WiMAX/802.16 Broadband Wireless Networks

Michel Barbeau and Christine Laurendeau
School of Computer Science
Carleton University

Outline

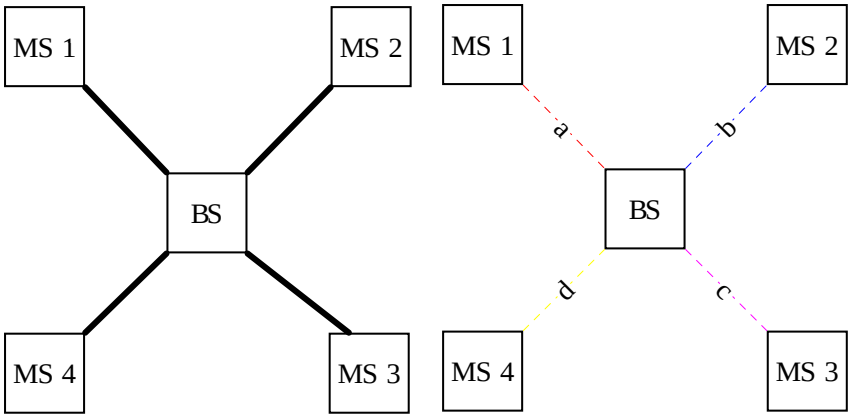
- Overview
- Physical Layer
- MAC Layer
- Security

Overview

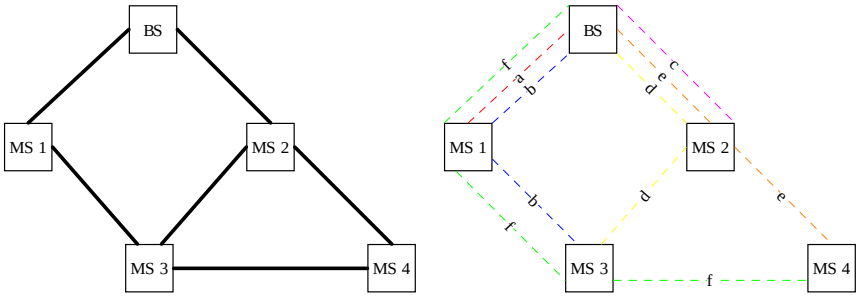
What is WiMAX/802.16?

- IP-based mobile and wireless access
  - Internet access
  - VoIP
- Secure communications
- Handover between networks of different technologies and management authorities
- Broadband in remote areas

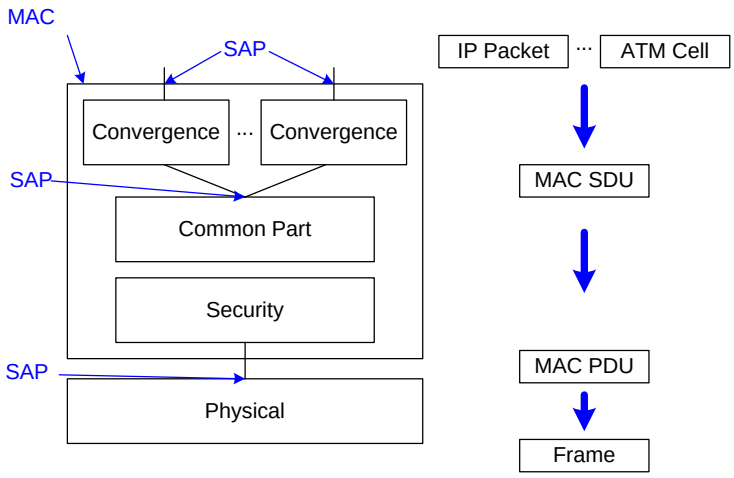
Point-to-multipoint Topology: Links and Connections



Mesh Mode Links and Connections



Layered Architecture



WiMAX Service in Canada

- Option 1: Fixed
  - Technician installed outdoor modem
  - Rural area coverage
  - Download speed 2 Mbps; Upload speed 256 kbps
  - $50 monthly
- Option 2: Nomadic
  - Portable wireless modem
  - Download speed 512kbps or 3Mbps; Upload speed 128kbps or 384 kbps
  - $45 or $60 monthly

WiMAX/802.16 vs WiFi/802.11

	WiMAX	WiFi
Regulation	(Un)licensed	Unlicensed
Range	in Kms	in Meters
Rate	Exclusive Mbps	Shared Mbps
Access	FDD, TDD, TDMA	CSMA/CA
Service	Connection	Best effort (opt. ack)

Physical Layer

Why is WiMAX faster?

