R.Chithra *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 9, September- 2015, pg. 14-19 **ISSN: 2321-8363**

REVIEW ON SECURITY ISSUES IN WiMAX NETWORKS FOR E-LEARNING

R.Chithra[1], Dr.B.Kalaavathi[2]

[1]Assistant Professor (Senior Grade), Department of Information Technology, K S Rangasamy College of Technology, Thiruchengode, email: chithra@ksrct.ac.in
[2]Professor and Head, Department of Computer Science and Engineering, K S R Institute for Engineering and Technology, Thiruchengode

Abstract

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless broadband technology, which supports point to multi-point (PMP) broadband wireless access. WiMAX Networks provides wireless communications with high quality of service. In the E-Learning System using WiMAX networks, the users of the subscriber station must be authenticated. The authentication in WiMAX is performed using Extensible Authentication Protocol. The EAP protocol based on Privacy Key Management in WiMAX is susceptible to security problems. In this paper the security mechanisms for authentication, encryption, and availability and its potential threats for E-Learning Systems is analyzed.

Keywords: *WiMAX, E-Learning, Authentication, security, Extensible Authentication Protocol*

1. Introduction

WiMAX is a telecommunication technology which offers high data transfer rates, high throughput and long distance connectivity coverage. IEEE standards for WiMAX such as IEEE 802.16d for fixed WiMAX, IEEE 802.16e for mobile WiMAX and IEEE 802.16j for mobile multi-hop relay based network. In WiMAX some of the management messages are not encrypted or even unencrypted to keep it simple and easy and some of them are, Traffic indication message to wake up MS, Neighbor advertisement message to tell MS about neighboring BS for handover purpose, Power control message, Ranging request message when MS is trying to find connection to BS. Security is always important in data networks, but it is mainly critical in wireless networks such as WiMAX. Security threats are a problem that needs more research in order to find solutions to these threats, fact that will help WiMAX to become a successful and reliable technology.

WiMAX uses Key Management Protocol for authentication. PKM protocol is included in the IEEE 802.16 security sub-layer [1] within the 802.16 MAC layer to perform two functions [4]. PKM protocol provides secure key material distribution between SS and BS. It also enables BS to enforce access control over network services. It also used to define, manage and distribute the keys among the network entities to maintain the data secrecy . IEEE 802.16 has an efficient and power saving mechanism called Multicast and Broadcast service (MBS) to distribute data to more number of SS in the network simultaneously. This feature of WiMAX networks supports for E-Learning.

2. WiMAX Network Architecture for E-Learning

The entities of WiMAX network involved in E-Learning are NAP(Network Access Provider),Network services provider(NSP),Application service provider(ASP).The Network Access Provider owns and operates on ASN(Access Service Network). ASN consists of two or more BS(Base Station) controlled by ASN-GW(ASN-Gate Ways).The Network services provider (NSP) which constructs Connectivity Service Network(CSN), which supply Internet Protocol(IP) connectivity and WiMAX bandwidth services to SS(Subscriber Station). CSN comprises Authentication, Authorization and Accounting (AAA) server to execute authentication, access control and accounting functions.

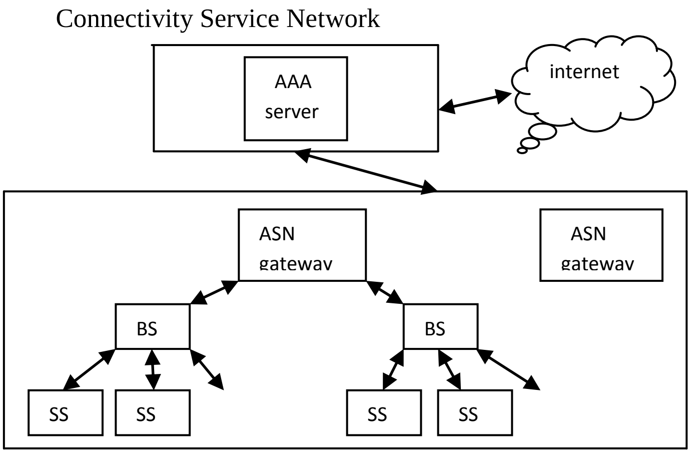

Fig.1 Entities of WiMAX Network.

