THEME 5

WIMAX Security

Telecommunication systems department

Lecturer: assistant professor Persikov Anatoliy Valentinovich

PURPOSE OF THE WIMAX TECHNOLOGY

WiMAX technology is a **wireless metropolitan area network** (WMAN) communications technology that is largely based on the wireless interface defined in the IEEE 802.16 standard. The industry trade association, the **WiMAX Forum**, coined the WiMAX trademark and defines the precise content and scope of WiMAX technology through technical specifications that it creates and publishes.

The **original purpose of IEEE 802.16 technology** was to provide last-mile broadband wireless access as an alternative to cable, digital subscriber line-, or T1 service. Developments in the IEEE 802.16 standard shifted the technology's focus toward a more cellular-like, mobile architecture to serve a broader market. Today, WiMAX technology continues to adapt to market demands and provide enhanced user mobility.

WIMAX STANDARDS

The IEEE amendment that enabled mobile WiMAX operations is **IEEE 802.16e-2005**.

Prior to its release, deployment of WiMAX networks was limited to fixed operations by the **IEEE 802.16-2004** standard.

Additionally, IEEE 802.16e-2005 provided significant security enhancements to its predecessor by incorporating more robust mutual authentication mechanisms, as well as support for Advanced Encryption Standard (AES). Although the IEEE 802.16-2004 and 802.16e-2005 standards were released within a year of each other, IEEE 802.16e-2005 product certification did not start until 2008, and **IEEE 802.16-2004 products are still used in today's information technology (IT) environments**. The most recently ratified standard is **IEEE 802.16-2009**, which consolidated IEEE 802.16-2004, IEEE 802.16e-2005, and other IEEE 802.16 amendments from 2004 through 2008.

IEEE also released **IEEE 802.16j-2009** to specify multi-hop relay networking. This publication addresses IEEE 802.16-2004, IEEE 802.16e-2005, IEEE 802.16-2009, and IEEE 802.16j-2009.

WIMAX THREATS

WiMAX wireless interface threats focus on **compromising the radio links between WiMAX nodes**.

These radio links support both **line-of-sight** (LOS) and **non-line-of-sight** (NLOS) signal propagation.

Links from **LOS WiMAX** systems are generally harder to attack than those from NLOS systems because an adversary would have to physically locate equipment between the transmitting nodes to compromise the confidentiality or integrity of the wireless link.

WiMAX NLOS systems provide wireless coverage over large geographic regions, which expand the potential staging areas for both clients and adversaries.

Like other networking technologies, all WiMAX systems must address threats arising from **denial of service attacks**, **eavesdropping**, **man-in-the-middle attacks**, **message modification**, and **resource misappropriation**.

WIMAX SECURITY RECOMMENDATIONS

To improve WiMAX system security, organizations should implement the following recommendations:

Organizations should develop a robust WMAN security policy and enforce it.

A **security policy** is an organization's foundation for designing, implementing, and maintaining properly secured technologies. WMAN policy should address the design and operation of the technical infrastructure and the behavior of users.

Client devices should be configured to comply with WMAN policies, such as disabling unneeded services and altering default configurations.

In addition, **policy-driven software solutions** can be implemented on client devices to prevent or allow certain actions to take place when specific conditions are met. **Policy-driven software** helps ensure that client devices and users comply with an organization's defined policies.

WIMAX SECURITY RECOMMENDATIONS

Organizations should assess WiMAX technical countermeasures before implementing a vendor's WiMAX technology.

As of this writing, few WiMAX products employ Federal Information Processing Standard (FIPS) validated cryptographic modules. Consequently, vendors often integrate their WiMAX products with other security solutions that meet FIPS requirements.

WiMAX interoperability certifications do not extend to these add-on approaches, which means there may be no assurance that the vendor's offering will function as intended. Given the diversity in potential approaches and the risk that integration issues could affect the security of the system, organizations should work closely with WiMAX vendors to gain a better understanding of potential system configuration constraints.

Organizations should independently determine the need for compensating controls to address technical security functionality that the WiMAX product may not address.

WIMAX SECURITY RECOMMENDATIONS

Organizations using WiMAX technology should require mutual authentication for WiMAX devices.

WiMAX technology supports mutual device authentication between a base station (BS) and a user's subscriber unit (i.e., mobile phone, laptop, or similar device), but the feature must be activated to realize the benefit of the approach. Organizations should strongly consider WiMAX solutions capable of supporting Extensible Authentication Protocol (EAP) methods for mutual authentication.

EAP methods that support mutual device authentication typically also support integrated user authentication using passwords, smart cards, biometrics, or some combination of these mechanisms. WiMAX solutions that cannot meet these criteria should employ a different means of authentication at a higher layer (e.g., encryption overlay or virtual private network).

Specifically, native IEEE 802.16-2004 authentication does not support mutual device authentication and thus should be avoided.

WIMAX SECURITY RECOMMENDATIONS

Organizations using WiMAX networks should implement FIPS-validated encryption algorithms employing FIPS-validated cryptographic modules to protect communications.

WiMAX communications consist of management and data messages.

Management messages are used to govern communications parameters necessary to maintain wireless links, and data messages carry the data to be transmitted over wireless links.

Encryption is not applied to management messages to increase the efficiency of network operations, while data messages are encrypted natively in accordance with the IEEE standards. IEEE 802.16e-2005 and IEEE 802.16-2009 support the Advanced Encryption Standard (AES) (as documented in FIPS Publication 197), whereas IEEE 802.16-2004 supports Data Encryption Standard in Cipher Block Chaining mode (DES-CBC). DES-CBC has several well-documented weaknesses, making it a vulnerable encryption algorithm that should not be used to protect data messages.

FUNDAMENTAL WIMAX CONCEPTS

WiMAX networks have five fundamental architectural components:

- **Base Station (BS).** The BS is the node that logically connects wireless subscriber devices to operator networks. The BS maintains communications with subscriber devices and governs access to the operator networks. A BS consists of the infrastructure elements necessary to enable wireless communications, i.e., antennas, transceivers, and other electromagnetic wave transmitting equipment. BSs are typically fixed nodes, but they may also be used as part of mobile solutions—for example, a BS may be affixed to a vehicle to provide communications for nearby WiMAX devices. A BS also serves as a Master Relay-Base Station in the multi-hop relay topology.

- **Subscriber Station (SS).** The SS is a stationary WiMAX-capable radio system that communicates with a base station, although it may also connect to a relay station in multi-hop relay network operations.

- **Mobile Station (MS).** An MS is an SS that is intended to be used while in motion at up to vehicular speeds. Compared with fixed (stationary) SSs, MSs typically are battery operated and therefore employ enhanced power management. Example MSs include WiMAX radios embedded in laptops and mobile phones. This document uses the term SS/MS to refer to the class of both MS and stationary SS.

- **Relay Station (RS).** RSs are SSs configured to forward traffic to other RSs or SSs in a multi-hop Security Zone. The RS may be in a fixed location (e.g., attached to a building) or mobile (e.g., placed in an automobile). The air interface between an RS and an SS is identical to the air interface between a BS and an SS.

- **Operator Network –** The operator network encompasses infrastructure network functions that provide radio access and IP connectivity services to WiMAX subscribers. These functions are defined in WiMAX Forum technical specifications as the access service network (radio access) and the connectivity service network (IP connectivity).

WiMAX devices communicate using two wireless message types: management messages and data messages.

Data messages transport data across the WiMAX network.

Management messages are used to maintain communications between an SS/MS and BS, e.g., establishing communication parameters, exchanging security settings, and performing system registration events (initial network entry, handoffs, etc.)

FUNDAMENTAL WIMAX CONCEPTS

IEEE 802.16 defines frequency bands for operations based on signal propagation type. In one type, it employs a radio frequency (RF) beam to propagate signals between nodes. Propagation over this beam is highly sensitive to RF obstacles, so an unobstructed view between nodes is needed. This type of signal propagation, called **line-of-sight** (LOS), is limited to fixed operations and uses the 10 to 66 gigahertz (GHz) frequency range.