- Bandwidth
- Power
- Sensitivity
- Modulation

Shannon's Equation

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

Bandwidth

System	Bandwidth	Modulation	Rate	Transmission
Bluetooth	1 M Hz	GFSK	1 M bps	FH SS
802.11	1 M Hz	GFSK	1 and 2 M bps	FH SS
	10 M Hz	DBPSK	1 M bps	DS SS
	10 M Hz	DQPSK	2 M bps	DS SS
802.11b	10 M Hz	CCK	11 M bps	CCK
802.11a	16.6 M Hz	OFDM	54 M bps	OFDM
802.16 SC-25	25 M Hz	QPSK	40 M bps	SC
802.16 SC-25	25 M Hz	QAM-16	60 M bps	SC
802.16 OFDM-7	7 M Hz	QAM-64	120 M bps	OFDM

Power

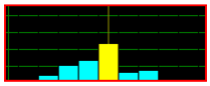
Radio	Frequency	Power
Bluetooth Class 1	2.4 - 2.4835 G Hz	20 dBm
Bluetooth Class 2		4 dBm
Bluetooth Class 3		0 dBm
802.11	2.4 - 2.4835 G Hz	20 dBm
802.11b	2.4 - 2.4835 G Hz	20 dBm
802.11a	5.15- 5.35 G Hz	16 - 29 dBm
802.16 SC-25 QPSK	10 - 66 G Hz	$\geq$ 15 dBm
802.16 SC-25 QPSK	10 - 66 G Hz	$\geq$ 15 dBm
802.16 SC-25 QAM-16	10 - 66 G Hz	$\geq$ 15 dBm
802.16 SC-25 QAM-16	10 - 66 G Hz	$\geq$ 15 dBm
802.16 OFDM-7	2 - 11 G Hz	15 - 23 dBm

Sensitivity

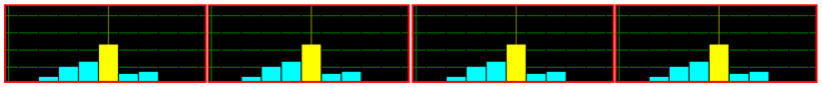
Radio	Rate	Error	Sensitivity
Bluetooth Class 1	1 M bps	10^{-3} (BER)	-70 dBm
Bluetooth Class 2	1 M bps	10^{-3} (BER)	-70 dBm
Bluetooth Class 3	1 M bps	10^{-3} (BER)	-70 dBm
802.11	1 M bps	3% (FER)	-80 dBm
	2 M bps	3% (FER)	-75 dBm
802.11b	11 M bps	8% (FER)	-83 dBm
802.11a	54 M bps	10% (PER)	-65 dBm
802.16 SC-25 QPSK	40 M bps	10^{-3} (BER)	-80 dBm
802.16 SC-25 QPSK	40 M bps	10^{-6} (BER)	-76 dBm
802.16 SC-25 QAM-16	60 M bps	10^{-3} (BER)	-73 dBm
802.16 SC-25 QAM-16	60 M bps	10^{-6} (BER)	-67 dBm
802.16 OFDM-7	120 M bps	10^{-6} (BER)	-78 - -70 dBm

