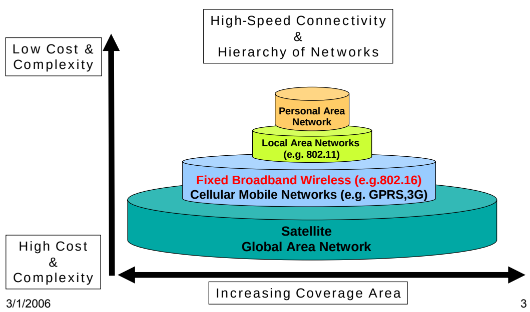
IEEE 802.16 WiMAX

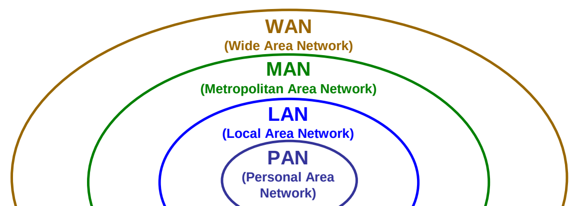
Outline

- An overview
- An insight into IEEE 802.16 WiMAX
- IEEE 802.16 WiMAX Security Issues

Background: Wireless Landscape



Background: Wireless Technologies

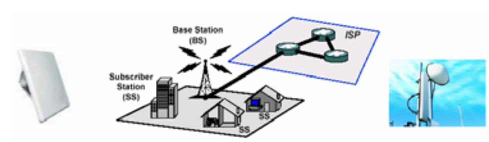


	PAN	LAN	MAN	WAN
Standards	Bluetooth, UWB	802.11 HiperLAN2	802.16 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G, 802.16
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 replacement, last mile access	PDAs, Mobile Phones, cellular access

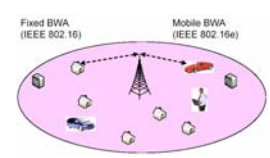
What is WiMAX?

- WiMAX (Worldwide Interoperability for Microwave Access)
  - BWA (Broadband Wireless Access) Solution
  - Standard for constructing Wireless Metropolitan Area Networks (WMANs)
  - Can go places where no wired infrastructure can reach
  - Backhauling Wi-Fi hotspots & cellular networks
  - Offers new and exciting opportunities to established and newly emerging companies
    - Incorporate cable (wired technology) standard
    - Comply with European BWA standard

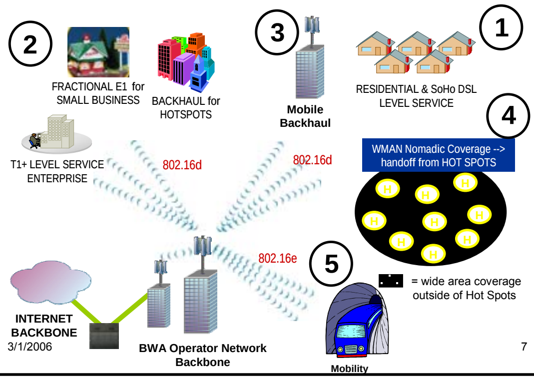
WiMAX Overview



- Complement the existing last mile wired networks (i.e. xDSL, cable modem)
- Fast deployment, cost saving
- High speed data, voice and video services
- Fixed BWA, Mobile BWA



WiMAX Applications



Comparing Technologies

	802.11 WiFi	802.16 WiMAX	802.20 Mobile-FI	UMTS 3G
Bandwidth	11-54 Mbps shared	Share up to 70 Mbps	Up to 1.5 Mbps each	384 Kbps – 2 Mbps
Range (LOS) **Range (NLOS)**	100 meters 30 meters	30 – 50 km 2 - 5 km ('07)	3 – 8 km	Coverage is overlaid on wireless infrastructure
Mobility	Portable	Fixed (Mobile - 16e)	Full mobility	Full mobility
Frequency/ Spectrum	2.4 GHz for 802.11b/g 5.2 GHz for 802.11a	2-11 GHz for 802.16a 11-60 GHz for 802.16	<3.5 GHz	Existing wireless spectrum
Licensing	Unlicensed	Both	Licensed	Licensed
Standardization	802.11a, b and g standardized	802.16, 802.16a and 802.16 REVd standardized, other under development	802.20 in development	Part of GSM standard
Availability	In market today	Products 2H05	Standards coming Product late '06	CW in 6+ cities
Backers	Industry-wide	Intel, Fujitsu, Alcatel, Siemens, BT, AT&T, Qwest, McCaw	Cisco, Motorola, Qualcom and Flarion	GSM Wireless Industry