The other type of signal propagation is called **non-line-of-sight** (NLOS). NLOS employs advanced RF modulation techniques to compensate for RF signal changes caused by obstacles that would prevent LOS communications. NLOS can be used for both fixed WiMAX operations (below 11 GHz) and mobile operations (below 6 GHz).

NLOS signal propagation is more commonly employed than LOS because of obstacles that interfere with LOS communications and because of strict regulations for frequency licensing and antenna deployment in many environments that hinder the feasibility of using LOS.

OPERATING TOPOLOGIES

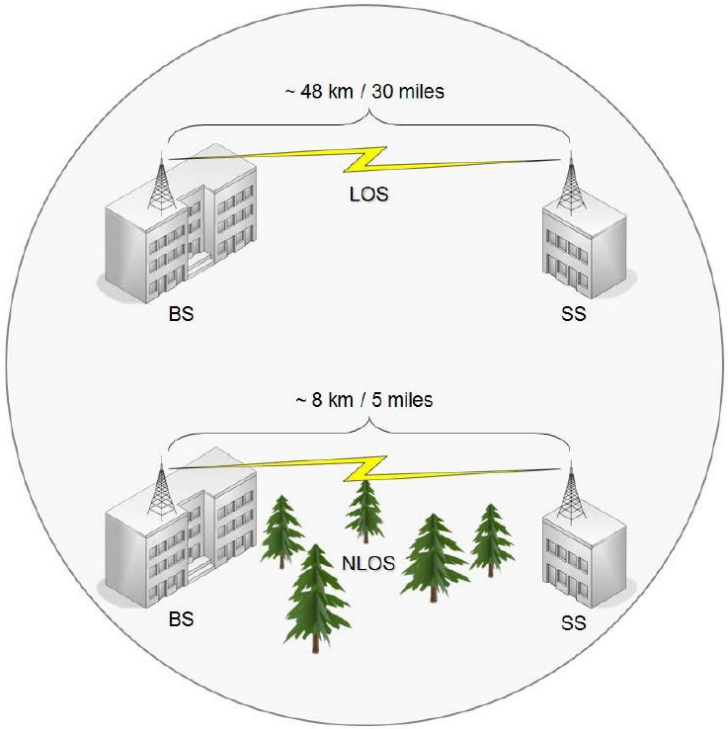
There are four primary topologies for IEEE 802.16 networks:

- point-to-point,
- point-to-multipoint,
- multi-hop relay, and
- mobile.

Each of these topologies is briefly described below.

POINT-TO-POINT (P2P)

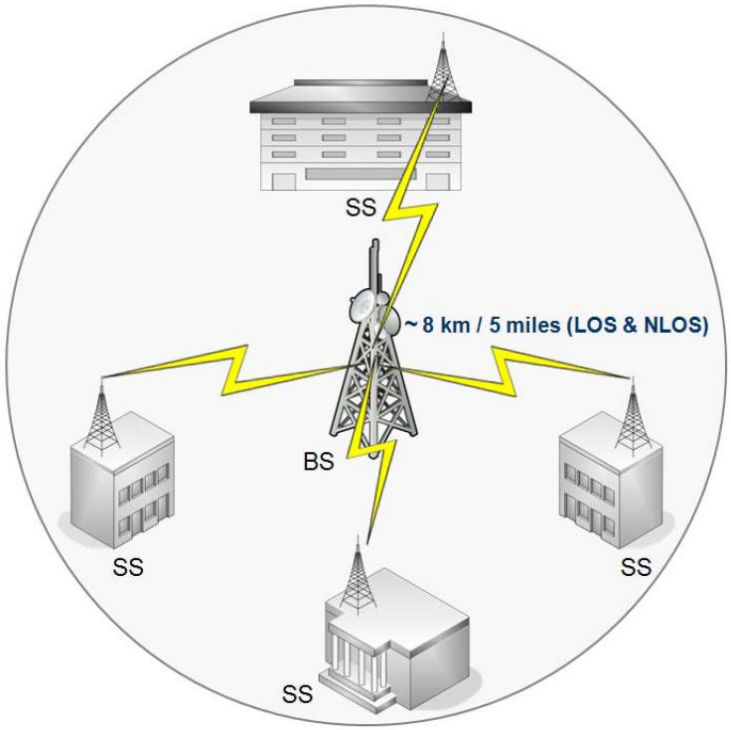
A point-to-point (P2P) topology consists of a dedicated long-range, high-capacity wireless link between two sites.



Typically, the main or central site hosts the BS, and the remote site hosts the SS. The BS controls the communications and security parameters for establishing the link with the SS. The P2P topology is used for high-bandwidth wireless backhaul8 services at a maximum operating range of approximately 48 kilometers (km) (30 miles) using LOS signal propagation, and eight km (five miles) using NLOS.

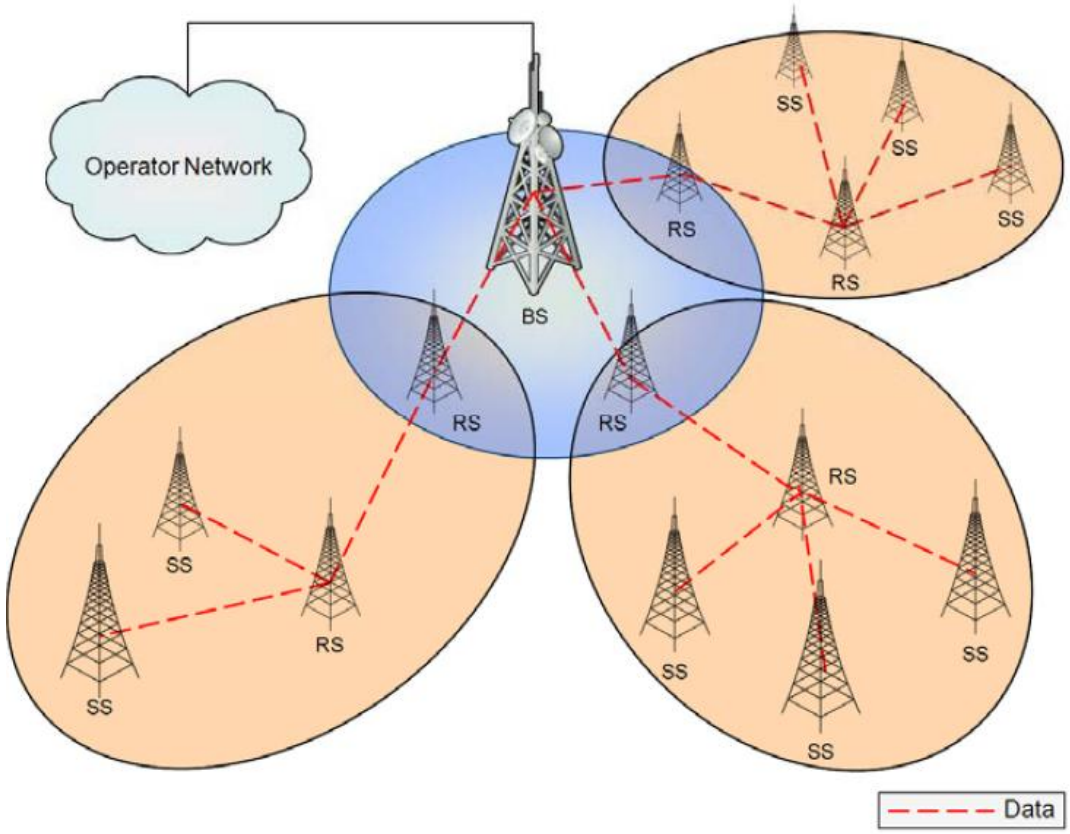
POINT-TO-MULTIPOINT (PMP)

A point-to-multipoint (PMP) topology is composed of a central BS supporting multiple SSs, providing network access from one location to many.



