Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.641 – 646

RESEARCH ARTICLE

Wireless Broadband Network, WiMAX Security and Applications

Vandana V. Gawit[1], Namrata D. Ghuse[2]

[1]ME Student, Department of Computer Science and Engineering, P.R.Pote(Patil) College of Engineering and Management, Amravati, India

[2]Asst. Professor, Department of Computer Science and Engineering, P.R.Pote(Patil) College of Engineering and Management Amravati, India

[1] vandanagawit@gmail.com, [2] namrata_ghuse@rediffmail.com

Abstract — The growth of wireless broadband networks is expected to gradually outpace landline communications because advancements in these technologies have continued to enable higher broadband speeds. This can be attributed to high demand for wireless multimedia services such as data, voice, video, and the development of new wireless standards. This paper explores Wireless broadband network security solution. Worldwide Interoperability for Microwave Access (WiMax) is an emerging fixed broadband network. WiMax Technology security issues, its security mechanism and Wireless broadband network applications.

Keywords— Wireless broadband network, WiMax, Encryption, Security, Applications

I. INTRODUCTION

Wireless broadband is high-speed Internet and data service delivered through a wireless local area network (WLAN) or wide area network (WWAN).Generally, broadband wireless networks can be categorized into two types: fixed and mobile wireless. The broadband fixed wireless network technologies of interest here are Wireless Fidelity (Wi-Fi), which is an IEEE 802.11 standard and Worldwide Interoperability for Microwave Access (WiMax), which is also an IEEE 802.16 standard. The two broadband mobile wireless network technologies are the third Generation (3G) and Fourth Generation (4G) networks. The 3G standards are defined by ITU-T, IMT2000 and the standards for the 4G are currently being defined. 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. 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 ecommerce 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) *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.

II. WIRELESS BROADBAND WORK

Essentially you need a piece of equipment in each building where you want to connect two LAN segments. For those situations, where a clear line of sight is not available, one or multiple hubs may be deployed – acting as repeaters and logical diverters of radio signals. The Customer Premise Equipment (CPE) in most implementations consists of two fundamental components: a Network Interface Unit (NIU) - an indoor unit providing circuit emulation and Ethernet data services – essentially a Transceiver and an antenna unit mounted on the top or side of the building. In some cases, the transceiver and antenna are integrated into one unit – e.g. in Nortel's Reunion Broadband Wireless Access products. NIU is connected to the data network (typically a LAN) in the two buildings.

A. *Point to Point Broadband Network*

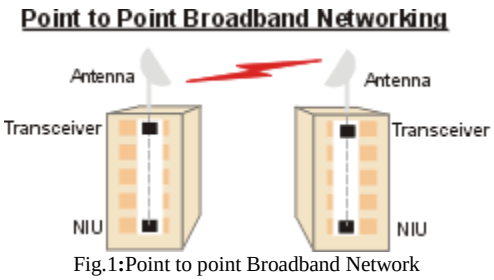

Fig.1:Point to point Broadband Network

- Where multiple services (voice and data are employed), there is another piece of equipment that is called Base station equipment – that provides multiplexing and channel separation.
- In those cases where a clear line of site is not available between to points or where multiple locations need to be served, there is a Hub in the center as shown in the following schematic.

B. Multipoint Broadband Network

- Differences in data transfer between components reveal some of the benefits of a wireless system as opposed to other technical alternatives like cable and Digital Subscriber Line (DSL), or traditional ISDN.