The Application service provider (ASP) provides value added services such as Multimedia application and corporate virtual private network (VPN).

2.1 WiMAX Network Protocol STACK

IEEE 802.16 standard protocol stack consist of two layers: MAC (Medium Access Control) layer and PHY (Physical) layer. The MAC layer is subdivided into three sub-layer that is Convergence Sub-layer (CS), Common Part Sub-layer (CPS) and Security Sub-layer(SS)[1].

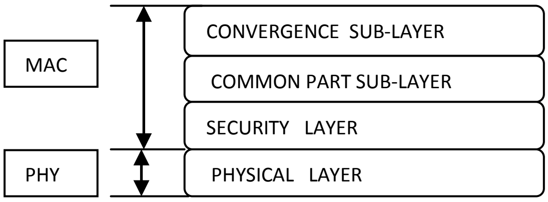

Fig.2 WiMAX Network Protocol Stack

Security Sub-layer (SS) consist of two main protocols[3]

Encapsulation protocol which is used for cipher texting operations in the networks. Encapsulation protocol is responsible to provide encryption, decryption and authentication methods using cryptographic encryption and authentication algorithms. WiMAX uses this protocol to address confidentiality, integrity and access control. This protocol establishes a privacy encryption between BS and SS and encryption of service flows access the network.

Privacy Key Management (PKM) protocol which is used for secure key distribution between BS and SS and also it enables BS to enforce conditional access control over network services.BS protects unauthorized access from E-Learning users using this protocol. The following figure3 represents the authentication process during E-Learning. PKM v2 authentication methods are based on three types.

1) Authentication based on RSA: using X.509 certificates with RSA encryption.
2) Authentication based on EAP: using user certificates
3) RSA-EAP: Authentication based on RSA followed by EAP

The major responsibility of PKM protocol is to attain authorization, authentication, key exchange and data encryption between the network entities.

The major responsibility of PKM protocol is to attain authorization, authentication, key exchange and data encryption between the network entities.

In the figure 3 The ES represents E-Learning users requesting for authentication using WiMAX network. The user forwards the request to the base station. The base station verifies the identity of the user and allows to proceed with the authentication process by forwarding the request to the Authentication Authorization

Accounting (AAA) Server. Successful authentication process supplies Master Session Key, Pair wise Master Session Key, Authentication Key to the E-Learning users.

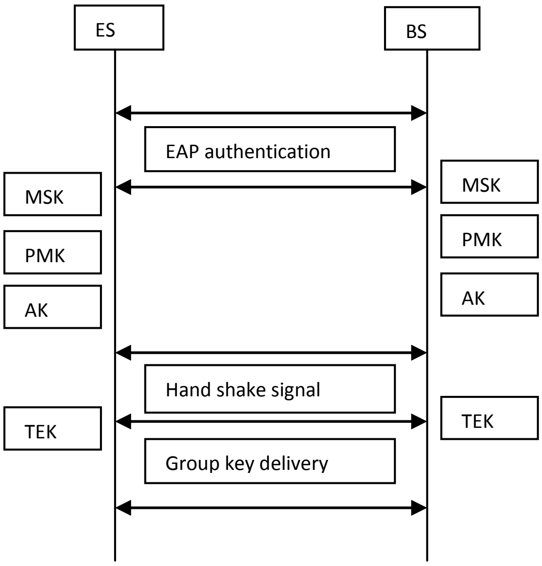

Fig.3 Key Management in WiMAX

3. WiMAX Security Threats for E-Learning

WiMAX security is implemented in the security sub-layer which is above the PHY layer[2,3]. Therefore the PHY is not protected from attacks targeting at the natural vulnerability of wireless links such as jamming, scrambling or water torture attack and Man-in-the Middle attack. WiMAX mobility with mobility support is more vulnerable to these attacks since the attackers do not need to exist in a fixed place so the E-Learning systems must be protected against these attacks.