Potential Services

	802.11 WiFi	802.16 WiMAX	802.20 Mobile-FI	UMTS 3G
VoIP	Limited, QoS concerns	Limited, QoS concerns	Limited, QoS concerns	Yes
Video	Yes, in home	Possible, QoS concerns	No	Possible, via HSDPA
Data/Internet	Yes	Yes	Yes	Yes
WLAN	Yes, small scale	Yes, large scale	No	No
Security	WEP & 802.11i	Developing WEP	None (today)	WEP
QoS	802.11e	802.16b in development	None (today)	None (today)

Benefits of WiMAX

- Speed
  - Faster than broadband service
- Wireless
  - Not having to lay cables reduces cost
  - Easier to extend to suburban and rural areas
- Broad coverage
  - Much wider coverage than WiFi hotspots

Benefits for Network Service Providers

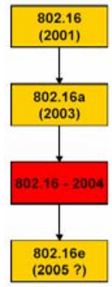
- Allow service providers to deliver high throughput broadband based services like VoIP, high-speed Internet and Video
- Facilitate equipment compatibility
- Reduce the capital expenditures required for network expansion
- Provide improved performance and extended range
- Allow service providers to achieve rapid ROI (Return On Investment) and maximize revenues

Benefits for Consumers

- Range of technology and service level choices from both fixed and wireless broadband operators
- DSL-like services at DSL prices but with portability
- Rapidly declining fixed broadband prices
- No more DSL "installation" fees from incumbent

An Insight into IEEE 802.16

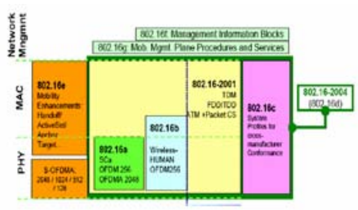
IEEE 802.16 Evolution



- Fixed BWA at 10-66hz
- Line of sight
- Fixed BWA at 2-11hz
- None line of sight
- Revision of 802.16
- Combine previous 802.16 standards
- Mobile BWA based on 802.16-2004 (802.16a)
- Roaming with vehicular speed

IEEE 802.16 Specifications

- **802.16a**
  - use the licensed and license-exempt frequencies from 2 to 11Ghz
  - Support Mesh-Network
- **802.16b**
  - Increase spectrum to 5 and 6GHz
  - Provide QoS (for real-time voice and video service)



- **802.16c**
  - Represents a 10 to 66GHz system profile
- **802.16d**
  - Improvement and fixes for 802.16a
- **802.16e**
  - Addresses on Mobile
  - Enable high-speed signal handoffs necessary for communications with users moving at vehicular speeds

IEEE 802.16 Basics

	802.16a/REVd	802.16e
Completed	802.16a: Jan 2003 802.16REVd: Q3'04	Approved on Dec.7, 2005
Spectrum	< 11 GHz	< 11 GHz
Channel Conditions	Non line of sight	Non line of sight
Bit Rate	Up to 75 Mbps at 20MHz	Up to 75 Mbps at 20MHz
Modulation	OFDM 256 sub-carriers QPSK, 16QAM, 64QAM	OFDMA OFDM
Mobility	Fixed	Pedestrian mobility High-speed mobility
Channel Bandwidths	Selectable channel bandwidths between 1.25 and 20 MHz	Same as 802.16d with sub-channelization