It is commonly used for last-mile broadband access, private enterprise connectivity to remote offices, and long-range wireless backhaul services for multiple sites. PMP networks can operate using LOS or NLOS signal propagation. Each PMP BS has a maximum operating range of 8 km (5 miles), but it is typically less than this due to cell configuration and the urban density of the target coverage area.

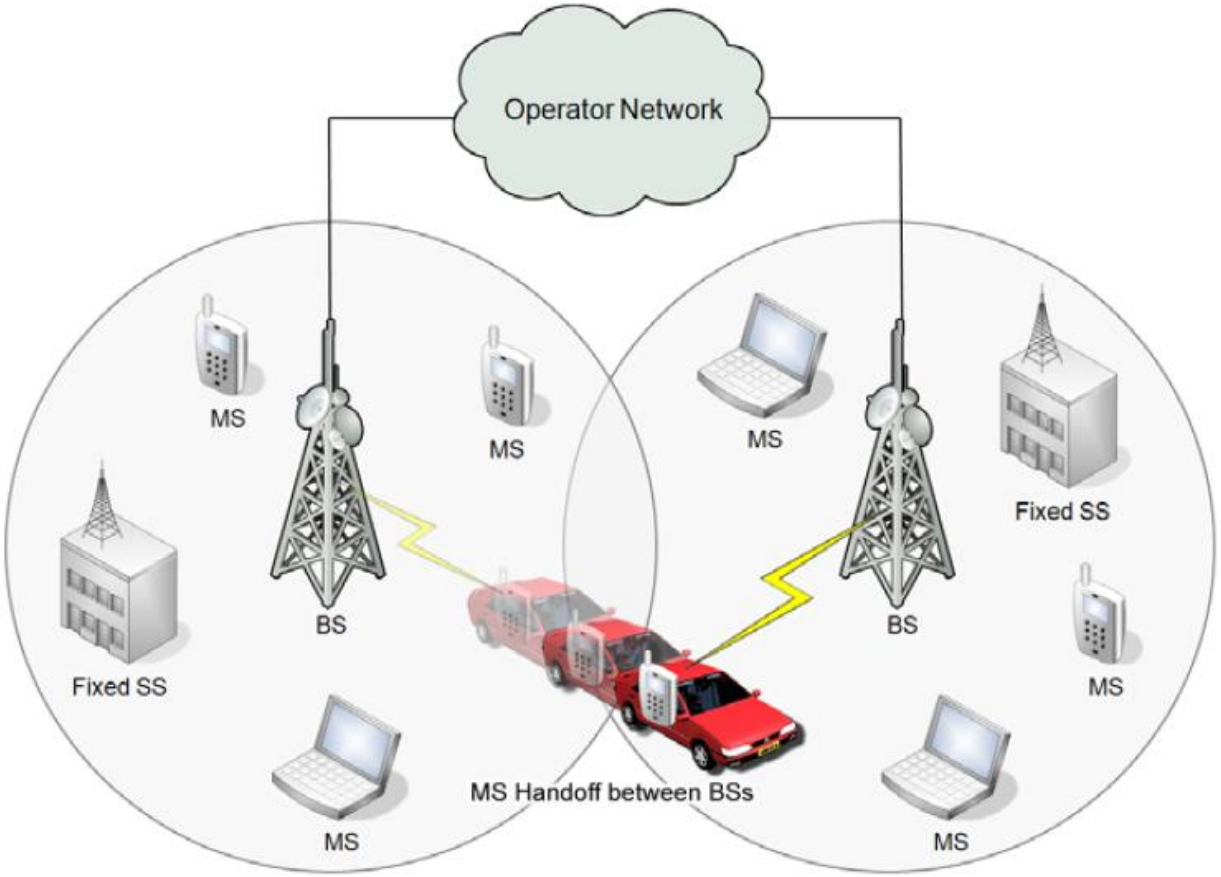
MULTI-HOP RELAY



A multi-hop relay topology, defined by IEEE 802.16j-2009, extends a BS's coverage area by permitting SSs/MSs to relay traffic by acting as RSs. Data destined to an SS/MS outside of the BS's range is relayed through adjacent RSs. An RS can only forward traffic to RSs/SSs within its Security Zone. A Security Zone is a set of trusted relationships between a BS and a group of RSs. Data originating outside of a BS's coverage area is routed over multiple RSs, increasing the network's total geographical coverage area. Multi-hop relay topology typically uses NLOS signal propagation because its purpose is to span large geographic areas containing multiple RF obstacles; however, technically it can operate using LOS propagation as well.

The maximum operating range for each node in a multi-hop relay topology is approximately 8 km (5 miles), but the actual operating range is typically less depending on environmental conditions (e.g., building obstructions) and antenna configuration.

MOBILE



A mobile topology is similar to a cellular network because multiple BSs collaborate to provide seamless communications over a distributed network to both SSs and MSs. This topology combines the coverage area of each member BS and includes measures to facilitate handoffs of MSs between BS coverage areas, as seen by the car MS. It uses advanced RF signaling technology to support the increased RF complexity required for mobile operations.

Each BS coverage area is approximately 8 km (5 miles). Mobile WiMAX systems operate using NLOS signal propagation on frequencies below 6 GHz.

WIMAX SECURITY FEATURES

The IEEE 802.16 standards specify two basic security services: **authentication** and **confidentiality**.

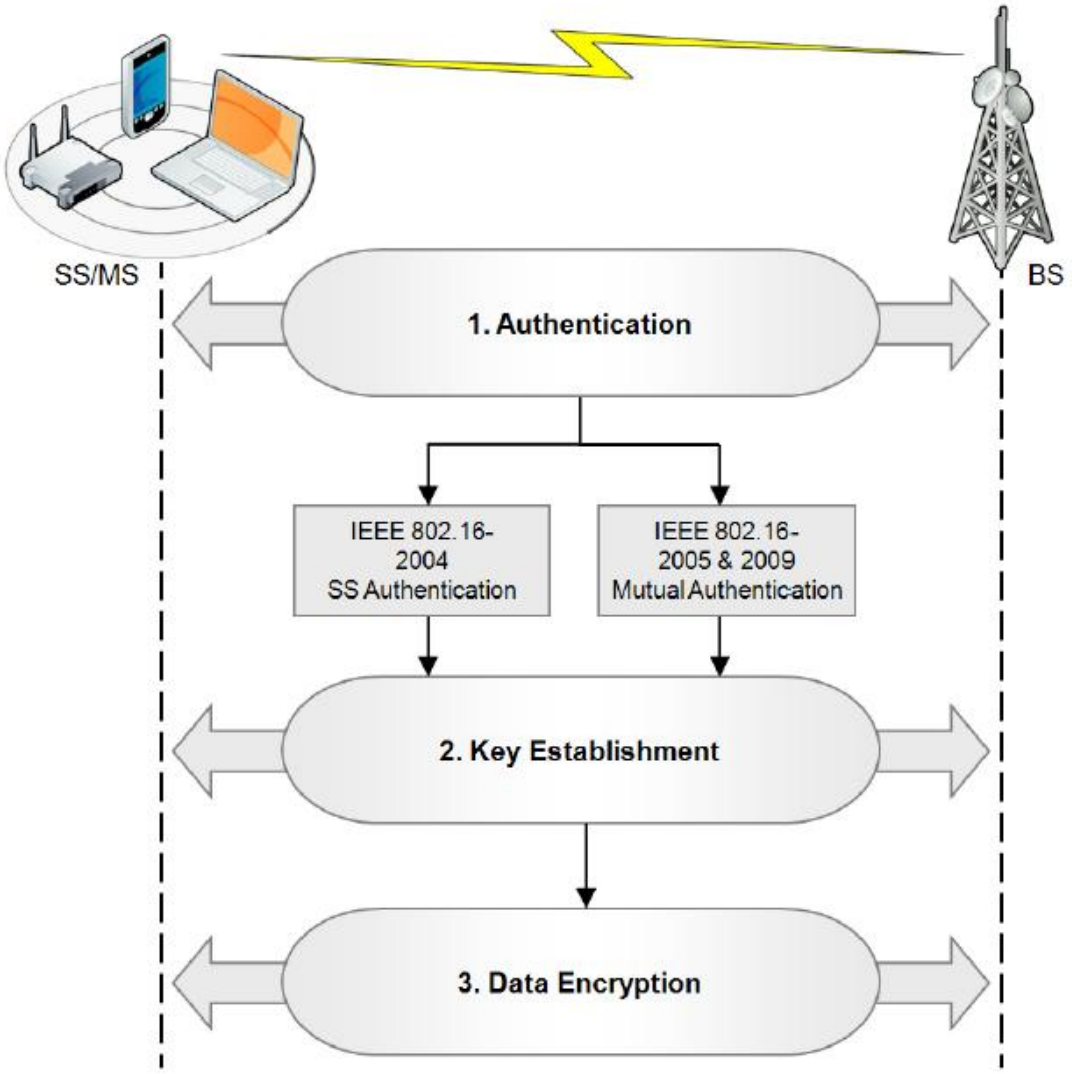
Authentication involves the process of verifying the identity claimed by a WiMAX device.

