A Review on Authentication and Privacy Key Management Protocol in WiMax

G. Rama Subba Reddy
Research Scholar, Department of Computer Science and Engineering, SunRise University, Alwar, Rajasthan, India

DOI: 10.23956/ijarcsse/V7I6/0338

Abstract: IEEE 802.16a-2003 WiMax is the Worldwide Interoperability for Microwave Access is a new technology dealing with provision of data over long distance using wireless communication method in many different ways. WiMax is used for the wireless network. This technology is going to be an emerging technology for wireless technology in future. It is similar to Wi-Fi but its area of coverage and bandwidth is much higher than the Wi-Fi. So the security become very important issue. WiMax technology includes some security features such as Privacy Key management, Authentication and confidentiality. For security first priority is across wireless network and other is to provide access control to the network and the access control can be provided using access control protocols.

Keywords: WiMax, Security, Privacy Key management, Authentication

I. INTRODUCTION

The IEEE 802.16 is the standard for the Wireless Metropolitan Area Network (WMAN), better known as WiMAX (Worldwide Interoperability Microwave Access). WiMAX Forum is on a mission to advance and certify compatibility and interoperability of broadband wireless products based on IEEE 802.16 family standards. The standard IEEE 802.16 gives the specifications for the air interface allowing point-to-point and PMP BWA in the 10-66 GHz frequency band under line-of-sight (LOS) conditions. In 2004, IEEE 802.16d [1] was published to address the requirements of fixed BWA under nonline-of-sight (NLOS) conditions. An amendment to IEEE 802.16d was drafted in 2005 as IEEE 802.16e [2] to increase the scope of WiMAX which provide support for mobility of mobile subscriber stations (MS) moving at a vehicular speed up to 150km/h.

The key feature of WiMAX networks is that the security layer is built into the protocol stack instead of being added on later. The messages for authentication and key exchange are defined as part of the medium access control (MAC) layer. The MAC layer performs encryption based on the keys negotiated during the key exchange phase. The IEEE 802.16d standard defines the security mechanisms for fixed network. The security architecture of the IEEE 802.16d standard is based on PKMv1 (Privacy and Key Management) protocol. The IEEE 802.16e standard defines the enhanced security mechanisms for the mobile network. The security architecture of the IEEE 802.16e is based on PKMv2 protocol which resolved most of the issues present in the IEEE 802.16d, with a major improvement in mutual authentication.

II. WIMAX LAYER ARCHITECTURE

Fig. 1 WiMax Layer architecture IEEE 802.16

Basically WiMAX Layer Architecture consists of Two layers.They are
1)Physical layer
2)Datalink Layer

Physical layer
The IEEE 802.16 physical layer protocols include multiple specifications, defined through several amendments and revisions, each appropriate for a particular frequency range and application. The IEEE 802.16 compliant devices include mobile stations or base stations.
It is responsible for receiving MAC frame.
In this we used OFDMA (orthogonal frequency division multiplexing technique).
It supports both full duplex and half duplex transmission.
It uses TDD and FDD techniques.

**Datalink Layer**
The data link layer of IEEE 802.16 standard comprises three sub-layers
I. MAC CS (convergence sub layer)
II. MAC CPS (common part sub layer)
III. Security sub layer

**Medium Access Control Service Specific Convergence Sublayer (MAC CS)**
The service-specific convergence sub-layer (CS) provides any transformation or mapping of network-layer data packets into MAC SDUs. On the transmitter side, the CS receives the data packets through the CS Service Access Point (SAP) and delivers MAC SDUs to the MAC Common Part Sub-layer (MAC CPS) through the MAC SAP.

**Medium Access Control Common Part Sub layer (MAC CPS)**
The MAC CPS provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. It can receive data from the various convergence sub-layers, through the MAC SAP classified into particular MAC connections.

**Security sub layer**
The MAC also contains a separate security sub-layer providing authentication, secure key exchange, and encryption. It used two protocol for maintain security in Wi-Max
- Encryption protocol: used for encryption data packet.
- PKM protocol: used for key management and authentication technique.