IEEE 802.16 Operation

- WiMAX consists of two parts

  - A **WiMAX tower**, similar in concept to a cell-phone tower - A single WiMAX tower can provide coverage to a very large area -- as big as 3,000 square miles
  - A **WiMAX Receiver** The receiver and antenna could be a small box or PCMCIA card, or they could be built into a laptop the way WiFi access is today

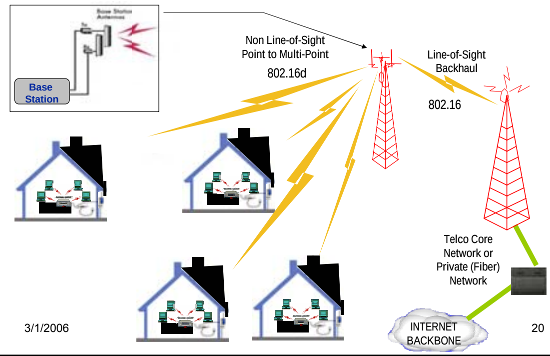
Service Types

- Non-Line-Of-Sight
  - A Service where a small antenna on your computer connects to the tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to WiFi)
- Line-Of-Sight
  - A Service where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz

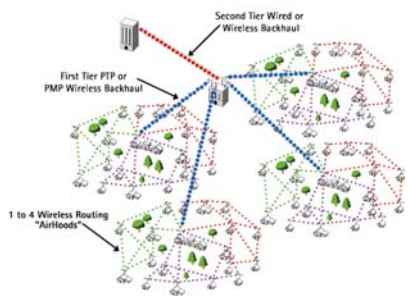
Architecture

- P2MP (Point to Multi point)
  - Wireless MAN
  - BS connected to Public Networks
  - BS serves Subscriber Stations (SS)
  - Provides SS with first mile access to Public Networks
- Mesh Architecture
  - Optional architecture for WiMAX

P2MP Architecture

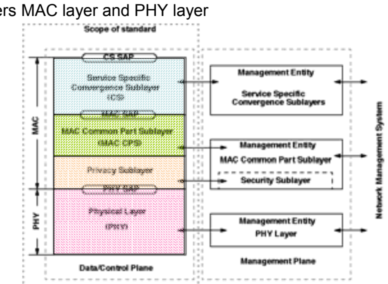


Mesh Architecture



Reference Model

- Supports multiple services (e.g. IP, voice over IP, video) simultaneously, with different QoS priorities
- Covers MAC layer and PHY layer

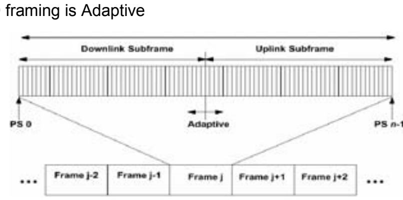


PHY Layer

- Burst single-carrier modulation with adaptive data burst profiles
  - Transmission parameters (e.g. modulation and FEC settings) can be modified on a frame-by-frame basis for each SS.
  - Profiles are identified by "Interval Usage Code" (DIUC and UIUC)
    - On downlink, multiple SS's can associate the same DL burst
    - On uplink, SS transmits in an given time slot with a specific burst
- Allows use of directional antennas
  - Improves range
- Allows use of two different duplexing schemes:
  - Frequency Division Duplexing (FDD)
  - Time Division Duplexing (TDD)
- Support for both full and half duplex stations

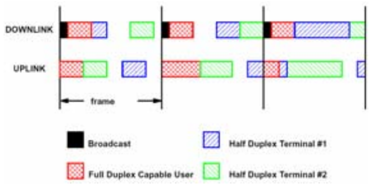
Time Division Duplexing (TDD)

- In case of TDD both uplink and downlink transmissions share the same frequency but are separated on time
- A TDD frame has a fixed duration and also consists of one uplink and one downlink frame
- TDD framing is Adaptive



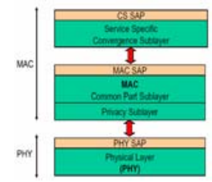
Frequency Division Duplexing (FDD)