Confidentiality is limited to protecting the contents of WiMAX data messages so that only authorized devices can view them. IEEE 802.16e-2005 and IEEE 802.16-2009 share the same authentication and confidentiality mechanisms; they both support user authentication and device authentication.

The IEEE 802.16 standards do not address other security services such as **availability** and **confidentiality protection for wireless management messages**; if such services are required, they must be provided through additional means.

Also, while IEEE 802.16 security protects communications over the WMAN link between an SS/MS and a BS, it does not protect communications on the wired operator network behind the BS. End-to-end (i.e., device-to-device) security is not possible without applying additional security controls not specified by the IEEE standards.

WIMAX SECURITY FEATURES



WiMAX systems provide secure communications by performing three steps: **authentication**, **key establishment**, and **data encryption**.

The authentication procedure provides common keying material for the SS/MS and the BS and facilitates the secure exchange of data encryption keys that ensure the confidentiality of WiMAX data communications.

SECURITY ASSOCIATIONS

A **security association** (SA) is a shared set of security parameters that a BS and its SS/MS use to facilitate secure communications.

Similar in concept to Internet Protocol Security (IPsec), an SA defines the security parameters of a connection, i.e., **encryption keys** and **algorithms**.

SAs fall into one of three categories: authorization, data (for unicast services), and group (for multicast services).

A distinct SA is established for each service offered by the BS. For example, a unicast service would have a unique data encryption SA, whereas a multicast service would have a unique group SA.

AUTHORIZATION SECURITY ASSOCIATION

Authorization SAs facilitate authentication and key establishment to configure data and group SAs. Authorization SAs contain the following attributes:

- **X.509 certificates.** X.509 digital certificates allow WiMAX communication components to validate one another. The manufacturer's certificate is used for informational purposes, and the BS and SS/MS certificates contain the respective devices' public keys. The certificates are signed by the device manufacturer or a third-party certification authority.
- **Authorization key (AK).** AKs are exchanged between the BS and SS/MS to authenticate one another prior to the traffic encryption key (TEK) exchange. The authorization SA includes an identifier and a key lifetime value for each AK.
- **Key encryption key (KEK).** Derived from the AK, the KEK is used to encrypt TEKs during the TEK exchange.
- **Message authentication keys.** Derived from the AK, the message authentication keys validate the authenticity of key distribution messages during key establishment. These keys are also used to sign management messages to validate message authenticity.
- **Authorized data SA list.** Provided to the SS/MS by the BS, the authorized data SA list indicates which data encryption SAs the SS/MS is authorized to access.

DATA SECURITY ASSOCIATION

Data SAs establish the parameters used to protect unicast data messages between BSs and SSs/MSs. Data SAs cannot be applied to management messages, which are never encrypted. A data SA contains the following security attributes:

- **SA identifier (SAID).** This unique 16-bit value identifies the SA to distinguish it from other SAs.
- **Encryption cipher to be employed.** The connection will use this encryption cipher definition to provide wireless link confidentiality.
- **Traffic encryption key (TEK).** TEKs are randomly generated by the BS and are used to encrypt WiMAX data messages. Two TEKs are issued to prevent communications disruption during TEK rekeying; the first TEK is used for active communications, while the second TEK remains dormant.
- **Data encryption SA type indicator.** This indicator identifies the type of data SA. There are three types:
  - **Primary SA.** This SA is established as a unique connection for each SS/MS upon initialization with the BS. There is only one primary SA per SS/MS.
  - **Static SA.** This SA secures the data messages and is generated for each service defined by the BS.
  - **Dynamic SA.** This SA is created and eliminated in response to the initiation and termination of specific service flows.

GROUP SECURITY ASSOCIATION

Group SAs contain the keying material used to secure multicast traffic. Group SAs are inherently less secure than data SAs because identical keying material is shared among all members of a BS's group. Group SAs contains the following attributes:

- **Group traffic encryption key (GTEK).** This key is randomly generated by the BS and used to encrypt multicast traffic between a BS and SSs/MSs.

- **Group key encryption key (GKEK).** This key is also randomly generated by the BS and used to encrypt the GTEK sent in multicast messages between a BS and SSs/MSs.

AUTHENTICATION AND AUTHORIZATION

Networking technologies traditionally refer to authorization as the process that determines the level of access a node receives after the subject is identified and authenticated.

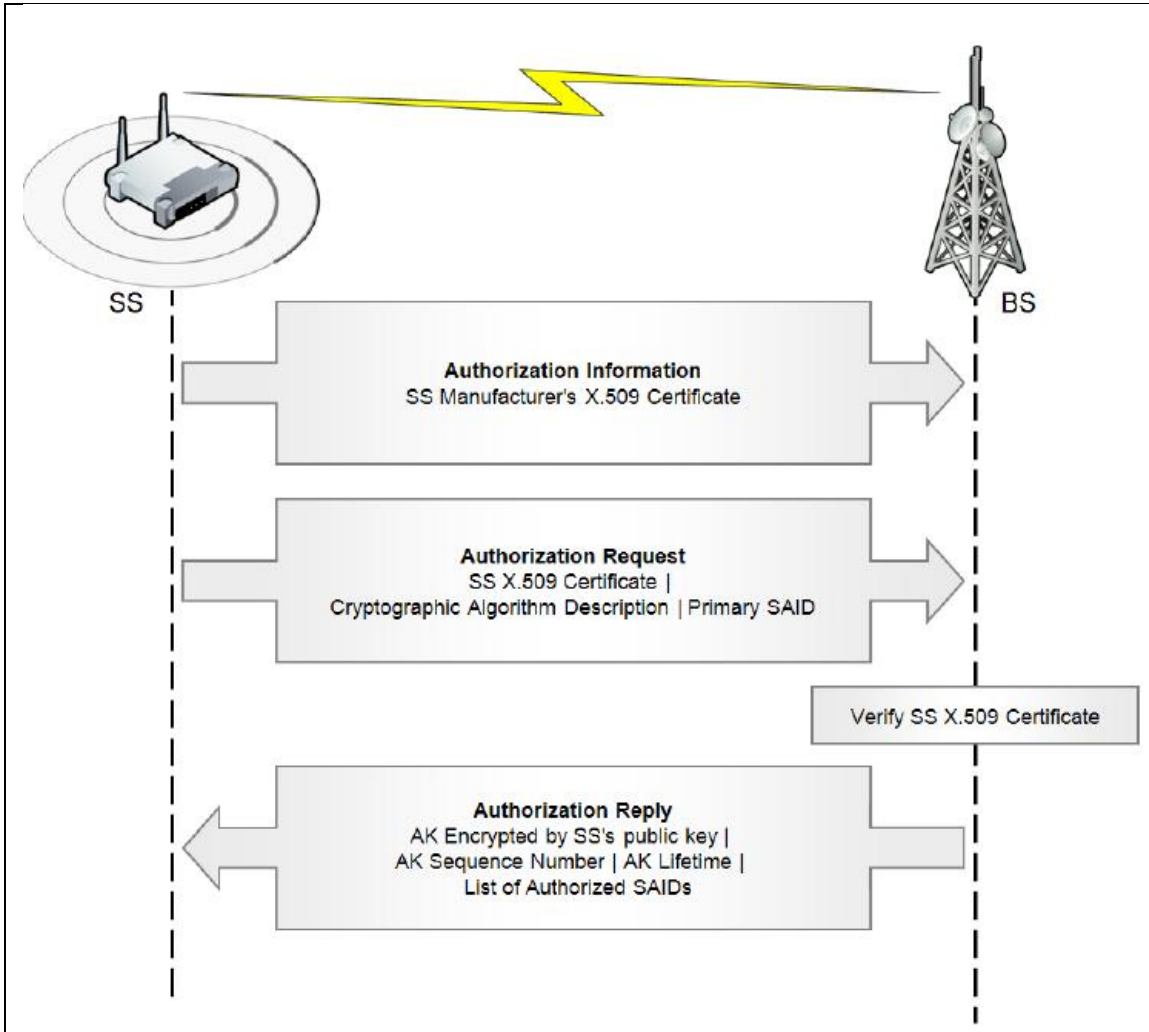
The IEEE 802.16 standard generally refers to authorization as the process of authenticating WiMAX nodes and granting them access to the network. This slight distinction made by IEEE 802.16 is that authorization processes implicitly include authentication.