### III. WIMAX NETWORK ARCHITECTURE

![WiMAX Network Architecture](image)

**Fig. 2 WiMAX Network Architecture**

WiMAX architecture consists of two types of fixed (non mobile) stations:
- Subscriber Stations (SS): serves a building (business or residence)
- Base station (BS): connects to public network and provide SS with first-mile access to public networks

The communication path between SS and BS has two directions:
- Uplink (from SS to BS)
- Downlink (from BS to SS)

### IV. WIMAX SECURITY PROTOCOLS

The security protocol provides mechanisms to ensure confidentiality, integrity and client authentication with the implementation of a PKM. PKM provides secure key distribution between BS and SS. The PKM uses security associations (SAs) of which there are two types [5]:
(a) Data SA specifies the messages encryption algorithm and the keys to be used and related information. Each data SA includes an ID (SAID), an encryption algorithm to protect the confidentiality of messages, traffic-encryption key (TEK), a TEK identifier, a lifetime for the TEK, and an indication of the type of data SA (primary or dynamic);
(b) Authorization SA includes a credential, an authorization key (AK) to authorize the use of the links, an identifier for the AK, a lifetime for the AK, a key-encryption key (KEK), a downlink hash-based message authentication code (DHMAC), an uplink hash code (UHMAC), and a list of authorized data SAs. The WiMAX communications follow the security procedure in phases to ensure secure access of a connection [6].
**Phase 1 (SS Authentication and Authorization):** To establish the genuine identity of the SS wishing to join BS, the SS sends Authentication Information message containing the X.509 certificate to BS. The X.509 is used in the public key cryptography and the digital signatures. The certificate contains information like version, a serial number, the certificate issuer, validity period, public key of SS etcetera. The BS may choose to ignore this message. Then SS sends authorization request to BS. It contains the X.509 certificate, the description of the requesting SS’s cryptographic capabilities that SS supports and the SS’s Basic CID (connection ID), which is the first static CID assigned by the BS to SS during initial ranging. After receiving this message, BS authorizes the SS via X.509 certificate and sends authorization reply message back containing AK (authorization key), AK sequence number, AK lifetime and SA descriptors.

**Phase 2 (TEK exchange):** After AK exchange the SS derives three keys. (a) KEK for the encryption of the TEK, that BS sends to each SS. TEKs are used for the data encryption to ensure confidentiality. (b) DHMAC key for derivation of the HMAC digest of the management messages sent by the BS to the SS and the SS uses this key to verify the HMAC Digest of the messages received from BS. (c) UHMAC key for derivation of the HMAC digest of the management messages sent by the SS to the BS and the BS uses this key to verify the HMAC Digest of the messages received from SS. For each SAID, the authenticated SS starts a separate TEK process. The TEK process periodically (TEK’s lifetime varies between 30 minutes and 7 days) sends TEK key request messages to the BS, requesting a refresh of keying material. The BS responds to the key request message with a key reply message which contains TEK sequence number, TEK’s SAID, the old and new TEK encrypted with KEK and the digest of the message with the UHMAC key.

**Phase 3 (Encrypted Data Traffic):** After the completion of authorization and initial key exchange, data transmission between the BS and the SS starts by using the TEK for encryption. The data encryption is done based on the TEK length, DES in Cipher Block Chaining (CBC) mode using a 56-bit key with 64-bit block encryption along with the 64-bit IV (initialization vector), AES in CCM mode with 128-bit key and 128-bit block size and AES in CBC mode with 128-bit TEK key and 128-bit block size.

### V. COMPARING WITH OTHER WIRELESS TECHNOLOGIES

<table>
<thead>
<tr>
<th></th>
<th>802.11 Wi-Fi</th>
<th>802.16 WiMax</th>
<th>802.20 Mobile-Fi</th>
<th>UMTS 3G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>11-54Mbps</td>
<td>Upto 70Mbps</td>
<td>Upto 1.5Mbps</td>
<td>384Kbps-2Mbps</td>
</tr>
<tr>
<td>Range(LOS)</td>
<td>100meters</td>
<td>30-50Km</td>
<td>3-8Km</td>
<td>Coverage is overlaid on wireless infrastructure</td>
</tr>
<tr>
<td>Frequency/Spectrum</td>
<td>2.4GHz for 802.11b/g</td>
<td>2-11 GHz for 802.16a</td>
<td>11-60 GHz for 802.16</td>
<td>&lt;3.5GHz</td>
</tr>
<tr>
<td>Standardization</td>
<td>802.11a,b and g</td>
<td>802.16, 802.16a and, 802.16</td>
<td>802.20 In Development</td>
<td>Part of GSM standard</td>
</tr>
<tr>
<td>Mobility</td>
<td>Portable</td>
<td>Fixed(Mobile-16e)</td>
<td>Full Mobility</td>
<td>Full Mobility</td>
</tr>
</tbody>
</table>

Fig. 4 Comparing with other Wireless Technologies
VI. SECURITY ISSUES AND SOLUTIONS

In this section we will present some security issues for WiMAX found in literature and discuss which solutions are proposed for these issues.

