solutions based on certain criteria.

Research questions

The main research question for this paper is:

1. Are the proposed security solutions concerning authentication and authorization for WiMAX satisfactory based on certain criteria?
2. What are the main authentication and authorization aspects in WiMAX?
3. What are the main security issues associated with authentication and authorization for WiMAX?
4. What are the proposed solutions in literature for these security issues?
5. What criteria can be used to analyze those solutions?
6. Which security solutions satisfy the criteria?

IV. Authentication and Authorization

In this paper we will first explain the basic security aspects of WiMAX considering authentication and authorization. Authentication addresses establishing the genuine identity of the device or user wishing to join a wireless network. Authorization addresses determining whether the authenticated user or device is permitted to join the network, see [DCA06]. When a subscriber station (SS) wants to connect to a WiMAX base station (BS), see [Aiko06], at first a connection is established between them. The next step is the authentication of the SS so it can enter the network. SS sends a so-called X.509 certificate [Hou02] to BS to identify itself. The certificate is like a signature for the SS. It contains data like a serial number, the certificates issuer, the public key of the sender, its MAC address etcetera.

After the authentication message SS sends an authorization message to BS. This message contains SSs supported authentication and data encryption algorithms. If BS determines that SS is authorized it sends a message back containing an authentication key (AK), a 4-bit sequence number and a lifetime for it containing the number of seconds before it expires [Aik06]. MS refers here to a mobile subscriber station (SS). When all these steps have been done successfully, the SS has entered the network of BS and it can communicate with all the entities in its network. Authentication and authorization [LL06] the communication between SS and BS is protected by the so-called security associations (SAs). These SAs perform encryption on the data between SS and BS using a 'traffic encryption key' (TEK). Different types of encryption are supported. [Aik06].

V. Security Issues and Solutions

a) DOS (Denial of Service)/ Reply attack

Denial of Service (DoS) is one of the major issues of all types of wireless networks especially broadband wireless networks. When authorized users are not provided a requested service within a defined maximum waiting time, it means that a DoS violation has occurred. It is the most harmful and dangerous attack which can be launched on any layer of broadband Wireless Network. DoS attacks target availability by preventing communication between network devices or by preventing a single device from sending or receiving traffic, where availability ensures that authorized users can access the data, services and network resources from anywhere anytime.

Physical Layer Vulnerabilities WMN and IEEE 802.11 uses 2.4 GHz frequency band while IEEE 802.16 uses 10-66 GHz and 2-11 GHz bands at physical layers. DoS attack can be launched against physical layer by using radio jamming device or a source of strong noise to interfere the physical channels and may compromise the service availability. However this kind of attack is not common as it need specialized hardware equipment to be launched, furthermore jamming attacks can be detected using radio analyzers. It can create great problems during exchange of sensitive information or during warfare. For jamming attack in

- IEEE 802.11, the attacker needs to be close to the target AP
- IEEE 802.16, the attacker needs to be close to the Base Station (BS)
- WMN, the attacker can launch the attack from anywhere. Due to the vast coverage area and dense deployment of wireless mesh routers in WMN, it is more vulnerable to physical layer DoS attacks.

Currently, IEEE 802.11 uses Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS), IEEE 802.16 is using Orthogonal Frequency Division Multiple Access (OFDM) and Scalable OFDM access (SOFDMA), while WMN uses OFDM and Ultra wide band (UWB) mechanisms for radio transmission. None of the mechanism is capable enough to handle the jamming attack on these broadband wireless networks.

b) Distributed Flooding DoS

A distributed flooding DoS attack is a huge challenge for all the wireless broadband networks, as this attack can bring down an entire network or consume the network bandwidth to a great extent. This kind of attack is launched by first compromising large number of innocent nodes in the wireless network termed as Zombies, which are programmed by highly skilled programmer. These zombies send data to selected attack targets such that the aggregate traffic congests the network. In most of the cases, the DDoS is impossible to prevent and it has the ability to flood and overflow the network. In IEEE 802.11 the target of distributed flooding would be Access Point (AP), in WMN the target is wireless mesh router while in IEEE 802.16 it is base station.