The Privacy Key Management (PKM) protocol is the set of rules responsible for authentication and authorization to facilitate secure key distribution in WiMAX.

PKM uses authorization SAs to authenticate system entities so that data and group encryption SAs can be established. PKM's authentication enforcement function provides the SS/MS and BS with identical AKs; each AK is then used to derive the message authentication keys and KEKs that facilitate the secure exchange of the TEKs.

IEEE 802.16-2004 derives the AK using PKM version 1 (PKMv1), whereas IEEE 802.16e-2005 and IEEE 802.16-2009 derive the AK using PKMv2.

IEEE 802.16-2004 AUTHENTICATION AND AUTHORIZATION



In PKMv1, the BS authenticates the identity of the SS, providing one-way authentication.

The authorization process is initiated when the SS sends an authorization information message to the BS. This message contains the X.509 certificate of the SS manufacturer and is used by the BS for informational purposes.

IEEE 802.16-2004 AUTHENTICATION AND AUTHORIZATION

Immediately following the authorization information message, the SS sends an authorization request to the BS, which contains the following information:

- The SS's unique X.509 certificate, which includes its RSA public key;
- A description of the SS's supported cryptographic algorithms;
- The primary SAID.

Next, the BS validates the SS's X.509 certificate, communicates the supported cryptographic algorithms and protocols, and activates an AK for the SS. Then the BS sends the SS an authorization reply message containing the following information:

- The activated AK, encrypted with the SS's public key
- The AK sequence number used to differentiate between successive generations of AKs
- The AK lifetime
- A list of SAIDs that the SS is authorized to access and their associated properties.

The AK is periodically reauthorized based on its lifetime. The reauthorization process is identical to the initial authorization process with the exception that the authorization information message is not re-sent. Reauthorization does not cause a service interruption because two AKs with overlapping lifetimes are supported simultaneously.

IEEE 802.16-2009 AUTHENTICATION AND AUTHORIZATION

IEEE 802.16-2009 includes security features of the 802.16e-2005 amendment, which was adopted after the publication of 802.16-2004. The WiMAX Forum Network Architecture Release 1.5 further extends the security framework.

In particular, the Base Specification delineates the required **Extensible Authentication Protocol** (EAP) methods that a certified device must support, and describes the use of **Remote Authentication Dial-In User Services** (RADIUS) (and its **Diameter** successor) for authentication, authorization, and accounting (AAA).

The addition of EAP and RADIUS/Diameter support enables WiMAX networks to be tailored to a wide range of robust enterprise security architectures, and also makes the design and implementation of WiMAX networks more complex than had been the case with IEEE 802.16-2004.

IEEE 802.16-2009 AUTHENTICATION AND AUTHORIZATION

The WiMAX Forum Network Architecture Release 1.5 states requirements for device and user authentication.

For **mutual device authentication** based on X.509 certificates, an SS/MS must support EAP-transport layer security (EAP-TLS).

For **user authentication**, the SS/MS must support either EAP-authentication and key agreement (EAP-AKA) or EAP-tunneled TLS (EAP-TTLS), preferably both.

EAP-AKA is an authentication method used in Universal Mobile Telecommunications System (UMTS) and CDMA2000 networks. It is based on symmetric key encryption that typically runs in a subscriber identity module (SIM) or similar smart card. EAP-TTLS authenticates the network to the user with an X.509 certificate and authenticates the user to the network with another “tunneled” EAP method. The WiMAX Forum Network Architecture Release 1.5 requires that EAP-TTLS support Microsoft Challenge-handshake authentication protocol version 2 (MS-CHAPv2) at a minimum. Vendors may implement other EAP methods at their discretion to support specialized authentication requirements. Organizations should strongly consider WiMAX solutions capable of supporting EAP methods for mutual authentication.

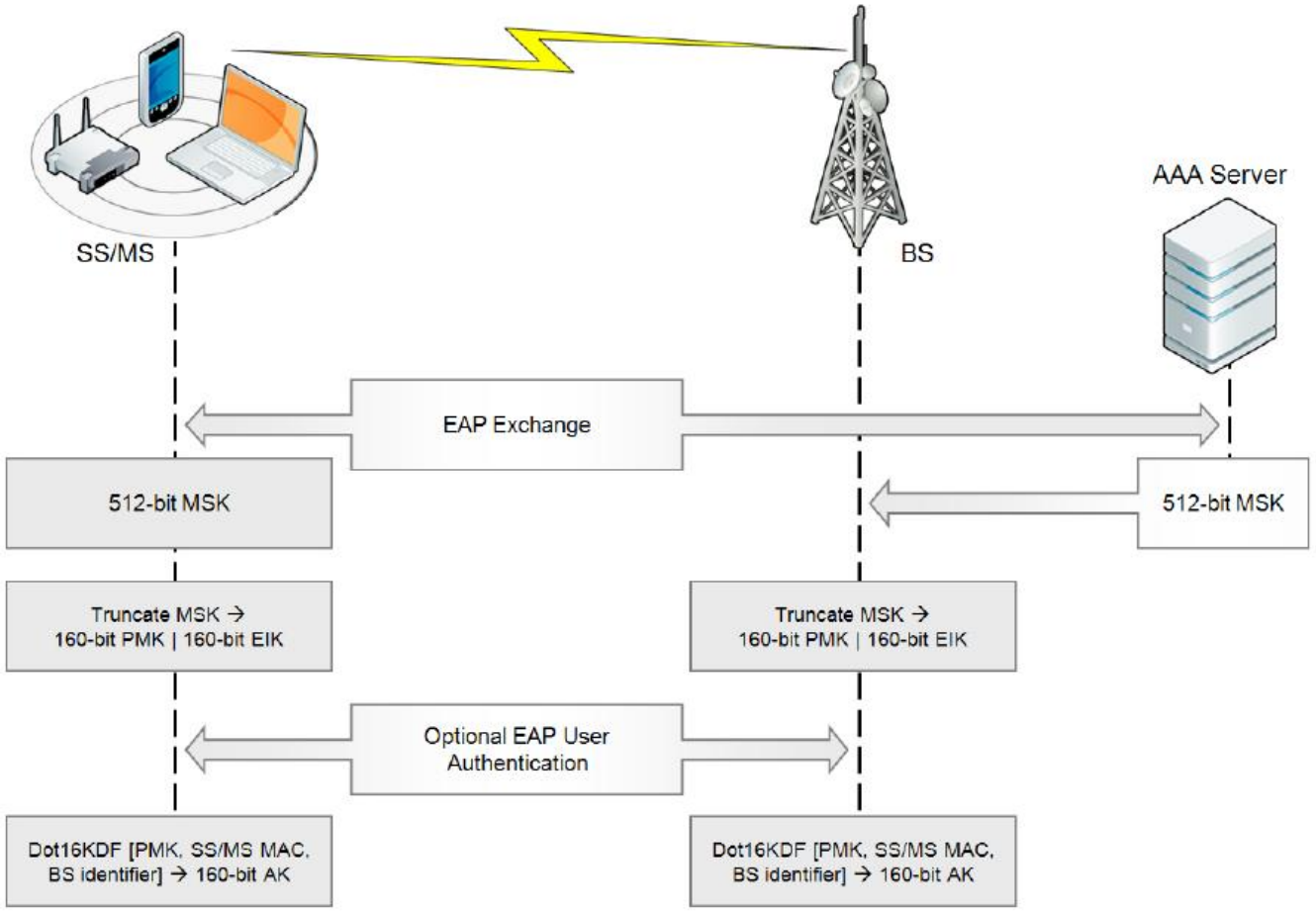
IEEE 802.16-2009 AUTHENTICATION AND AUTHORIZATION