Modulation

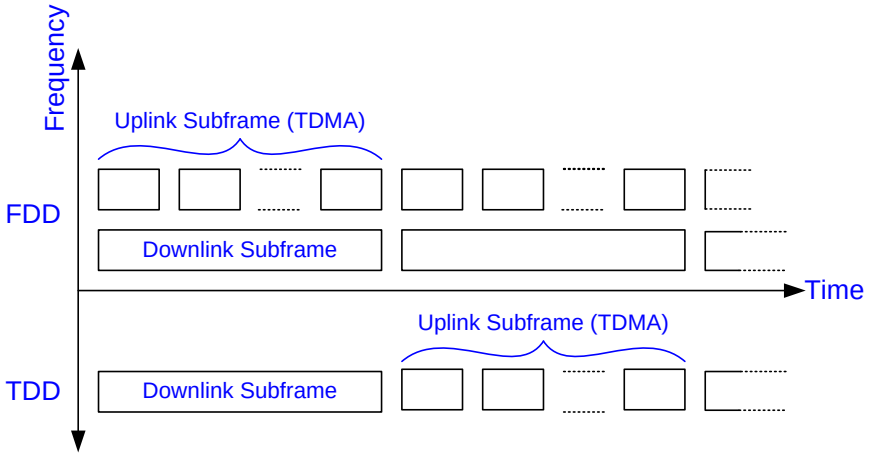
Standard



Orthogonal Frequency Division Multiple Access (OFDM)

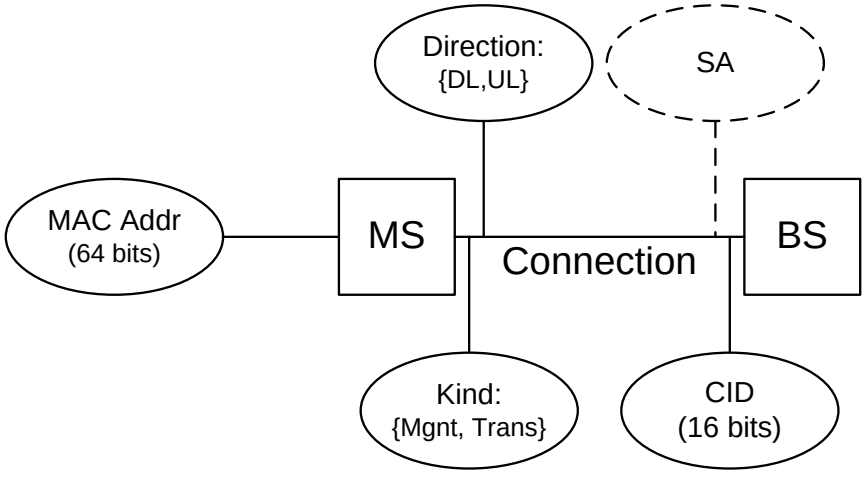


Framing



MAC Layer

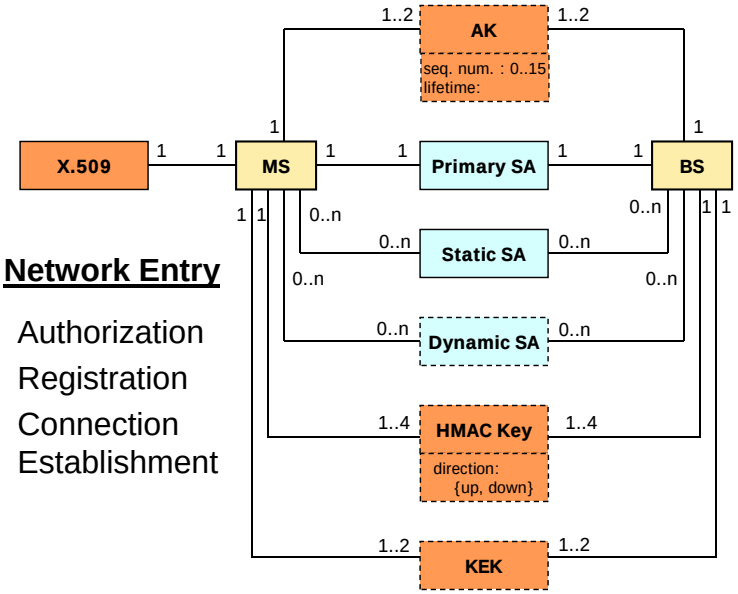
MAC Layer Concepts



Management Connections

Type	Usage	When	SA
DL Basic	Short & urgent mgnt msgs	MS init time	None
UL Basic			
DL Primary	Delay tolerant mgnt msgs		
UL Primary			
DL Secondary	IP encap mgnt msgs (e.g. DHCP, SNMP, TFP)	MS init time (optional)	Primary
UL Secondary			