c) Rogue and selfish backbone devices

The attacker can seriously disrupt the broadband wireless networks by compromising the core network devices. In WMN and IEEE 802.11, a selfish mesh router or selfish AP can degrade the network performance either causing congestion or unavailability. IEEE 802.16, a rogue BS is an attacker station which is used to confuse the mobile stations of the network; as such kind of BS seems and acts like a legitimate BS. Mesh routers or APs are compromised by the attackers using sniffers. A sniffer is an application which is used for passive traffic analysis attack to analyze the network traffic. In IEEE 802.16, the BS is compromised by reprogramming a device with the hardware address of another legitimate device with hardware address can be detected by intercepting the management messages of IEEE 802.1 using sniffers. The same mechanism can be applied on mesh routers and APs to compromise using hardware address of another network device.

Authorization flooding on backbone devices WMN and IEEE 802.11 nodes use Probe request frames to discover a wireless network, if a wireless network exist then the AP respond with Probe response frame. The clients select that AP which provides the strongest signal to it. Here the attacker can spoof a flood of probe request frames presenting a lot of nodes searching for wireless network, can seriously overload the AP or wireless mesh router. If the load exceeds the threshold value will cause the AP or wireless mesh router to stop responding and may create service unavailability. In IEEE 802.16 the client stations use certificate to authenticate and register with the BS. The client station can send a bulk of registration requests to the BS may result in DoS.

d) Node deprivation attack

In node deprivation attack, the attackers target a single node and isolate it from taking part in the normal network operations. In WMN and IEEE 802.11, the nodes first authenticate itself with the mesh router or AP, and needs to de-authenticate it if the node has no more desire to use the network resources. The attacker can spoof the de-authentication message on behalf of the target node so that to stop it from using the network resources. The same vulnerability exist in IEEE 802.16, where the adversary eavesdrop the authentication message exchange between the node and the BS, and then replays this message many times to BS, creating DoS for the target node.

VI. Results of Dos Attacks and Pcssible Countermeasures

The results of different DoS attacks on broadband wireless networks vary with the nature and type of DoS attack.

- DoS attack is of low intensity, if launched against a single node either to exhaust its battery or to isolate it from the network Soperations.
- DoS attack is of high intensity if it is launched to make services unavailable for a target area in wireless broadband networks. Selfish mesh router attack in WMN and rogue BS attack is used for this purpose.
- Dos attack will be of highest intensity if it is launched to cripple down the entire broadband wireless network by distributive flooding.

Distributed flooding is normally used for this purpose to exhaust the bandwidth of the network or to overflow the resources of the gateways. DoS in any form against any network is regarded as a severe attack. Some possible countermeasure needs to be investigated to overcome to some extent against DoS and related issues in broadband networks.

Message 1. SS → BS : Cert (SS. Manufacturer)
Message 2. SS → BS : T_S | Cert (SS) | Capabilities | SAID | SIG_{SS} (2)
Message 3. BS → SS : T_S | T_B | KU_{SS} (AK) | Lifetime | SeqNo | SAIDList | Cert (BS) | SIG_{BS} (3)

'Cert' stands for the X.509 certificates used. 'KUss (AK)' is the Authentication Key encrypted by SSs public key. Ts and Tb are timestamps of respectively the SS and BS. SeqNo and Lifetime are a sequence number and lifetime for the AK. SIGss and SIGbs are signatures for respectively the SS and BS. The SAID List defines the security associations ID´s to be used for communication. By adding the timestamps and signatures, freshness can be guaranteed for both messages. This way both SS and BS know that the message is fresh and not intercepted and replayed. The key management protocol (see figure 5) is also vulnerable for these attacks. Both the message from BS to SS and vice versa can be replayed to cause DoS or other unwanted behaviour.

HMAC stands for Hash Message Authentication Code, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. What happens is that SS requests (or BS forces him to, using message 1) a new TEK in message 2. HMAC (1) can be used by SS to detect forgery attacks. HMAC (2) assures BS that the message is authenticate. HMAC (3) assures SS that message 3 is from BS and has not been modified.

