Global Journal of Researches in Engineering
Electrical and Electronics Engineering
Volume 12 Issue 8 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Comparative Analysis and Security Issues in Broadband Wireless Networks

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

Abstract - Broadband wireless networks are considered to be enterprise-level networks providing more capacity and coverage. Wireless networking has offered an alternative solution to the problem of information access in remote inaccessible areas where wired networks are not cost effective. They have changed the way people communicate and share information by eliminating worrisome factors of distance and location. This paper provides a technical analysis of alternatives for implementing last-mile wireless broadband services. It provides detailed technical differences between 802.11 (Wi-FI) wireless networks with 802.16 (WiMAX), a new technology that solves many of the difficulties in last-mile implementations.

Keywords : *Broadband wireless, Last mile access, Rural connectivity, WiMAX, Wi-Fi, Digital divide, Network Security.*

GJRE-F Classification : *FOR Code : 100510*

Strictly as per the compliance and regulations of:

Comparative Analysis and Security Issues in Broadband Wireless Networks

Dr. Gurjeet Singh

Abstract - Broadband wireless networks are considered to be enterprise-level networks providing more capacity and coverage. Wireless networking has offered an alternative solution to the problem of information access in remote inaccessible areas where wired networks are not cost effective. They have changed the way people communicate and share information by eliminating worrisome factors of distance and location. This paper provides a technical analysis of alternatives for implementing last-mile wireless broadband services. It provides detailed technical differences between 802.11 (Wi-FI) wireless networks with 802.16 (WiMAX), a new technology that solves many of the difficulties in last-mile implementations.

Keywords : Broadband wireless, Last mile access, Rural connectivity, WiMAX, Wi-Fi, Digital divide, Network Security.

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].

Author : AP, Deptt of CSE/IT, Desh Bhagat Institute of Engg & Management, Moga. E-mail : hi_gurjeet@rediffmail.com

II. Overview of Wi-Fi and Wimax

a) The IEEE 802.11 (Wi-Fi)

The Wireless Fidelity (Wi-Fi) devices made possible the discovery of the wireless network world. In the WLAN field, the only major competition comes from HIPERLAN II. The Wi-Fi standard family allows wireless network over short distances. These standards are sometimes associated with directional antennas to establish point-to-point connections. WLANs based on the IEEE 802.11 standard are expected to be a major component to enable an integrated office, hospital, home networks and for campus buildings. The 802.11 WLANs operate in the ISM (industrial scientific and medical) bands, with several flavors of physical layer available. The first 802.11 wireless network standards were developed in 1997 as an extension to the Local Area Network. It was known as wireless Ethernet that only supported a maximum speed up to 2 Mbps. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) were the modulation techniques supported. There are three well known 802.11 wireless family standard widely used today.

b) The IEEE 802.11b

A refined standard for the original 802.11 and was successful due to its high data rates of 11 Mb/s - range of 100 m to a maximum of a few hundreds meters, operates on 2,4 GHz unlicensed band. 802.11b is the most widely deployed wireless network within the 802.11 wireless families [4, 5]. It uses the DSSS modulation technique that is more reliable than the FHSS.

c) The IEEE 802.11g

The IEEE 802.11g wireless standard also operates on the 2.4 GHz band and has similar range and characteristics as the 802.11b. It has a data rate of 54Mbps. The 802.11g has backward compatibility with 802.11b and differs only on the modulation technique; it uses Orthogonal Frequency Division Multiplexing (OFDM). This then makes the 802.11b devices not able to pick the signal from the 802.11g devices.

d) The IEEE 802.11a

Operates in the 5 GHz band with a maximum data rate of 54Mbps. The major disadvantage in deploying 802.11a with the other 802.11 standards b

and g is that, they cannot co-exist, as they operate on different frequency bands. 802.11b/g operates on the 2.4 GHz spectrum. There are some wireless card and access points which are compatible to all the three standards thereby supporting the 2.4GHz and 5GHz frequencies. The benefits of using Wi-Fi for last-mile solutions are:

1. Off-the-shelf 802.11 standard products are currently available
2. 2. Initial investment is cost effective for small deployments
3. 3. Flexibility over wired installations can be achieved

e) The IEEE 802.16 (WiMAX)

