**Security in WiMAX**

**Introduction:**

WiMAX (Worldwide interoperability for microwave access) also called as wireless metropolitan area network(WMAN). Also WiMAX is also defined based on IEEE 802.16 standard. Main aim of IEEE 802.16 is to provide wireless network over miles on behalf of cable network. WiMAX technology was first introducing in 2001.WiMAX main entities which are used in communications are Base Station(BS), Subscriber Station(SS), Mobile Station(MS), Relay Station(RS) and Operator Network.

BS is main component in WiMAX network. BS station operates all components of networks. All networks components need to register in BS station. Also BS helps to maintain communication between all components of network and network operator. SS works as stationary stations and also like RS.MS is main users of WiMAX network. MS is device which wants communicate with network operator via RS and BS. Example of MS are mobile and laptops.RS are SS configured worked for forward traffic to other BS or RS. Radio access and IP connectivity services are providing by Network operator. Whole WiMAX network, mainly communicate with each other by only two types of messages. One is data message and other is management message. Data message used to transport data across the network components. And management message use to manage communication between BS and SS/MS. WiMAX networks work on radio frequency. WiMAX networks contain basic four topologies. 1) Point to Point(P2P) 2) Point to MultiPoint (P2M) 3) Multi hop Relay 4) Mobile topology.

**WiMAX Architecture**

WiMAX contains main three parts in architecture.1) Mobile Station(MS) 2) Access Service Network(ASN)3) Connectivity Service Network(CSN). WiMAX contain mainly two types of architectures. Standard WiMAX architecture and two dimensions’ architecture. In standard architecture contain central IP core which is operate ASN gateway and component of CSN. ASN works for BS and RS which provides network access to MS. In WiMAX architecture main authentication service to MS by CSN. CSN also provide service to manage IP address. IP core work middle layer of CSN and ASN. In WiMAX two dimensions’ architecture have main two components WiMAX tower and WiMAX receiver. Main WiMAX tower is directly wired connected with internet backbone. Most of connection in networks are two types some are line of sight and some are non-line of sight connection.

**Security Feature of WiMAX**

WiMAX (IEEE 802.16) works on only two security services. 1) authentication 2) Confidentiality. In WiMAX, Authentication service used for authenticate device which wants to connect network. Confidentiality service used to protect data messages which send over network. We cannot get any other security service over IEEE 802.16 network. If we want to use other service, we need to get from other provider. WiMAX uses just three steps to provide secure connection. First step will be authentication then key establishment and data encryption. In authentication process keys exchange done between BS and MS/SS. Those keys can be used for secure data exchange.



**WiMAX security framework**

**Security Associations (SA):**

There are some security parameters shared by MS/SS and BS for secure communication that called security association. There should be unique SA for every service offered by BS. Every BS contain mainly two SA, one for unique encryption SA and other is unique group SA for multicast service.

Authorization process attributes of SA

* X 509 Certificates: this certificate used for validate users which are using WiMAX service. Third party or some time manufacture sign certificates.
* Authorization Key: Authorization key(AK) should be exchange between MS/SS and BS prior to data transfer. AK contain unique number and lifetime of AK.
* Key Encryption Key: KEK calculate from AK.
* Message Authentication Keys: MAK calculate from AK. Which used for to validate the authenticity of key to distribute message during key.
* Authorized data SA list: this list is provided to MS/SA by BS. That contain all SAs information of BS.
* SA identifier: 16-bit unique number of SA to differentiate from other SAs.

**Authentication and authorization:**

Authorization process provides information of how many level access of nodes after authentication of that node. In IEEE 802.16 authorization process give authentication and some level of access to WiMAX nodes(MS/SS). The Privacy Management Key(PMK) protocol used for authentication and authorization in WiMAX network. PKM used authenticate system entities by authorize by SA. In this process first BS authenticate SS by doing one-way authentication process. In process SS send message with information about x.509 certificate of manufacturer of SS and cryptographically algorithm which SS support and SAID. In next step BS validate the information about the x.509 certificate. And send back the AK of SS with AK lifetime. The upgrade protocol version 1.5 support remote authentication dial-in services for authentication, authorization and accounting. In that, device level authentication done by x**.**509 certificates and transport layer security. In new protocol first EAP exchange between SS/MS and Remote AAA server. Using that MS/SS and BS get 512 bit MSK. Which is useful in authentication and authorization of MS/SS.

Once authentication and authorization process complete, BS and SS/MS share an activated Authentication Key(AK). They will use this AK to get information about 160-bit authentication key of message and 128 bit KEK. In first step, SS/MS get some TKE message from BS. After that MS/SS send request to BS as TKE-Request. Once BS get message of TKE -request BS check the random number with random number send in TKE- challenges.

**The privacy and key management (PKM) authorization protocol:**

Authorized SS can get authorization keys by PKM authorization protocol. Key distribution is just done in three steps.

* In first message SS send security information message to BS.BS will decide that SS is trusted one or not.
* In second message also SS send information about capacity and his unique id for registration in BS.
* In third message BS send authentication reply with required information for SS.

Once authentication process complete SS wants to make data SA between it and BS.in this process also they are using PKM protocol.

**Threats and Vulnerabilities in WiMAX**

Every system contains some threats. Thought we improve protocol; it contains some threats in network.

* In PKMv1, we all see that authentication only one direction process from SS to BS, not from BS to SS. Due to that some time attacker create threated BS which work as BS for SS and get information of network.
* As we know that we only encrypt data message in this protocol to increase efficiency of network. Management messages are not encrypted. attacker just put their eyes on this type messages over the network.
* Here we are just using simple encryption algorithms likes DES-CBC. These are very simple and no longer industry using these algorithms.
* In TEK, IEEE 802.16 standard use only 2-bit of encryption sequence. By 2 bit we get only 4 possible combination of sequence. On other hand attacker easily break that encrypted message by TEK. This problem is resolved in latest version.
* SS/MS just need to use devise manufacture x.509 certificates, which limiting in practical use.
* Rf Jamming attack we can experience in every network over wireless. RF jamming basically attack when system use radio frequency used by WiMAX.
* WiMAX system suffer from Danial of Service(DOS) attacks. Hacker can attack by multiple ways using DOS something like, request/response message ranging, sometime using mobile advertisements.
* Scrambling attacks injection on RF interference during the transferring important data about management message. Scrambling attack is more hard than jamming.

**Security Issues Solutions:**

* As solution of DOS attack, we need to improve authentication and authorization protocol of WiMAX, we can add timestamp and signature in messages of PKM protocol. By using these extra fields BS and SS can get information about how much fresh is message.
* We can improve security by using RSA algorithms a mac layer for authentication and authorization. In this SS/MS can work something like client and BS can work as server. So they exchange authorization message like client-server.
* We can implement hash based authentication and authorization to improve security.

**Conclusion:**

WiMAX is technology which we can use in metropolitan area network. WiMAX is more similar to Wi-Fi network but it is more powerful and covered more area then Wi-Fi network. We know that security is very big problem in WiMAX technology, but the benefits of technology make good position for itself. We have some proposal on security threats problems solution, we can implement these.

**Reference**:

[1] Mohammed El-Gammal, “Overview of WiMAX security”.

[2] Steven J. Vaughan-Nichols, “Achieving Wireless Broadband with WiMax”.

[3] M Alzaabi, K D Ranjeeth, T Alukaidey, Dr K Salman, “SECURITY ALGORITHMS FOR WIMAX”, IJNSA, May 2013.

[4] Karen Scarfone, Cyrus Tibbs, Matthew Sexton, “Guide to Securing WiMAX Wireless Communications” Sep 2010.