Message 1. BS → SS: SeqNo | SAID | HMAC (1)
Message 2. SS → BS: SeqNo | SAID | HMAC (2)
Message 3. BS → SS: SeqNo | SAID | OldTEK | NewTEK | HMAC (3)

Because message 1 is optional, Tb2 will be set to 0 in message 2 by SS when it initiates re-keying. Tb2 in message 3 is generated by BS in responding to SSs request to assure SS the freshness and aliveness. When BS starts the rekeying, TB2 is generated in message 1 by BS and SS should include it in message 2 to assure BS the freshness and aliveness, but BS can omit it in message 3 by setting it to 0.

Message 1. BS → SS: T_{B2} | SeqNo | SAID | HMAC (1)
Message 2. SS → BS: T_{B2} | T_{S2} | SeqNo | SAID | HMAC (2)
Message 3. BS → SS: T_{S2} | T_{B2} | SeqNo | SAID | OldTEK | NewTEK | HMAC (3)

VII. Analysis

We will seem, per problem, at all answers by means of the principles stated over. For every explanation there is a table showing how they score on each criterion. A '+' means it scores well on that criterion, a '+/-' that it is doubtable and a '–' means a bad score. A '?' means no information was available for that criterion, for example no performance information because no simulations were ran.

a) DoS/Reply attack

[XMH06] depicts good quality development for authentication and authorization beside rerun assaults. Adding together the timestamp and signatures needs a sensible alteration to the normal. No data is obtainable concerning presentation but our anticipation would be a minute plunge in presentation. Even though the answer is deconcentrated, the argument in communication dimension in not radically. Yet, owing to the forward of timestamps and signatures, measurability might be exaggerated. [9]

VIII. Conclusion

From the above analysis, we are able to consider different issues pertaining to security aspect of broadband technology. When discussing the security of wireless technologies, there are several possible Perspectives. Different authentication, access control and encryption technologies all fall under the umbrella of security. Although relevant and important building blocks for overall security, these are not the focus of this paper. Instead, it will explore the problems at the implementation level of the current wireless access technologies and their Real world implications. As future technology of broadband is wireless communication, in that WIMAX plays a major role. In other way, in this research paper we would be discussing issues of security feature of WiMax and analyse one of the security features to work on it.

References Références Referencias

1. Advanced Encryption Standard Fact Sheet. (2001, January 19). Retrieved August 28, 2010, from http://www.kern.com/files/SecurityFinal_F.pdf
2. Aikaterini, A-V. (2006). Security of IEEE 802.16. Royal Institute of Technology.
3. Bai,L.(2007).Analysis of the Market for WiMax Services.
4. Barbeau, M. (2005). WiMax/802.16 Threat Analysis. Q2SWinet'05.
5. Barongo,M.W. (2008). Dimensioning MobileWIMAX in the Access & Core Network: A Case Study. HELSINKI UNIV.
6. Bruno Puzzolante, G.R. (2006). Nationwide Implementation of a WiMAX Mobile Access Network
7. Chungo-Kuo Chang, C.-T.H. (2007). Secure Mobility for IEEE 802.16e Broadband Wireless Networks.

2007 International Conference on Parallel Processing.
8. Edurado B.Fernandez, M.V. (2007). Patterns for Wimax security.
9. G.Cayla, S.C. (November, 2005,). WIMAX an Efficient.WiMax Forum.
10. G.Nair, J.C. (2004). IEEE 802.16 Medium access Control & Service Provisioning Intel Technology Journal.
11. Hasan J. (2006). Security Issues of IEEE 802.16. School of Computer and Information.
12. IEEE. (2004). IEEE Std 802.16-2004, IEEE standard for WiMax 802.16-2004.
13. Muleta, J. (2005). Broadband Technologies for rural Development. NCC Rural Access.
14. Prakash, N. (2006). Wireless Broadband Access Using WiMax Standard.
15. Sikkens B. (2008). Security Issues and proposed solutions concerning authentication and authorization for WiMax. 8th twente student Conference on IT.