IEEE 802.16-2009 also specifies a **Rivest, Shamir, Adleman** (**RSA**) authentication protocol for mutual device authentication that uses X.509 certificates that contain the device's media access control (MAC) address.

According to the standard, devices that use this protocol must either have factory-installed public/private key pairs or provide an internal algorithm to generate the pair automatically. The method has no known security vulnerabilities. However, it is not included in the WiMAX Forum Network Architecture Release 1.5 and, consequently, WiMAX certified products do not necessarily have an RSA Authentication feature.

Additionally, IEEE 802.16-2009 RSA Authentication should not be confused with EAP methods that also use X.509 certificates and employ RSA algorithms.

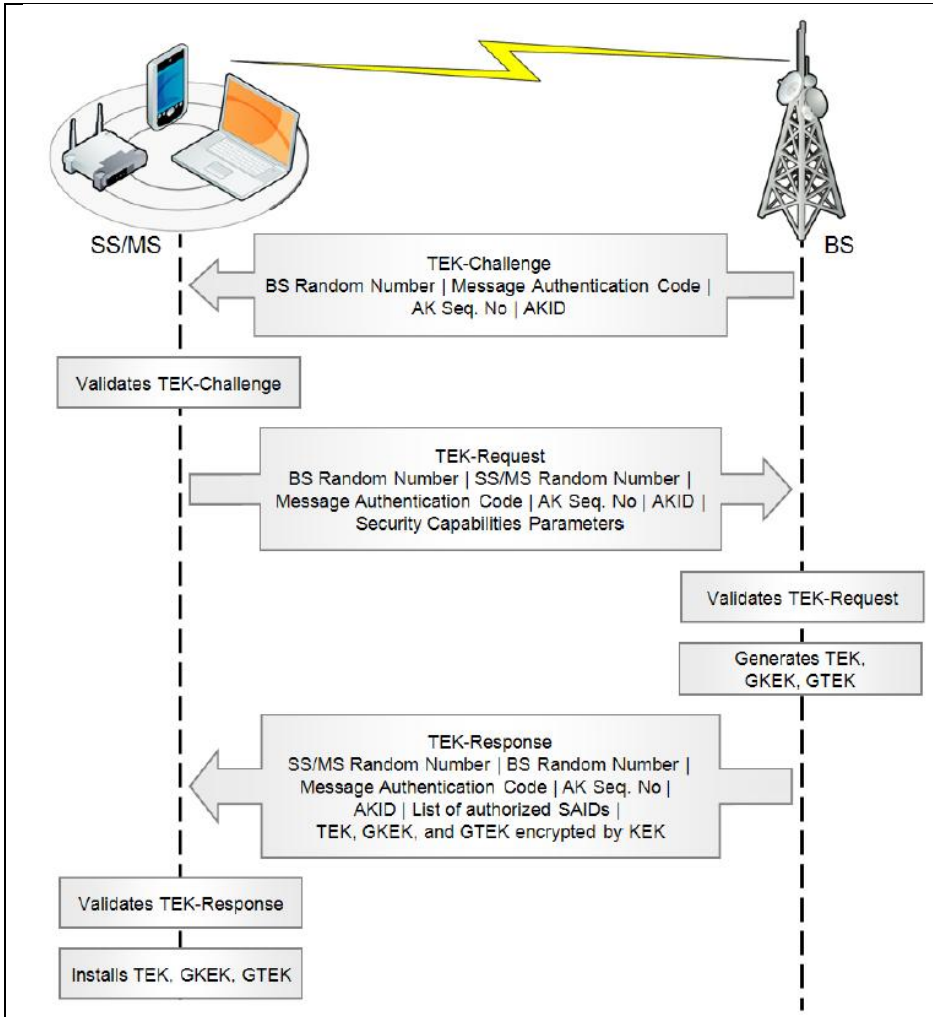
IEEE 802.16-2009 AUTHENTICATION AND AUTHORIZATION



The **first EAP exchange** results in the production of a 512-bit **master session key** (MSK) that is disclosed to the AAA server, the operator network, and the SS/MS.

The BS and SS/MS truncate the MSK to 320 bits – 160 bits for the **pairwise master key** (PMK) and 160 bits to create another **EAP Integrity Key** (EIK) to protect an optional EAP user authentication procedure. The PMK, the SS/MS MAC address, and the BS identifier are then used to derive the AK.

ENCRYPTION KEY ESTABLISHMENT



Once authentication is complete, the BS and SS/MS share an activated AK. PKM then uses the 160-bit AK to derive the 128-bit KEK and the 160-bit message authentication keys, which are used to facilitate a secure exchange of TEKs. The secure TEK exchange uses a three-way handshake between the BS and the SS/MS.

ENCRYPTION KEY ESTABLISHMENT

The first step in this procedure is the TEK-Challenge sent from the BS to the SS/MS. The TEK-Challenge is sent during initial network entry or during reauthorization. The TEK-Challenge includes the following attributes:

- **BS random number.** This number is attached to the TEK-Challenge to prevent replay attacks by validating message freshness.
- **Message authentication code.** This validates data authenticity of the key distribution messages sent from the BS to the SS/MS.
- **AK sequence number and AK identifier (AKID).** These attributes identify which AK is used for the TEK exchange.

ENCRYPTION KEY ESTABLISHMENT

Upon receipt of the TEK-Challenge, the SS/MS validates the authenticity of the TEK-Challenge using the message authentication keys. After the TEK-Challenge has been validated, the SS/MS then sends the TEK-Request to the BS, which contains the following attributes:

- **BS and SS/MS random numbers.** In addition to sending back the BS random number from the TEK-Challenge, the SS/MS attaches its own random value.
- **Message authentication code.** These validate data authenticity of the key distribution messages sent from the SS/MS to the BS.
- **AK sequence number and AKID.** These identify which AK is used for the TEK exchange.
- **Security capabilities parameters.** These describe the security capabilities of the SS/MS, including supported cryptographic suites. During initial network entry, the TEK-Request will also include a request for SA descriptors to identify the primary, static, and dynamic SAs that the SS/MS is authorized to access.