1. DOS (DENIAL OF SERVICE) /REPLAY ATTACK

In [LL06] the following DoS attack is described. If a SS sends a lot of false authorization requests to a BS, the BS will use all its resources to calculate whether the certificate is right. This will cause a DoS, because BS will not be able to serve any SSs anymore. Another DoS attack possibility is described in [XMH06], where an adversary eavesdrops the authentication message from a SS to a BS. Then he replays this message multiple times to the BS, which will make the BS ignore the SS and thus creating a Denial of Service.

In the first type of DoS attack, the BS will not be able to serve any SSs anymore. In the second type of DoS attack, only the SS whose message got eavesdropped will experience the attack.

In this solution some modifications to the authentication protocol and the key management protocol are proposed to solve both this security issue and the authorization vulnerability issue, see Section 2.

2. AUTHORIZATION VULNERABILITY

In [LL06] is emphasized that WiMAX uses mutual authentication to protect from forgery attacks, but the authorization process is still vulnerable because there is no way to ensure integrity of the messages. Anyone with a properly placed radio receiver can catch an authorization message, modify and retransmit it. There is no digest used to prove that the message has not been modified.

3. KEY SPACE VULNERABILITY

In 802.16e, a 4-bit key sequence number is used to distinguish between successive generations of AKs. Also, a 2-bit key sequence number is used for the same purpose with TEKs. The size of the key is insufficient to protect the keying material from attacks according to [LL06].

4. DOWNGRADE ATTACK

The first message of the authorization process is an unsecured message from SS telling BS what security capabilities he has. An attacker, see [MPF07], could send a spoofed message to BS containing weaker capabilities in order to convince the BS and the attacked SS to agree on an insecure encryption algorithm. The standard does not specify a concrete solution for the situation that two valid answers are received by a BS.

5. AUTHORIZATION ATTACK

According to [HLY07] it is possible for a malicious radio receiver to make both an honest SS enter his network and to get permission to enter an honest BSs network. This can be done by recording messages and replaying them to the BS and SS. They describe the problem as “lack of clear clarification of intended receiver”.

6. WIRELESS PUBLIC KEY INFRASTRUCTURE (WPKI)

[LL06] proposes an enhancement to the 802.16e security called Wireless Public Key Infrastructure (WPKI). The two major changes are Elliptic Curve Cryptography (ECC) and Wireless Transport Layer Security (WTLS) certificates. ECC, as defined in [Cer00], will replace RSA [RSA02] as encryption method. The advantage of ECC is that the same encryption strength can be reached with a much smaller key size. WTLS defines a compressed certificate format, similar to X.509 [Hou02] but using smaller data structures.

7. PROBLEM FORMULATION

Wi-Max was security vulnerabilities in both PHY and MAC layers, presenting to different classes of wireless assault. Right now Wi-Max just characterizes the security instrument to ensure the correspondence which occurs in MAC layer. Be that as it may, there are no security instrument is characterized for the Physical layer. The authentication instrument in light of the EAP protocol is the tedious procedure. It is hard to bolster Real time application by EAP protocol.

VII. CONCLUSIONS

This paper started by describing what WiMAX is and especially how its authentication and authorization works. Then we looked at security issues and described the solutions proposed in the literature. Finally, we analyzed those solutions and concluded that a complete solution combining all solutions mentioned should be possible.

The next conclusion to be made is that although security in 802.16e is certainly not perfect yet, not many solutions have been proposed yet in literature. The explanation for this could be that the 802.16e standard was only published in 2006 and maybe we can expect to see more solutions coming up in 2008.

VIII. FUTURE WORK

Future work activities can be related on performance experiments of the listed solutions, in order to evaluate their performance and scalability. For the solution to the key space vulnerability, it will be necessary to find key sizes that provide a balance between security and performance/scalability.
REFERENCES

AUTHOR BIOGRAPHY
G. Rama Subha Reddy Pursuing Ph.D at Sunrise university, Alwar Rajasthan. Received his M.E (Computer Science &Engineering) from Sathyabama University, Chennai in 2010., his B.Tech degree in Computer Science and Information Technology from JNTUH Hyderabad in 2004. His research interests Computer Networks, Wireless Networks He is a member of ISTE, IAENG and ISRD.