- In case of FDD both uplink and downlink channels are on separate frequencies
- The capability of downlink to be transmitted in bursts simultaneously supports two different modulation types
  - Full Duplex SS's (which can transmit and receive simultaneously
  - Half Duplex SS's (which cannot)



MAC Layer

- Wireless MAN: Point-to-Multipoint and optional mesh topology
- Connection-oriented
  - Connection ID (CID), Service Flows (FS)
- MAC layer is further subdivided into three layers
  - Convergence sub-layer (CS)
  - Common part sub-layer (CPS)
  - Privacy sub-layer

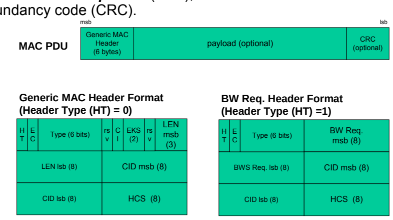


MAC Addressing

- SS has 48-bit 802.3 MAC address
- BS has 48-bit base station ID
  - Not a MAC address
- Connection ID (CID)
  - 16 bit
  - Used in MAC PDU
  - Connection Oriented Service

MAC PDU

- Each MAC packet consists of the three components,
  - A ***MAC header***, which contains frame control information.
  - A variable length ***frame body***, which contains information specific to the frame *type*.
  - A ***frame check sequence*** (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).



MAC PDU Types

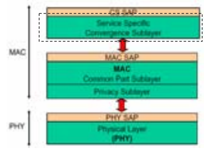
- Data MAC PDUs
  - HT = 0
  - Payloads are MAC SDUs/segments, i.e., data from upper layer (CS PDUs)
  - Transmitted on data connections
- Management MAC PDUs
  - HT = 0
  - Payloads are MAC management messages or IP packets encapsulated in MAC CS PDUs
  - Transmitted on management connections
- BW Req. MAC PDUs
  - HT = 1; and no payload, i.e., just a Header

MAC PDU Transmission

- MAC PDU’s are transmitted on PHY bursts
- The PHY burst can contain multiple FEC blocks
- Concatenation
  - Multiple MAC PDU's can be concatenated into a single transmission in either uplink or downlink direction
- Fragmentation
  - Each MAC SDU can be divided into one or more MAC PDU's
- Packing
  - Packs multiple MAC SDU's into a single MAC PDU

MAC CS Sub-layer

- Interoperability requires convergence sub-layer to be service specific
- Separate CS layers for ATM & packet protocols
- CS Layer:
  - Receives data from higher layers
  - Classifies data as ATM cell or packet
  - Forwards frames to CPS layer



3/1/2006 31

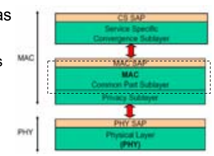
MAC CS Sub-layer (cont.)

- Packet Convergence Sub-Layer
  - Initial support for Ethernet, VLAN, IPv4, and IPv6
  - Payload header suppression
  - Full QoS support
- ATM Convergence Sub-Layer
  - Support for VP/VC switched connections
  - Support for end-to-end signalling of dynamically created connections
  - ATM header suppression
  - Full QoS support

3/1/2006 32

MAC CPS Sub-layer

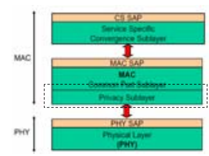
- Performs typical MAC functions such as addressing
  - Each SS assigned 48-bit MAC address
  - Connection Identifiers used as primary address after initialization
- MAC policy determined by direction of transmission
  - Uplink is DAMA-TDM
  - Downlink is TDM
- Data encapsulated in a common format facilitating interoperability
  - Fragment or pack frames as needed
  - Changes transparent to receiver



3/1/2006 33

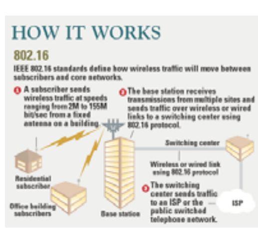
MAC Privacy Sub-layer

- Provides secure communication
  - Data encrypted with cipher clock chaining mode of DES
- Prevents theft of service
  - SSs authenticated by BS using key management protocol