ENCRYPTION KEY ESTABLISHMENT

Upon receipt of the TEK-Request, the BS verifies that the BS random number matches the number sent in the TEK-Challenge and validates the message authentication keys. The BS next confirms that the AKID refers to an available AK and that the security capabilities parameters provided by the SS/MS are supported. Once the TEK-Request is validated, the BS will generate two TEKs, along with the GKEK and the GTEK. The BS then sends the TEK-Response to the SS/MS, which contains the following attributes:

- **BS and SS/MS random number.** The BS attaches the BS random number generated in the TEK-Challenge and the SS/MS random number generated in the TEK-Request.
- **Message authentication code.** These validate data authenticity for the key distribution messages sent from the BS to the SS/MS.
- **AK sequence number and AKID.** These attributes identify which AK is used for the TEK exchange.
- **List of authorized SAIDs.** This is the list of primary, static, and dynamic SAs that the SS/MS is authorized to access.
- **TEKs, GKEK, and GTEK.** Using the KEK derived from the AK, the BS encrypts the two TEKs, the GKEK, and the GTEK. These keys include all of the required keying material needed to facilitate secure communications.

ENCRYPTION KEY ESTABLISHMENT

Upon receipt of the TEK-Response, the SS/MS will ensure the BS random number matches the value given in the TEK-Challenge and that the SS/MS random number matches the value delivered in the TEK- Request. The SS/MS will then validate the message authentication keys. Once validation is complete, the SS/MS will install the appropriate TEKs, GTEK, and GKEK, and secure communications can begin.

In the case of an MS performing a handover to a new BS, the TEK-Response message also includes TEK, GTEK, and GKEK parameters of the previously serving BS to reduce latency associated with renewing SAs.

DATA CONFIDENTIALITY

The completion of the TEK exchange provides the SS/MS and BS with the TEKs required to encrypt WiMAX data communications. The type of encryption employed by the TEK varies by IEEE 802.16 standard.

IEEE 802.16-2004 only supports one encryption algorithm, the **Data Encryption Standard** (DES) in **cipher block chaining** (CBC) **mode** (DES-CBC).

During the TEK three-way handshake, the BS sends the SS an SA-specific initialization vector (IV) as part of the TEK-Response. The DES-CBC algorithm uses this SA-specific IV in conjunction with the TEK to encrypt data traffic. DES-CBC has significant weaknesses and should not be used to provide confidentiality for communications.

DATA CONFIDENTIALITY

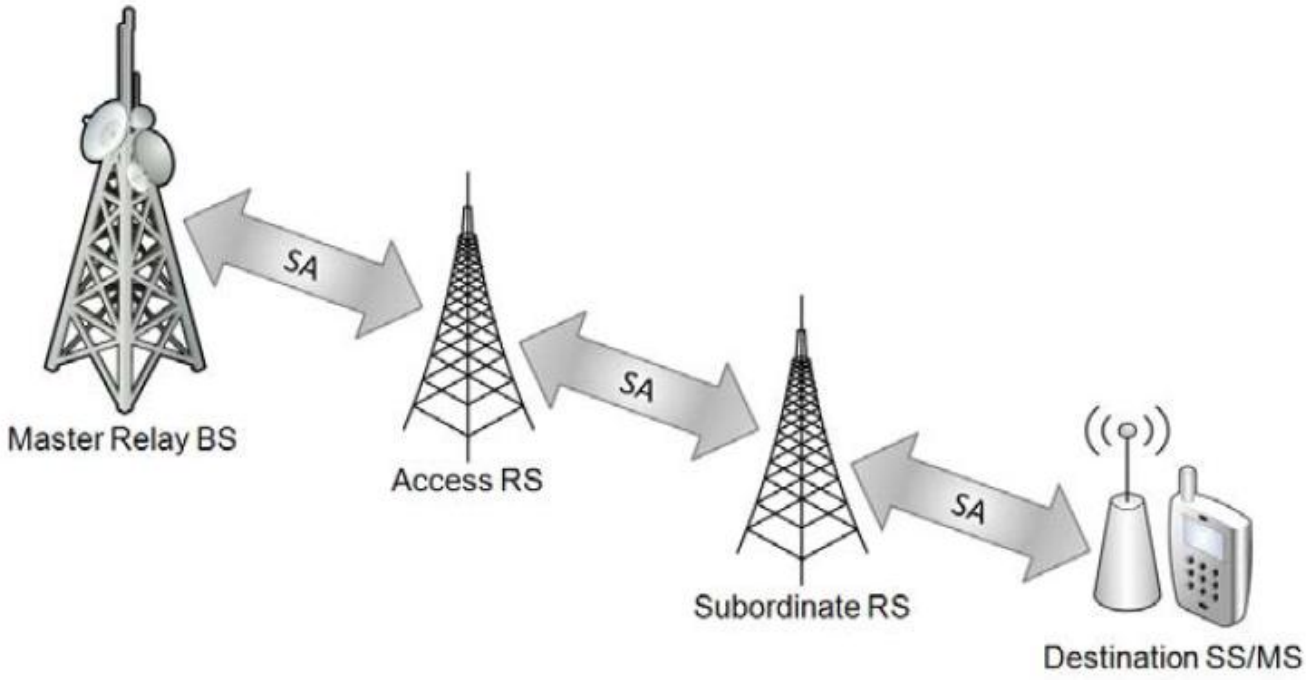
IEEE 802.16e-2005 and IEEE 802.16-2009 support DES-CBC and three AES modes of operation for data encryption: **CBC**, counter (**CTR**), and CTR with CBC message authentication code (**CCM**). Any of the three specified AES modes is acceptable for protecting data message confidentiality. CTR mode is considered stronger than CBC because CTR mode is less complex to implement, offers encryption block preprocessing, and can process data in parallel. CCM mode enhances CTR by adding the capability to verify the authenticity of encrypted messages.

CCM was specifically designed to have the following characteristics:

- A single cryptographic key for confidentiality and integrity to minimize complexity and maximize performance (minimize key scheduling time);
- Integrity protection of the packet header and packet payload, in addition to providing confidentiality of the payload;
- Computation of some cryptographic parameters prior to the receipt of packets to enable fast comparisons when they arrive, which reduces latency;
- Small footprint (hardware or software implementation size) to minimize costs;
- Small security-related packet overhead (e.g., minimal data expansion due to cryptographic padding and integrity field).

IEEE 802.16J-2009 MULTI-HOP RELAY SECURITY ARCHITECTURE

The confidentiality and authentication security mechanisms used in IEEE 802.16j-2009 are identical to those in IEEE 802.16-2009. An additional security mechanism is required to operate a WiMAX network in a multi-hop relay – the establishment of a Security Zone (SZ). An SZ is the set of trusted relationships between a BS (acting as the master relay), RSs, and SSs/MSs. RSs and SSs/MSs become members of a BS's SZ by authenticating using PKMv2. Upon authenticating, the BS delivers SZ key material used to provide integrity protection to management messages in the SZ.



VULNERABILITIES FOR WIMAX SYSTEMS

- **Lack of BS to SS/MS authentication.** PKMv1 defines authentication of SSs by BSs but provides no means to authenticate BSs by SSs/MSs. Lack of mutual authentication may allow a rogue BS to impersonate a legitimate BS, thereby rendering the SS/MS unable to verify the authenticity of protocol messages received from the BS. A successful attack would enable a rogue BS operator to take complete control of all traffic to and from the SS/MS, including capture of authentication credentials. Such an attack would also enable the rogue BS to impersonate name servers, allowing it to redirect user requests to computers with malware without easy detection. This vulnerability is mitigated in IEEE 802.16e-2005 and IEEE 802.16-2009 by the use of mutual authentication.

- **Weak encryption algorithms.** For encrypting communications, IEEE 802.16-2004 only supports the use of DES-CBC, which has well-documented weaknesses and is no longer approved for Federal agency use in protecting communications. IEEE 802.16e-2005 and IEEE 802.16-2009 support DES-CBC, but they also support multiple modes of AES that are approved for Federal government use.

