WiMAX Security: Privacy Key Management

Nirwan Ansari
Advanced Networking Laboratory
Department of Electrical and Computer Engineering
New Jersey Institute of Technology
Newark, NJ 07102-1982, USA
Phone: +1-973-596-3670
Email: Nirwan.Ansari@njit.edu
http://web.njit.edu/~ansari

© 2007 Sendai International Workshop on Network Security and Wireless Communications
24 January 2007

Outline

- What's WiMAX?
  - WiMAX applications
  - WiMAX revolution
  - Advanced features of WiMAX
- WiMAX standards structure
  - PHY Layer
  - MAC Layer
- Security issues in WiMAX
  - Threats in WiMAX
  - Security mechanism in WiMAX
- Privacy and Key Management (PKM) in WiMAX
  - PKM v1
  - PKM v2
- Future research issues

Comparison with other wireless Technologies

Table:

<table>
<thead>
<tr>
<th></th>
<th>802.11 Wi-Fi</th>
<th>802.16 WiMAX</th>
<th>802.20 Mobile-Fi</th>
<th>UMTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>11-54 Mbps</td>
<td>75 Mbps</td>
<td>2-11 Mbps</td>
<td>384 Kbps – 2 Mbps</td>
</tr>
<tr>
<td>Range (LOS) Range (NLOS)</td>
<td>30 – 300 km</td>
<td>15 – 50 km</td>
<td>11-54 Mbps</td>
<td>Existing wireless spectrum</td>
</tr>
<tr>
<td>Frequency/Spectrum</td>
<td>2.4 GHz for 802.11 b/g</td>
<td>2-11 GHz for 802.16</td>
<td>5.2 GHz for 802.11a</td>
<td>2.4 GHz for 802.20</td>
</tr>
<tr>
<td>Licensing</td>
<td>Unlicensed</td>
<td>Both</td>
<td>Licensed</td>
<td>Licensed</td>
</tr>
<tr>
<td>Standardization</td>
<td>802.11a, b and g</td>
<td>802.16, 802.16a and 802.16b</td>
<td>802.20 in development</td>
<td>Part of GSM standard</td>
</tr>
<tr>
<td>Mobility</td>
<td>Portable</td>
<td>Fixed (Mobile – 16c)</td>
<td>Full mobility</td>
<td>Full mobility</td>
</tr>
</tbody>
</table>
Integrated Funct. Specifications for 10-66 GHz (amendment 1)

Advanced features in WiMAX

High Data Rates: support peak DL data rates up to 63 Mbps per sector and peak UL data rates up to 28 Mbps per sector in a 10 MHz channel.

Quality of Service (QoS): define Service Flows which can map to DiffServ code points or MPLS flow labels that enable end-to-end IP based QoS. Also provide a flexible mechanism for optimal scheduling of space, frequency and time resources over the air interface on a frame-by-frame basis.

Outline

- What’s WiMAX?
- WiMAX standard protocol structure
  - Supports multiple services
  - Covers MAC layer and PHY layer
- WiMAX standards structure
  - PHY Layer
  - MAC Layer
- Security issues in WiMAX
- Privacy and Key Management (PKM) in WiMAX
- Future research issues

IEEE 802.16 Specifications

- Original fixed wireless broadband air Interface for 10 - 66 GHz: Line-of-sight only, Point-to-Multi-Point applications.
- 802.16 Amendment 10 - 66 GHz, system profiles
- Extension for 2-11 GHz: non-line-of-sight, Point-to-Multi-Point applications like “last mile” broadband access; define mesh mode.
- Revise and combine previous 802.16 standards
- MAC/PHY Enhancements to support subscribers moving at vehicular speeds

Timelines in WiMAX
**PHY Layer**

- Burst single-carrier modulation with adaptive data burst profiles
  - Transmission parameters can be modified on a frame-by-frame basis for each SS.
  - Profiles are identified by "Interval Usage Code" (DIUC and UIUC)
- Use of Adaptive Antenna System
  - Improve range
- Use of two different duplexing schemes
  - Frequency Division Duplexing (FDD)
  - Time Division Duplexing (TDD)
- Support for both full and half duplex stations

**MPDU data format**

- MPDU (MAC Protocol Data Unit) consists of a MAC header, service data, and an optional cyclic redundancy check (CRC).

<table>
<thead>
<tr>
<th>MPDU Type</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic MAC header</td>
<td>MAC Service Data Unit (MSDU)</td>
</tr>
</tbody>
</table>

**PHY Layer (cont’d)**

- WiMAX PHY layer supports significant flexible operations across a wide range of spectrum allocations.
- WiMAX defines a common MAC layer feature set, including initial ranging, network entry, bandwidth requests, and connection-oriented channels for management and transport connections.