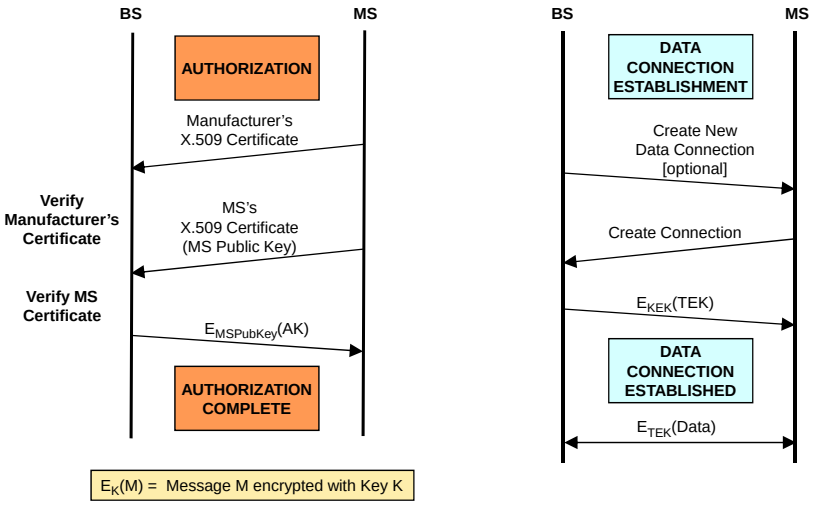
WiMAX/802.16 Security Model



Network Entry

- Authorization
- Registration
- Connection Establishment

Authorization and Connection Establishment



Threat Analysis: The Idea

- Determine principal threats to WiMAX/802.16
  - Threat to Authentication: Masquerading
  - Threat to Confidentiality: Eavesdropping
  - Threat to Integrity: Message Modification

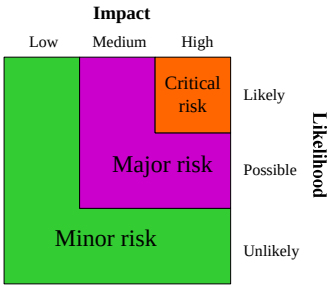
- Choose threat analysis methodology
  - European Telecommunications Standards Institute

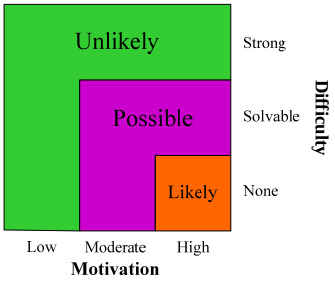
ETSI World Class Standards

- For each threat:
  - Evaluate risk factors on a scale of severity
  - Combine risk factors to rank overall risk

ETSI Risk Assessment

- Overall Risk Assessment:
  - Critical, Major, Minor
- Risk Factors:
  - Likelihood of threat occurrence
  - Impact on user or system





- Likelihood Assessment Factors:
  - Motivation of attacker
  - Technical difficulty

WiMAX/802.16 Threat Analysis

Threat	Security Measures	Likelihood	Impact	Risk
Eavesdropping Management Msgs	None	Likely	Medium	Major
			High	Critical
Eavesdropping Data Traffic Msgs	DES-CBC, AES-CCM	Unlikely	Medium	Minor
Masquerading MS: Identity Theft BS: Rogue Station	Device List	Likely	High	Critical
			Medium	Major
	X.509 certificate	Possible	High	Major
		Unlikely	Medium	Minor
	EAP	Possible	High	Major
			Medium	

References

- M. Barbeau and C. Laurendeau, "Analysis of Threats to WiMAX/802.16 Security", in: Y. Zhang and H.-H. Chen (Editors), *Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Networks,* CRC Press, 2008.
- M. Barbeau and E. Kranakis. *Principles of Ad Hoc Networking*. John Wiley & Sons Ltd, West Sussex, England, 2007.
- M. Barbeau and C. Laurendeau, "Tilting at Giants: Avoiding Quixotic Pursuits in Understanding the Threats to Wireless Network Security," MITACS e-newsletter, *Connections*, September 2007.
- M. Barbeau, "WiMax/802.16 Threat Analysis*," 1st ACM Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet)*, 2005.

URLs: **www.scs.carleton.ca/~barbeau**
www.scs.carleton.ca/~claurend