3.1 Security problems at physical layer

The possible attacks in WiMAX network at physical layer is represented as follows

Jamming Attack:

Jamming attack occurs by introducing a cause of noise strong enough to significantly decrease the capacity of the channel. Jamming can be either planned or unintentional. It is not hard to perform a jamming attack because essential information and equipment’s are easy to acquire. Jamming is about reducing the channel capacity. Attacker introduce a source of noise strong enough to significant reduce the capacity of channel.

Scrambling Attack:

Scrambling attack is sort of jamming but for a short intervals of time. It is targeted to a specific frames or parts of frames. Scramblers can choose what they want to scramble i.e. control information or organization information to affect the normal operations of the network. Scrambling becomes a major problem when the network deals with time sensitive messages.

Water Torture Attack:

This is a typical attack in which an attacker forces a SS to drain its battery or consume computing resources by sending a series of bogus frames. This kind of attack is considered even more destructive than a typical Denial-of-Service (DoS) attack since the SS which is a usually portable device is likely to have limited resources.

Man-in-the-Middle attack:

Man-in-the-Middle attack (MIMS) intercepts a connection between two systems. It occurs when security mechanism implementation does not provide mutual authentication.

Replay attack:
A replay attack is a form of system attack in which a valid data transmission is unkindly or fraudulently repeated or belated. This is carried out either by the creator or by an challenger who intercepts the data and retransmits it, possibly as part of a deception attack by IP packet substitution.

Forgery Attack:
This type of attack occurs when an attacker with an sufficient radio transmitter can write to a wireless channel without proper approval to access the channel.

3.2 Security problems at MAC Sub Layer

MAC privacy sub-layer helps in the authentication of network access and connection setup. It helps in the key exchange, encryption of data. MAC layer is is vulnerable to the following attacks,

Denial Of Service Attacks:
A Denial of Service (DoS) attack is one that attempts to prevent the injured party from being able to use all or part of the network link. Denial of service attacks may spread wider to all layers of the protocol stack. The aim of the service is availability or authorized users' access to a service provider.

Downgrade Attack:
The initial message of the authorization process is an unsecured message from MS telling BS what security capabilities it has to face the problem of attacks. An attacker could, therefore, send a spoofed message to BS containing weaker capabilities in order to convince the BS and the attacked MS to agree on an insecure encryption algorithm.

Bandwidth spoofing:
This kind of attack occurs when an attacker grabs the available bandwidth by sending the unnecessary BW request message to BS.

4. Threats to authentication

Many serious threats also arise from the WiMAX’s authentication scheme in which masquerading and attacks on the authentication protocol of PKM are the most considerable.

Masquerading threat:
Masquerade attack is a type of attack in which one system assumes the identity of another. WiMAX supports unilateral device level authentication which is a RSA/X.509 certificate based authentication. The certificate can be programmed in a device by the manufacturer. Therefore sniffing and spoofing can make a masquerade attack possible. Specifically, there are two techniques to perform this attack: identity theft and rogue BS attack.

Identity theft:
An attacker may reprogram a device with the hardware address of another device. The address can be stolen by interfering the management messages.

Rogue BS attack:
SS can be compromised by a forged BS which imitates a legitimate BS. The rogue BS makes the SSs believing that they are connected to the legitimate BS, thus it can intercept SSs’ whole information. In IEEE 802.16 using PKMv1, the lack of mutual authentication prevents confirming the authentication of BS and makes Man-In-The-Middle (MITM) attack through rogue BS possible by sniffing Auth-related message from SS. However, it is difficult to successfully perform this kind of attack in WiMAX which supports mutual authentication by using PKMv2.