**MAC CS Sub-layer**

CS performs the following functions:

- Accepting higher-layer protocol data units (PDUs) from the higher layer
- Performing classification of higher-layer PDUs
- Processing (if required) the higher-layer PDUs based on the classification
- Delivering CS PDUs to the appropriate MAC SAP (service access point)
- Receiving CS PDUs from the peer entity.

**MAC Layer**

- Mode: Point-to-Multipoint and optional mesh topology
- Connection-oriented
  - Connection ID (CID), Service Flows (FS)
- MAC layer is further subdivided into:
  - Convergence Sublayer (CS)
  - Common Part Sublayer (CPS)
  - Security Sublayer

**MAC CPS Sub-layer**

- The MAC CPS provides the core MAC functionality:
  - system access
  - bandwidth allocation
  - connection establishment
  - connection maintenance
MAC Security Sub-layer

MAC Security Sub-layer provides access control and confidentiality across the broadband wireless network through:
- Encryption
- Privacy and Key management

Outline

- What's WiMAX?
- WiMAX standards structure
- Security issues in WiMAX
  - Threats in WiMAX
  - Security mechanism in WiMAX
- Privacy and Key Management (PKM) in WiMAX
- Future research issues

Identity Attack in WiMAX

- Identity theft consists of reprogramming a device with the hardware address of another device.
- This is a well-known problem in unlicensed services such as WiFi/802.11, but has been under control in cellular networks because it is more difficult to execute with subscriber ID module (SIM) cards.
- The address can be stolen over the air by intercepting management messages.

Identity Attack in WiMAX (cont'd)

- Enterprise/Building
- Scenario: Bob communicates with his office.
- Step 1: Alice intercepts transmission between a victim and his office.
- Note: Insecure management packets between a non-LOS base station and a victim is usually the target.
- Step 2: Alice reprograms her device with Bob's profile (e.g., MAC address and ID).
- Step 3: Alice impersonates Bob to the base station and uses Bob's identity for her own transmission.
- Note: Usually Alice attacks Bob by flooding/DDoS/other attacks so Bob is temporarily disconnected with the base station.

Security Threats in WMAN

- PHY threats
  - Water torture attack, jamming, etc.
  - No protection.
- MAC threats
  - Typical threats of any wireless network
    - Sniffing, Masquerading, Content modification, Rouge Base Stations, DoS attacks, etc.
  - 802.16e: no constraints of attackers' location, management msg. more vulnerable.
Eavesdropping Attack in WiMAX

- Management messages (never encrypted) can provide valuable information to an attacker.
- There are no serious technical difficulties to resolve by an attacker.
- From the user perspective, eavesdropping of management messages may result in limited financial loss.
- Eavesdropping of management messages is a critical threat to both users and the system.
- Eavesdropping of traffic is a minor threat.

Eavesdropping Attack in WiMAX (cont’d)

Scenario: Bob communicates with his office.
Step: Alice eavesdrops Bob’s communications with his office (eavesdropping of data traffic) as well as with a base station (network management traffic).

Security Sublayer

MAC Security specifies the following two components:
- An encapsulation protocol for securing packet data across the BWA network.
  - a set of supported cryptographic suites
  - the rules for applying these algorithms to a MAC PDU payload.
- A key management protocol (PKM) providing the secure distribution of keying data from the BS to the SS.

Security mechanisms in WiMAX

- Authentication
- Access control
- Message encryption
- Message modification detection (Integrity)
- Message replay protection
- Key management

Outline

- What’s WiMAX?
- WiMAX standards structure
- Security issues in WiMAX
- Privacy and Key Management (PKM) in WiMAX
  - PKM v1
    - Authentication
    - Key exchange
    - Data Encryption
  - PKM v2
    - The mutual authorization process
    - Key exchange with RSA
    - Key exchange with EAP
- Future research issues

Protocol stack of the Security Sublayer

The privacy key management (PKM) protocol in the middle provides secure distribution of keying data from the BS to the SS.
PKM

- An SS uses the PKM protocol to obtain authorization and traffic keying material from the BS, and to support periodic reauthorization and key refresh.

- PKM supports two distinct authentication protocol mechanisms:
  - RSA protocol (support is mandatory in PKMv1)
  - Extensible Authentication Protocol (optional unless specifically required).

Keys used in PKM

- Five kinds of keys used to secure WiMAX communications:
  - Authentication Key (AK)
  - Key Encryption Key (KEK)
  - downlink hash function-based message authentication code (HMAC) key
  - uplink HMAC key
  - Traffic Encryption Key (TEK)

WiMAX security procedure

1. (re)Authentication
2. Key exchange
3. Data encryption

PKM: Authentication

- Authorization Information
  - [Manufacturer’s X.509 Certificate]
- Authorization Request
  - [SS’s Certificate | Security capabilities | SAID]
- Authorization Reply
  - [RSA encrypted (SS’s public key, AK) | key lifetime | Seq. No. | SAID(16)]

The key derivation process

- KEK = \text{Truncate} \_128(\text{SHA1}((\text{AK} \oplus 0^{53})))

- The downlink HMAC key and uplink HMAC key are generated from the AK in a similar way.