VULNERABILITIES FOR WIMAX SYSTEMS

- **Interjection of reused TEKs.** IEEE 802.16-2004 TEKs employ a 2-bit encryption sequence identifier to determine which TEK is actively used to secure communications. A 2-bit identifier permits only four possible identifier values, rendering the system vulnerable to replay attacks. The interjection of reused TEKs may lead to the disclosure of data and the TEK to unauthorized parties. This concern is resolved in IEEE 802.16e-2005 and IEEE 802.16-2009 with the introduction of AES-CCM.

- **Unencrypted management messages.** Management messages are not encrypted and are susceptible to eavesdropping attacks. Encryption is not applied to these messages to increase the efficiency of network operations. IEEE 802.16-2004 does not provide any data authenticity protection for management messages. IEEE 802.16e-2005 and IEEE 802.16-2009 provide integrity protection for certain unicast management messages by appending a unique digest to protect against malicious replay or modification attacks. This digest is not added to IEEE 802.16 multicast and initial network entry management messages. As with all wireless systems, digest integrity protection cannot be applied to management messages sent to multiple recipients (i.e., multicast transmissions), and initial network entry management messages cannot leverage integrity protection because nodes must first be authenticated to create the unique digest.

VULNERABILITIES FOR WIMAX SYSTEMS

- **Use of electromagnetic spectrum as a communications medium.** Using RF to communicate inherently enables execution of a DoS attack by introducing a powerful RF source intended to overwhelm system radio spectrum. This vulnerability is associated with all wireless technologies. The only defenses are either to locate and remove the source of RF interference or to move to another channel. Such actions can be challenging because of the large coverage areas of WMANs and the scarcity of alternative frequencies to support communications. It is recommended that organizations plan for out-of-band communications in the event of a DoS attack.

THREATS FOR WIMAX SYSTEMS

WiMAX network threats focus on compromising the radio links between WiMAX nodes. LOS WiMAX systems pose a greater challenge to attack compared with NLOS systems because an adversary would have to physically locate equipment between the transmitting nodes to compromise the confidentiality or integrity of the wireless link. NLOS systems provide wireless coverage over large geographic regions, which expands the potential staging areas for both clients and adversaries. The following threats affect all WiMAX systems:

- **RF jamming.** All wireless technologies are susceptible to RF jamming attacks. The threat arises from an adversary introducing a powerful RF signal to overwhelm the spectrum being used by the system, thus denying service to all wireless nodes within range of the interference. RF jamming is classified as a DoS attack. The risk associated with this threat is identical for IEEE 802.16-2004, IEEE 802.16e-2005, and IEEE 802.16-2009 WiMAX systems.
- **Scrambling.** Scrambling attacks, which are the precise injections of RF interference during the transmission of specific management messages, affect all wireless systems. These attacks prevent proper network ranging and bandwidth allocations with the intent to degrade overall system performance. Scrambling attacks are more difficult to identify than jamming attacks because they are engaged for short time periods and are not a constant source of interference. The risk associated with this threat is identical for IEEE 802.16-2004, IEEE 802.16e-2005, and IEEE 802.16-2009.

THREATS FOR WIMAX SYSTEMS

- **Subtle management message manipulation.** Exploitation of unauthenticated management messages can result in subtle DoS, replay, or misappropriation attacks that are difficult to detect. These attacks spoof management messages to make them appear as though they come from a legitimateor SS/MS, allowing them to deny service to various nodes in the WiMAX system. A water torturattack is an example of a subtle DoS in which an adversary drains a client node's battery by sending a constant series of management messages to the SS/MS. IEEE 802.16e-2005 and IEEE 802.16-2009 provide integrity protection for certain unicast management messages following initial network registration with an appended integrity protection digest. All other IEEE 802.16e-2005 and IEEE 802.16-2009 management messages, and all IEEE 802.16-2004 management messages, are susceptible to attacks involving manipulation.

THREATS FOR WIMAX SYSTEMS

- **Man-in-the-middle.** Man-in-the-middle attacks occur when an adversary deceives an SS/MS to appear as a legitimate BS while simultaneously deceiving a BS to appear as a legitimate SS/MS. This may allow an adversary to act as a pass-through for all SS/MS communications and to inject malicious traffic into the communications stream. An adversary can perform a man-in-the-middle attack by exploiting unprotected management messages during the initial network entry process. This is because the management messages that negotiate an SS's/MS's security capabilities are not protected. If an adversary is able to impersonate a legitimate party to both the SS/MS and BS, an adversary could send malicious management messages and negotiate weaker security protection between the SS/MS and BS. This weaker security protection may allow an adversary to eavesdrop and corrupt data communications. Mandating the use of AES-CCM in IEEE 802.16e-2005 and IEEE 802.16-2009 helps mitigate this attack because it appends a unique value to each data packet, which, in turn, prevents the man-in-the-middle traffic relays between BS and SS/MS. IEEE 802.16-2004 does not offer adequate protection against man-in-the-middle attacks.

THREATS FOR WIMAX SYSTEMS

- **Eavesdropping.** Eavesdropping occurs when an adversary uses a WiMAX traffic analyzer within the range of a BS or SS/MS. The large operating range of WiMAX networks helps to shield eavesdroppers from detection; eavesdropping mitigation relies heavily on technical controls that protect the confidentiality and integrity of communications. The adversary may monitor management message traffic to identify encryption ciphers, determine the footprint of the network, or conduct traffic analysis regarding specific WiMAX nodes. Data messages collected during eavesdropping can also be used to decipher DES-CBC encryption; however, AES provides robust data message confidentiality that cannot be circumvented through eavesdropping. The risk associated with eavesdropping management messages is identical for IEEE 802.16-2004, IEEE 802.16e-2005, and IEEE 802.16-2009. The risk associated with eavesdropping data messages is significant for IEEE 802.16-2004 systems due to weak encryption. IEEE 802.16e-2005 and IEEE 802.16-2009 systems offer the stronger AES cipher to protect data messages from eavesdropping.

COUNTERMEASURES FOR WIMAX SYSTEMS

Management countermeasures generally address any problem related to risk, system planning, or security assessment by an organization's management. Organizations should develop a wireless security policy that addresses WiMAX technology. A security policy is an organization's foundation for designing, implementing, and maintaining properly secured technologies. WiMAX policy should address the design and operation of the technical infrastructure and the behavior of users. Policy considerations for WiMAX systems should include the following:

Roles and responsibilities

- Which users or groups of users are authorized to use the WiMAX system
- Which office or officer provides the strategic oversight and planning for all WiMAX technology programs
- Which parties are authorized and responsible for installing and configuring WiMAX equipment
- Which individual or entity tracks the progress of WiMAX security standards, features, threats, and vulnerabilities to help ensure continued secure implementation of WiMAX technology
- Which individual or entity is responsible for incorporating WiMAX technology risk into the organization's risk management framework.

COUNTERMEASURES FOR WIMAX SYSTEMS

WiMAX infrastructure

- Physical security requirements for WiMAX assets
- The use of standards-based WiMAX system technologies
- Types of information permitted over the WiMAX system, including acceptable use guidelines
- How WiMAX transmissions should be protected, including requirements for the use of encryption and for cryptographic key management
- A mitigation plan or transition plan for legacy or WiMAX systems that are not compliant with Federal security standards
- Inventory of IEEE 802.16 BSs, SSs/MSs, and other devices

WiMAX client device security

- Conditions under which WiMAX client devices are allowed to be used and operated
- Standard hardware and software configurations that must be implemented on WiMAX devices to ensure the appropriate level of security
- Standard operating procedures (SOP) for reporting lost or stolen WiMAX client devices
- Frequency and scope of WiMAX security assessments
- Standardized approach to vulnerability assessment, risk statements, risk levels, and corrective actions