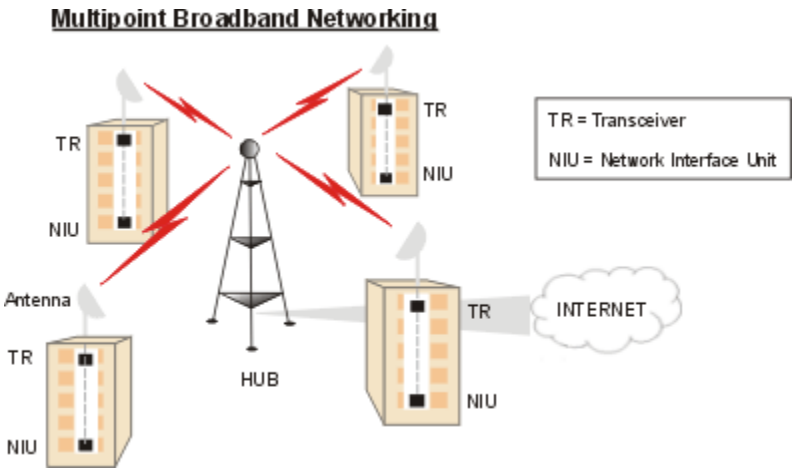

Fig2.:Multipoint Broadband Networking

III. WIRELESS & MOBILE COMPUTING SECURITY

A. Security in Broad Sense

Securing information from unauthorized access is a major problem for any network - wireline or wireless Security, in a broad sense, focuses on network security, system security, information security, and physical security. It is made up of a suite of multiple technologies that solve numerous authentication, information integrity, and identification problems. It includes the following technologies – firewalls, authentication servers, biometrics, cryptography, intrusion detection, virus protection, and VPNs

B. The task of securing wireless networks can be divided into five challenges:

- Network access control.
- Network resource protection.
- End-point, including wireless client, protection.
- Secure end-to-end data traffic transmission.
- Secure network configuration, operation and management.

C. Understanding the Components

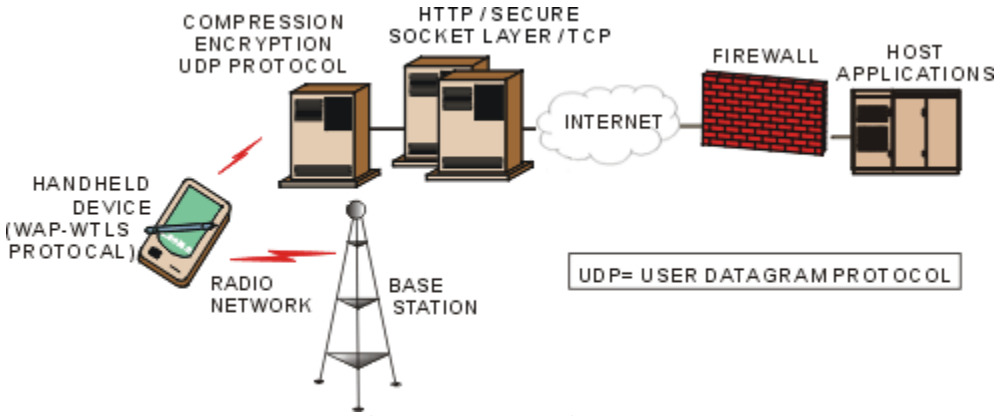

Fig3: A Schematic of Security Architecture for Mobile WAP-based Devices

IV. WiMax

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. 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. 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.

A. Security Issues

There are many security threats that have been found in the 802.16 standard. Because of the focus on the MAC level security, the PHY level is left vulnerable to attacks, especially with the addition of mobility in 802.16e. 802.16 also shares 802.11's data confidentiality insecurity due to WEP. The most serious security problems arise in relation to the lack of BS Authentication in earlier versions of the standard, as well as the high risk of replay and DoS attacks.

1) BS Authentication : One of the major holes in the initial versions of the 802.16 standard was the lack of authentication of the BS by the SS. This left WiMAX very vulnerable to Forgery and Man-in-the-Middle attacks where the SS would not know whether or not it was communicating with a legitimate BS. This problem has been patched in 802.16e by adding the mutual authentication described above in PKMv2.