Wireless networks adapted for covering cities and villages, arrived a few years after the Wi-Fi type WLAN. The IEEE 802.16 WiMAX (World Interoperability for Microwave Access) standard is based on global interoperability including ETSI HIPERMAN, IEEE 802.16d-2004 for fixed, and 802.16e for mobile high-speed data. It is an emerging technology that delivers carrier–class, high speed wireless broadband at a much lower cost than the cellular services while covering large distances than Wi-Fi. It has been designed to be a cost-effective way to deliver broadband over a wide area. It is intended to handle high-quality voice, data and video services while offering a high QoS. WiMAX is classified as the Wireless Metropolitan Area Network (WMAN) that operates in between 10 and 66 GHz Line of Sight (LOS) at a range up to 50 km (30 miles) and 2 to 11GHz non Line-of-Sight (NLOS) typically up to 6 - 10 km (4 - 6 miles) for fixed customer premises equipment (CPE) [11]. Both the fixed and mobile standards include the licensed (2.5, 3.5, and 10.5 GHz) and unlicensed (2.4 and 5.8 GHz) frequency spectrum. However, the frequency range for the fixed standard covers 2 to 11 GHz while the mobile standard covers below 6 GHz. Depending on the frequency band, it can be Frequency Division Duplex (FDD) or Time Division Duplex (TDD) configuration. The data rates for the fixed standard will support up to 75 Mbps per subscriber in 20 MHz of spectrum, but typical data rates will be 20 to 30 Mbps. The mobile applications will support 30 Mbps per subscriber, in 10 MHz of spectrum, but typical data rates will be 3 - 5 Mbps.

f) PHY (Physical) Layer

Apart from the usual functions such as randomization, forward error correction (FEC), interleaving, and mapping to QPSK and QAM symbols, the standard also specifies optional multiple antenna techniques. This includes space time coding (STC), beam forming using adaptive antennas schemes, and multiple input multiple output (MIMO) techniques which achieve higher data rates. The OFDM modulation/demodulation is usually implemented by performing fast Fourier transform (FFT) and inverse FFT on the data signal.

The MAC layer used by WiMAX is based on a time division multiple access (TDMA) mechanism to allow a homogeneous distribution of the bandwidth between all the devices which is more effective and support several channels compared to the mechanism used by Wi-Fi (CSMA-CA). This makes it possible to obtain a better optimization of the radio spectrum with better efficiency (bits/seconds/Hertz). Thus, WiMAX has an efficiency of 5 Bps/Hz compared to the 2.7Bps/Hz of Wi-Fi that makes it possible to transmit 100 Mb/s on 20 MHz channel.

g) Comparision of Wi-Fi and WiMAX

From the technical overview of the two wireless technologies given in previous section, it can be seen that they are not addressed to the same market but are very complementary. Wi-Fi allows the implementation of wireless local area network for a house or a small building. It can also be used to carry out a public hot spot allowing mobile points to connect in a hotel, an airport, etc. WiMAX is a metropolitan technology whose objective is to interconnect houses, buildings or even hot spots to allow communication between them and with other networks (Internet, etc).

Although not being targeted on the same use, more recently WiMAX technology has several advantages compared to Wi-Fi. Such as: a better reflection tolerance; a better penetration of obstacles; and an increased in the number of interconnections (a few hundreds of equipment rather than some tens of equipment for Wi-Fi). It's obvious that the WiMAX standard goal is not to replace Wi-Fi in its applications but rather to supplement it in order to form a wireless network web. Despite the similarity in equipment cost, WiMAX technology requires a costly infrastructure while Wi-Fi can be easily install using low cost access points. These two wireless technologies have common components in their operations with a major difference in the communication range. Table 1 below gives the detailed comparative analysis of the two broadband wireless access networks (WiFi and WiMAX) suitable for rural connectivity.

Table 1 : Comparison between 802.11 & 802.16

Properties	802.11(Wi-Fi)	802.16(WiMax)
Frequency Band	5GHz	2GHz to 11GHz
Range	100m	50km
Coverage	Optimized for indoor performance	Optimized for outdoor performance
Security	WAP+WEP	DES & RSA
Radio Technology	OFDM(64 channels)	OFDM(256 channels)

Modulation	QPSK-802.11b	QPSK 14, 64, 256-QAM
Data Rate	802.11a-54Mbps 802.11b-11Mbps	802.16a-75Mbps 802.16b-15Mbps

III. Security Issies 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.

IV. Results of Dos Attacks and Possible 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 operations.
- 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 SSspublic 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 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)

V. 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].

VI. 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.
8. Sikkens B. (2008). Security Issues and proposed solutions concerning authentication and authorization for WiMax. 8th twente student Conference on IT.