3/1/2006 34

How It Works



http://www.networkworld.com/news/tech/2001/0903tech.html

3/1/2006 35

802.16 Network Entry

- Scanning
  - Scan for BS downlink channel
  - Synchronize with BS
  - Specifies channel parameters
- Ranging
  - Set PHY parameters correctly
  - Establish the primary management channel (for negotiation, authentication, and key management)
- Registration
  - Result in establishment of secondary management connection (for transfer of standard based management messages such as DHCP, TFTP)
- Establishment of transport connection

3/1/2006 36

IEEE 802.16 Features

- Scalability
- QoS
- Range
- Coverage

- WiMAX vs. Wi-Fi

IEEE 802.11 vs. IEEE 802.16 (1/4)

- Scalability
  - 802.11
    - Channel bandwidth for 20MHz is fixed
    - MAC designed to support 10's of users
  - 802.16
    - Channel b/w is flexible from 1.5 MHz to 20 MHz.
    - Frequency re-use.
    - Channel bandwidths can be chosen by operator (e.g. for sectorization)
    - MAC designed to support thousands of users.

IEEE 802.11 vs. IEEE 802.16 (2/4)

- Quality Of Service (QoS)
  - 802.11
    - No QoS support today (802.11e working to standardize)
    - Contention-based MAC (CSMA/CA) => no guaranteed QoS
  - 802.16
    - QoS designed in for voice/video
    - Grant-request MAC
    - Supports differentiated service levels.
      - e.g. T1 for business customers; best effort for residential.
    - Centrally-enforced QoS

IEEE 802.11 vs. IEEE 802.16 (3/4)

- Range
  - 802.11
    - Optimized for users within a 100 meter radius
    - Add access points or high gain antenna for greater coverage
    - Designed to handle indoor multi-path delay spread of 0.8μ seconds
  - 802.16
    - Optimized for typical cell size of 7-10km
    - Up to 50 Km range
    - No "hidden node" problem
    - Designed to tolerate greater multi-path delay spread (signal reflections) up to 10.0μ seconds

IEEE 802.11 vs. IEEE 802.16 (4/4)

- Coverage
  - 802.11
    - Optimized for indoor performance
    - No mesh topology support within ratified standards
  - 802.16
    - Optimized for outdoor NLOS performance (trees, buildings, users spead out over distance)
    - Standard supports mesh network topology
    - Standard supports advanced antenna techniques

IEEE 802.16 Security Issues

WMAN Threat Model

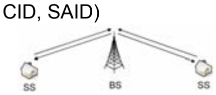
- PHY threats
  - Water torture attack, jammings, etc.
  - No protection.
- MAC threats
  - Typical threats of any wireless network
    - Sniffing, Masquerading, Content modification, Rouge Base Stations, DOS attacks, etc
  - 802.16a: assume trustworthiness of the next-hop mesh node
  - 802.16e: no constraints of attackers' location, management msg. more vulnerable.

Security Issues

- Provides subscribers with privacy across the fixed broadband wireless network
- Protect against unauthorized access to the data transport services
  - Encrypt the associated service flows across the network.
- Implemented by encrypting connections between SS and BS
- Security mechanisms
  - Authentication
  - Access control
  - Message encryption
  - Message modification detection (Integrity)
  - Message replay protection
  - Key management
    - Key generation, key transport, key protection, Key derivation, Key usage

IEEE 802.16 Security Model

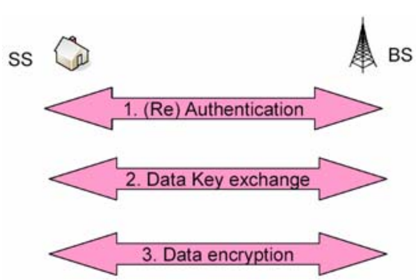
- Standard was adopted from DOCSIS specification (Data Over Cable Service Interface Specifications)
  - Assumption: All equipments are controlled by the service provider.
  - May not be suitable for wireless environment.
- Connection oriented (e.g. basic CID, SAID)
  - Connection
    - Management connection
    - Transport connection
    - Identified by connection ID (CID)
  - Security Association (SA)
    - Cryptographic suite (i.e. encryption algorithm)
    - Security info. (i.e. key, IV)
    - Identified by SAID