2) Replay and DOS Attacks : It is possible for an attacker to intercept and store an Authorization Reply Message and then repeatedly send the message to the BS. Since the BS will find that the message is from an authorized SS, its resources will be consumed, resulting in a Denial-of-Service Attack. Also, a replay attack is possible wherein an attacker intercepts TEK messages and then replays them in order to gain the information needed to decrypt traffic data by using the two-bit Key Sequence Number of the TEK.. Another threat arises from the lack of explicit definitions of the authorization SA, which leads to the possibility of encryption key reuse because the SSs cannot distinguish reused SAs2.

B. Security Mechanisms

In order to provide data integrity and privacy over an open radio channel, the MAC layer of 802.16 includes a security sub layer. The security mechanisms include the encryption of data between the base station (BS) and subscriber station (SS), certificate-based authentication of the SS, and privacy key management (PKM) as an authenticated client-server key management protocol. In order to patch up some major security issues described below and to account for the addition of mobile services, the standard 802.16e has specified some changes in the security measures.

1) Encryption: 802.16 includes RSA (Rivest Shamir Adleman), DES-CBC (Data Encryption Standard- Cipher Block Chaining) and AES-CCM (Advanced Encryption Standard in Counter with CBC-MAC) as the standard encryption algorithms and HMAC (Hashed Message Authentication Code) and CMAC (Cipher-based Message Authentication Code) as the cryptographic algorithms. These algorithms are used for the encryption of traffic encryption keys (TEKs), traffic data, and Authorization Reply messages.

2) Security Associations: Security Associations (SAs) are information sets that support secure communication that is shared between a Base Station (BS) and its client SSs or mobile stations (MSs) .This may include information such as the cryptographic suite used for the SA, data encryption methods, and TEKs along with their lifetimes and state information. Upon entering a network, an SS will set up a primary SA, and then may add static and dynamic SAs depending on specific service flows.

3) Certificate-Based Authentication: X.509 Version 3 certificate formats must be used by SSs in order to comply with the 802.16 standard. The manufacturer provides and installs a unique X.509 certificate in each SS, which contains the SS RSA

public key and SS MAC address. In standards 802.16-2004 and above there is also an X.509 certificate for the BS so that both the SS and BS can mutually verify authenticity.

4) Privacy Key Management Protocol (PKM): PKM establishes a shared secret between the SSs and BS to allow the BS to distribute keying materials such as Authorization Keys (AKs) and SAs to client SSs as well as periodic renewal and reauthorization of keys. The authorization and TEK state machines manage keys in the SS. PKM request and Response messages are sent between the BS and SS as MAC management messages to handle transmission of the AKs . A new instance of the TKE state machine is started by the SS for each SA that it receives from the BS. PKMv1 is used in the standard up until 802.16e when PKMv2 was introduced to provide stronger security. The greatest difference between the two is that in PKMv1 the BS authenticates the SS and then enables the ciphering of data by providing it with keying material, whereas in PKMv2 there is mutual authentication between the BS and MS. Also, in PKMv1, public key cryptography is used for the establishment of a shared secret between the SS and BS, but in PKMv2 RSA-based or EAP-based authentication protocols are used along with RSA and EAP as sources of keying materials.

V. WIRELESS BROADBAND NETWORK APPLICATIONS

A broadband application area is defined here as a general grouping of applications designed for specific purposes that can apply to different types of industries and consumers. This means there are various ways to categorize applications by type as opposed to categorizing by system requirements. This paper examines five major areas of broadband applications broadly relating to improving quality of life, medical care, education, and governance. These application areas are:

A. Video–based applications

One of the reasons advanced and mid–range applications require large amounts of bandwidth are the use of video and audio content. Video transfer is a component in many different applications. The focus here is on two prominent examples of entertainment–oriented applications, downloading media and online multiplayer games, and a business–oriented application, multi–point video conferencing.

B. Telehealth

Application of information technologies to the healthcare field has been slow and relatively haphazard compared to other major industries. The size, complexity, and number of stakeholders involved in the healthcare industry make it difficult to develop content and delivery standards for data .Telehealth is a general term used broadly to describe the use of any information technologies for healthcare, such as videoconferencing . Telemedicine is normally associated with the use of technology to provide clinical services to patients

C. Classroom applications and distance learning

Much like in the healthcare industry, the use of technology in education is an expansive field with a diverse set of stakeholders and disagreement over the best way to incorporate technology. (1) augment traditional teaching methods in the classroom; or, (2) facilitate distance learning platforms, such as synchronous interactive online instruction, where the learning environment is created exclusively online.