WiMAX security procedure (cont’d)
Data Key Exchange

- Traffic Encryption Key (TEK)
- TEK is generated by BS randomly
- TEK is encrypted with
  - Triple-DES (use 128 bits KEK)
  - RSA (use SS’s public key)
  - AES (use 128 bits KEK)
- Key Exchange message is authenticated by HMAC-SHA1

Data Encryption

- WiMAX MAC layer encrypts only data messages not management messages.
- Data Encryption Standard with Cipher Block Changing (DES-CBC)
  - Check the SA associated with the current connection and acquire the initialization vector (IV).
  - Encrypt the MPDU plaintext payload by employing the generated MPDU IV and the authenticated TEKs.
  - Set Encryption Control (EC) field of the MAC header to 1 to indicate that the payload in the MPDU is encrypted.
  - Use the 2-bit Encryption Key Sequence (EKS) to indicate which TEK is used.
  - Update the CRC field in accordance with changes in both the payload and MAC header.

The TEK exchange procedure

WiMAX MPDU encryption process

WiMAX security procedure (cont’d)

Security flaws in PKMv1

- Need for mutual authentication: authentication is one way
  - BS authenticates SS
  - No way for SS to authenticate BS
  - Rouge BS
- Authentication Key (AK) generation
  - BS generates AK
  - No contribution from SS
  - SS must trust BS for the generation of AK
PKMv2

- PKMv2, defined in IEEE 802.16e-2005, enhances PKMv1 by requiring mutual authentication between SS and BS.
- PKMv2 has also more enhanced security features such as new key hierarchy for AK derivation and Extensible Authentication Protocol (EAP).

PKMv2 (cont’d)

- The PKMv2 key hierarchy defines the key category and the algorithms used to generate keys.
- The authentication and authorization processes generate source key materials.
- All PKMv2 key derivations are based on the Dot16KDF algorithm.
- Support two authorization schemes
  - RSA-based authorization process
  - EAP-based authentication process
- AK is derived from PAK and PMK in RSA- and in EAP-based authorization procedure, respectively.

PKMv2: The mutual authorization process

- Authorization Request
  - RNs | SS Certificate | Security capabilities | SAID
- Authorization Reply
  - RNs | RNB | pre-PAK (SS’s public key) | key lifetime | seq No | SAIDList | AKID | BS certificate | SIG (BS)
- Authorization Information
  - Manufacturer SS Certificate
- Verify SS certificate
- Verify BS certificate

PKMv2: authorization messages

<table>
<thead>
<tr>
<th>Authorization Request Message</th>
<th>Authorization Reply Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>A manufacturer-issued X.509 certificate.</td>
<td>The BS’s X.509 certificate, used to verify the BS’s identity.</td>
</tr>
<tr>
<td>The security capabilities the requesting SS supports.</td>
<td>A pre-PAK encrypted with the SS’s public key.</td>
</tr>
<tr>
<td>The SS’s Basic CID, which is the first static CID the BS assigns to an SS during initial ranging.</td>
<td>A 4-bit PAK sequence number</td>
</tr>
<tr>
<td>A 64-bit random number ( N_j ) generated by the SS.</td>
<td>The lifetime of the pre-PAK.</td>
</tr>
<tr>
<td>The identities (i.e., the SAIDs).</td>
<td>The 64-bit random number generated by the SS.</td>
</tr>
<tr>
<td>The BS’s signature.</td>
<td>A 64-bit random number ( N_j ) generated by the BS.</td>
</tr>
</tbody>
</table>

AK derivation in RSA-based authorization

- RSA authorization succeed
- Pre-PAK (BS’s public key)
- EAP exchange
- MSK — 512 bits

AK derivation in EAP authorization

- RSA authorization succeed
- Pre-PAK (BS’s public key)
- EAP exchange
- MSK — 512 bits
- PMK = Truncate (MSK, 160)
- AK = Dot16KDF(PMK, SS MAC Address | BH | "AK", 160)
Outline

- What’s WiMAX?
- WiMAX standards structure
- Security issues in WiMAX
- Privacy and Key Management (PKM) in WiMAX
- Future research issues

Advanced Security Issues in WiMAX

- Since the MAC management messages are transmitted without encryption, valuable information can be given away to attackers.
- It is easy for an attacker to interject reused TEKs.
- Predictable IV impairs data security.
- The DES-CBC algorithm can only secure limited length of data.

For further studies