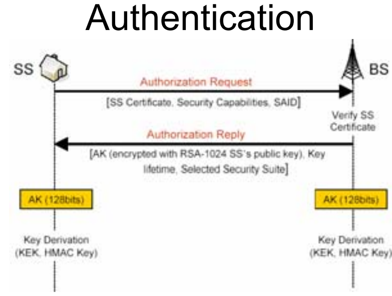
Security Association

- Data SA
  - 16-bit SA identifier
  - Cipher to protect data: DES-CBC
  - 2 TEK
  - TEK key identifier (2-bit)
  - TEK lifetime
  - 64-bit IV
- Authorization SA
  - X.509 certificate → SS
  - 160-bit authorization key (AK)
  - 4-bit AK identification tag
  - Lifetime of AK
  - KEK for distribution of TEK
    = Truncate-128(SHA1(((AK| 0^{44}) xor 53^{64})
  - Downlink HMAC key
    = SHA1((AK|0^{44}) xor $3A^{64}$)
  - Uplink HMAC key
    = SHA1((AK|0^{44}) xor $5C^{64}$)
  - A list of authorized data SAs

IEEE 802.16 Security Process

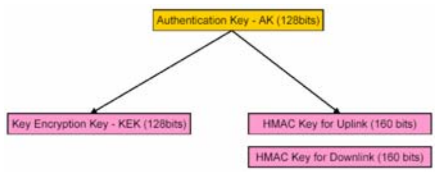


Authentication



SS →BS: Cert(Manufacturer(SS))
SS →BS: Cert(SS) | Capabilities | SAID
BS →SS: RSA-Encrypt*(PubKey(SS), AK) | Lifetime | SeqNo | SAIDList*

Key Derivation

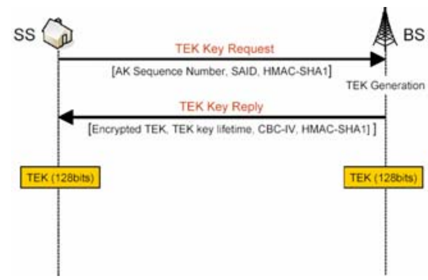


KEK = Truncate-128(SHA1(((AK| 0^{44}) xor 53^{64})

Downlink HMAC key = SHA1((AK|0^{44}) xor $3A^{64}$)

Uplink HMAC key = SHA1((AK|0^{44}) xor $5C^{64}$)

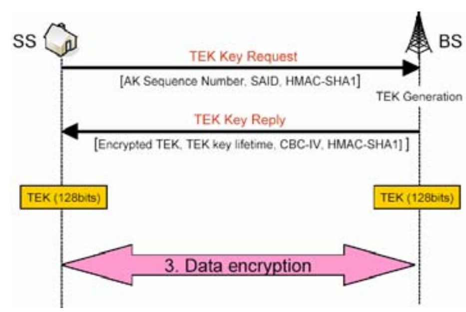
Data Key Exchange



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 – (provides Message Integrity and AK confirmation)

Data Encryption



Data Encryption

- Encrypt only data message not management message
- DES in CBC Mode
  - 56 bit DES key (TEK)
  - No Message Integrity Detection
  - No Replay Protection

Key Management

Message 1:
BS →*SS*: *SeqNo* | *SAID* | *HMAC*(1)
Message 2:
SS →*BS*: *SeqNo* | *SAID* | *HMAC*(2)
Message 3:
BS →*SS*: *SeqNo* | *SAID* | *OldTEK* |*NewTEK* | *HMAC*(3)