5. Attacks on the authentication protocols of basic PKM in 802.16 and its later version-PKMv2:

By adopting new version of PKM[5], WiMAX fixes many flaws in PKMv1 such as vulnerability to MITM due to the lack of mutual authentication. However, the newly proposed PKMv2 has been found to be also vulnerable to new attacks.

5.1 Attacks on basic PKM authentication protocol:
Attacker can intercept and save the messages sent by a legal SS and then perform a replay attack against the

BS. The SS also might face with this kind of attack. In the worse case, since mutual authentication is not supported in basic PKM, BS is not authenticated. Therefore malicious BS can perform a MITM attack by making its own Auth-Reply message and gain the control of the communication of victim .

5.2Attacks on Intel Nonce Version PKM:

In this version, nonce is a possible alternative to timestamp in authentication protocol. This approach does not protect a BS from a replay attack.

5.3 Attacks on PKMv2:

This version provides a three-way authentication with a confirmation message from SS to BS. There are two possible attacks as follows. First, a replay attack can be performed if there is no signature by SS. Second, even with the signature form SS, an interleaving attack is still possible.

6. Security mechanism in WiMAX based E-Learning

The whole security mechanism of WiMAX technology is defined by SA (Security Association), PKM Authorization, Privacy and Key Management and Data Encryption. Security policies are enforced by the BS to the SS, so it can only access authorized SA that respects the characteristic of that type of service.

Mutual Authentication:

Mutual authentication refers to two parties authenticating each other suitably. It refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity. Mutual authentication is frequently referred to as website-to-user authentication, or vice versa.

Key Management:

Key management deals with secure creation, sharing and storage of keys. Secure methods of key management are extremely important. Once a key is randomly generated it remains secret for to avoid unfortunate mishaps. In practice most attacks on public key system will be probably aimed at the key management level, rather than cryptographic algorithm itself. Users must be able to securely obtain a key pair suited to efficiency and security needs. Key management in multicast dynamic groups, where users in the network can leave or join at their ease is one of the most crucial and essential part of secure communication.

Encryption:

Also the amendment of 802.16e provided support for the Advanced Encryption Standard cipher leading to confidentiality of data traffic. Like Wireless-Lan standard management frames are not encrypted which gives support to an attacker to collect information about subscribers in the area range as well as other and other crucial characteristics of network.

Secure Multicast:

The challenge of a secure multicast service, such as the one included in IEEE 802.16, is to provide an efficient method for controlling access to the group and its communications. Encryption of group messages and selective distribution of the keys used for encryption is the primary method for ensuring the security. For a active group in which the membership changes regularly, the rekeying algorithm is a serious factor in overall service efficiency. MBRA algorithm should guarantee forward secrecy, which prevents a leaving member from accessing future communications; and backward secrecy, which prevents a joining member from accessing former communications. Additionally, a rekeying algorithm should be efficient as well.

7. Conclusion

In this paper WiMAX security issues that occur in PHY & MAC layer are discussed along with the possible solutions. WiMAX has the capability to attain success in wireless communication arena. We also analyzed various security mechanism in WiMAX for secured communication of messages, authentication.

References

[1]IEEE std 802.16e, 2006, IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Amendment and Corrigendum to IEEE Std 802.16-2004, IEEE Press.

[2] A. Deininger, S. Kiyomoto, J. Kurihara, T. Tanaka,2007, Security vulnerabilities and solutions in mobile WiMAX, IJCSNS International Journal of Computer Science and Network Security Vol.7.No 11.

[3] Perularaja Rengaraju, Chung-Horng Lung, Yi Qu,Anand Srinivasan,2009, Analysis on Mobile WiMAX Security, IEEETIC-STH, Information Assurance in Security and Privacy.

[4] Fuden Tshering,Anjali Sharma,2011,A Review of Privacy and Key Management Protocol in IEEE 802.16e,International Journal of Computer Applications.

[5] Noudjoud Kahya, Naara Ghoualmi, Pascal Lafourcade,2012, Key Management Protocol in WiMAX Revisited,Springer.