D. E–government

E–government is a term broadly used to describe online services or information provided by any government agency. The majority of e–government services typically involve downloading or uploading forms, permits, licenses, or other types of documents, as well as other account management services. Examples include renewing a driver's license or paying a utility bill online. Most studies examine the effectiveness of e–government services based on user perceptions of the service in comparison to user perceptions of e–commerce services.

E. Emergency management operations

Similar to the healthcare and education industry, policy experts spent much of the 2000s arguing how information technology can improve emergency management and help diminish the risk of natural and man–made disasters . Also similar to healthcare and education, these efforts met with varying degrees of success. The terrorist attacks of 9/11 provided a catalyst for an intense investigation into how to use information technology to better coordinate emergency management operations and first responders. This discussion sporadically centers on questions about bandwidth requirements for various emergency management software and emergency operations centers (EOCs); however, little serious scholarly research focuses on the bandwidth requirements of EOC.

VI. CONCLUSION

There has been an unprecedented rapid growth of Wireless Broadband Network demand for mobility globally, seamless communication, data services, and ubiquitous computing. When discussing the security of wireless broadband network there

are several possible solutions. Different authentication, access control and encryption technologies .This paper has been discussed WiMax security issues ,BS Authentication ,Replay and Dos Attack. Security mechanisms For WiMax Encryption, Security Associations, Certificate based authentication, privacy key management protocol.

REFERENCES

[1] Advanced Encryption Standard Fact Sheet. (2001, January 19). Retrieved August 28, 2010, from http://www.kern.com/files/SecurityFinal_F.pdf .

[2] Dr. Gurjeet Singh & Dr. Jatinder Singh," Security Issues in Wireless Broadband Networks" *Global Journal of researches in engineering Electrical and electronics engineering* Volume 12 Issue 5 Version 1.0 April 2012.

[3] Nandini Mishra, Neelam Maurya, Nikita Gaur, "Wireless Broadband Network Technology Infrastructure and Related Intellectual Property Application & Security",*International Journal of Scientific & Engineering Research,* Volume 3, Issue 11, November-2012.

[4] Aikaterini, A-V. (2006). Security of IEEE 802.16. Royal Institute of Technology. Global Journal of Researches in Engineering.

[5] Bai,L.(2007).Analysis of the Market for WiMax Services.

[6] Johnston, David; Walker, Jesse; "Overview of IEEE 802.16 security," IEEE Security and Privacy, v 2, n 3, 2004,Pages40-48, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1306971.

[7] Eren, Evren; "WiMAX security architecture - Analysis and assessment," 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS, 2007, Pages 673-677.

[8] Nuaymi, Loutfi; "WiMAX: Technology for Broadband Wireless Access," Wiley, 2007.

[9] Eklund, Carl; Marks, Roger B.; Ponuswamy, Subbu; Stanwood, Kenneth L.; van Waes, Nico J.M.; "WirelessMAN: Inside the IEEE 802.16 Standard for Wireless Metropolitan Networks," IEEE, 2006.

[10] Huang, Chin-Tser; Chang, J. Morris; "Responding to security issues in WiMAX networks," IT Professional, v 10,n5,2008,Pages15-21, http://www.ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=4629835&isYear=.

[11] Chungo-Kuo Chang, C.-T.H. (2007),Secure Mobility for IEEE 802.16e Broadband Wireless Networks.

[12] 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] 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.

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

[15] Jeff D. Saunders,Chareles R. McClure,Lauren H. Mandel "*Broadband applications:categories,requirement and future frameworks" Peer Revieved Journal on internet"*Volume 17, Number 11 - 5 November 2012.