M1: to rekey a data SA, or create a new SA
TEK: encrypted with Triple-DES-ECB

IEEE 802.16 Security Flaws

- Lack of Explicit Definitions
  - Authorization SA not explicitly defined
    - SA instances not distinguished: open to replay attacks
    - Solution: Need to add nonces from BS and SS to the authorization SA
  - Data SA treats 2-bit key as circular buffer
    - Attacker can interject reused TEKs
      - SAID: 2 bits → at least 12 bits (AK lasts 70 days while TEK lasts for 30 minutes)
    - TEKs need expiration due to DES-CBC mode
      - Determine the period: 802.16 can safely produce 2^32 64-bit blocks only.

IEEE 802.16 Security Flaws

- Need for mutual authentication
  - Authentication is one way
    - BS authenticates SS
    - No way for SS to authenticate BS
    - Rouge BS → possible because all information's are public
    - Possible enhancement : BS certificate

  - SS→BS : Cert (Manufacturer)
  - SS→BS : SS-Rand | Cert(SS) | Capabilities | SAID
  - BS→SS : BS-Rand | SS-Rand | E(Pub(SS),AK)| Lifetime | Seq No | SAID | Cert (BS) | Sig (BS)

IEEE 802.16 Security Flaws

- Authentication Key (AK) generation
  - BS generates AK
  - No contribution from SS
  - SS must trust BS for the generation of AK

- AK = HMAC-SHA1(contribution from SS+ contribution from BS)
  - AK = HMAC-SHA1(pre-AK, SS-Random | BS-Random | SS-MAC-Addr | BS-MAC-Addr | 160)

IEEE 802.16 Security Flaws

- Key management
  - TEK sequence space (2-bit sequence #)
    - Replay attack can force reuse of TEK/IV
    - Increase it to 12-bit
  - No specification on the generation of TEK and therefore TEKs are random
  - No TEK freshness assurance

Message 1:
BS → SS: SS-Random | BS-Random | *SeqNo*12 | *SAID* | *HMAC*(1)]
Message 2:
SS → BS: SS-Random | BS-Random | *SeqNo*12 | *SAID* | *HMAC*(2)
Message 3:
BS →SS: SS-Random | BS-Random | *SeqNo*12 | *SAID* | *OldTEK* | *NewTEK* | *HMAC*(3)

Not transmit TEK, generate TEK:
TEK = HMAC-SHA1(pre-TEK, SS-Random | BS-Random | SS-MAC-Addr | BS-MAC-Addr | SeqNo12 | 160)
SS-Random | BS-Random is used as an instance identifier

IEEE 802.16 Security Flaws

- Alternative Cryptographic Suite
  - IEEE 802.16 used DES-CBC
    - DES uses 64 bit block size
    - According to studies a CBC mode using block cipher with n-bit block loses its security after operating on 2^n/2 blocks with the same encryption key.
    - So IEEE 802.16 can safely produce 2^32 64-bit blocks.
    - Also IV used in DES-CBC are predictable.

  - Use AES-CCM as encryption primitive
    - 128 bit key (TEK)
    - HMAC-SHA1
    - Replay Protection using Packet Number

IEEE 802.16 Security Flaws

- Data protection errors
  - 56-bit DES… does not offer strong data confidentiality
  - Forgeries or replies (WEP-like vulnerability)
    - Writes are not prevented, read-protects only
    - even w/o encryption key
  - Uses a PREDICTABLE initialization vector (while DES-CBC requires a random IV)
    - IV is the xor of the IV in SA and the PHY synchronization field from the most recent GMH

  - Generates each per-frame IV randomly and inserts into the payload.
    - Though increases overhead, no other choice.

IEEE 802.16 Security Flaws

- No data Authentication
  - Encryption only prevents reading but any one without key can write (change the message).
  - Strong MAC needs to be included in the message

3/1/2006 61

Remedies

- 802.16e
  - Use AES-CCM as encryption primitive
  - Use flexible EAP authentication scheme
  - Add fields to messages to compute AK better
- Formally define authorization SA

3/1/2006 62