



NAVAL  
POSTGRADUATE  
SCHOOL

# Threat Level Orange: How much can you count on your wireless mobile device?

29 Oct 2009

John McEachen, Ph.D.

Professor

Department of Electrical and Computer  
Engineering

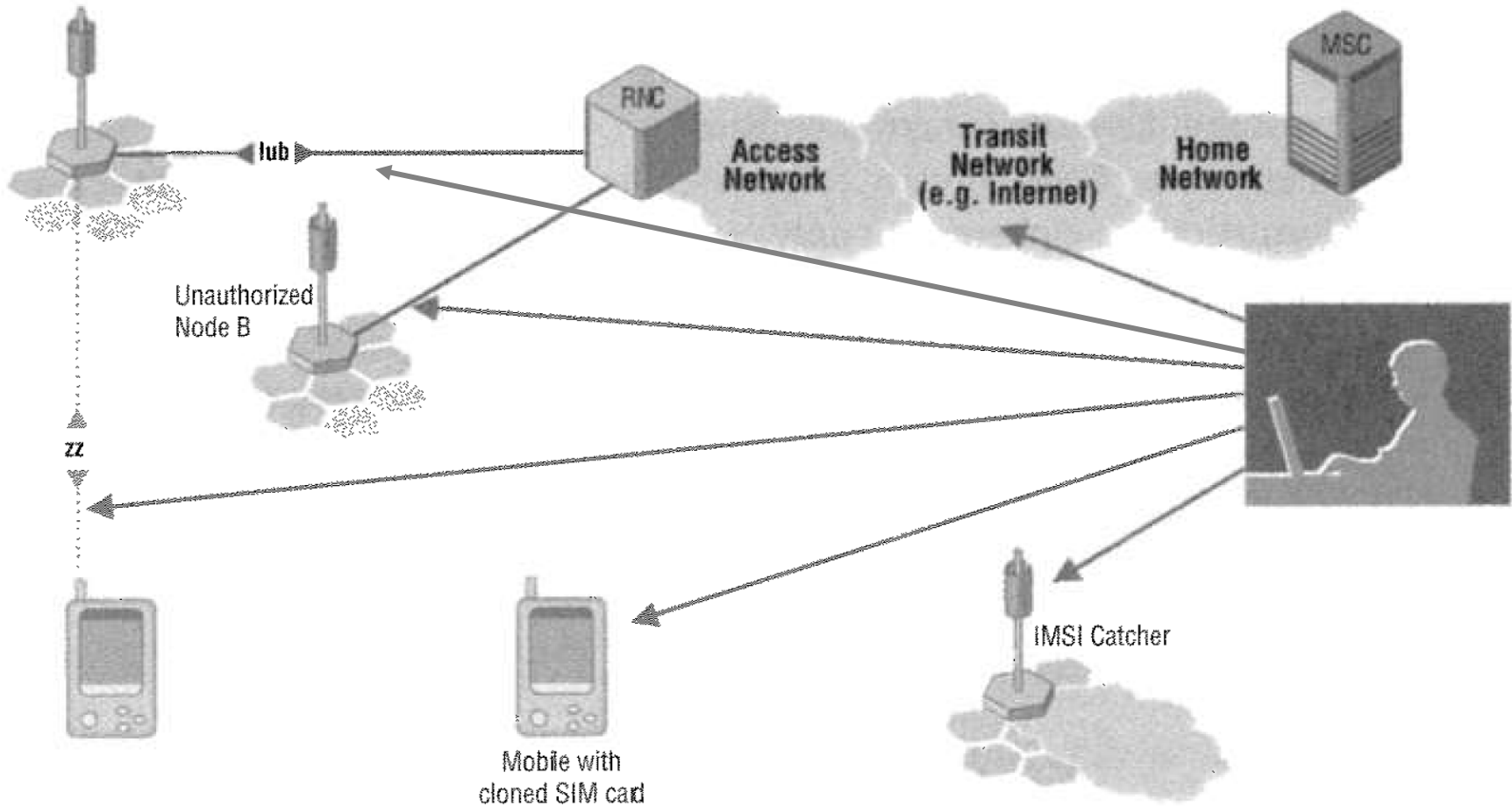
Naval Postgraduate School



# So how important is your mobile?

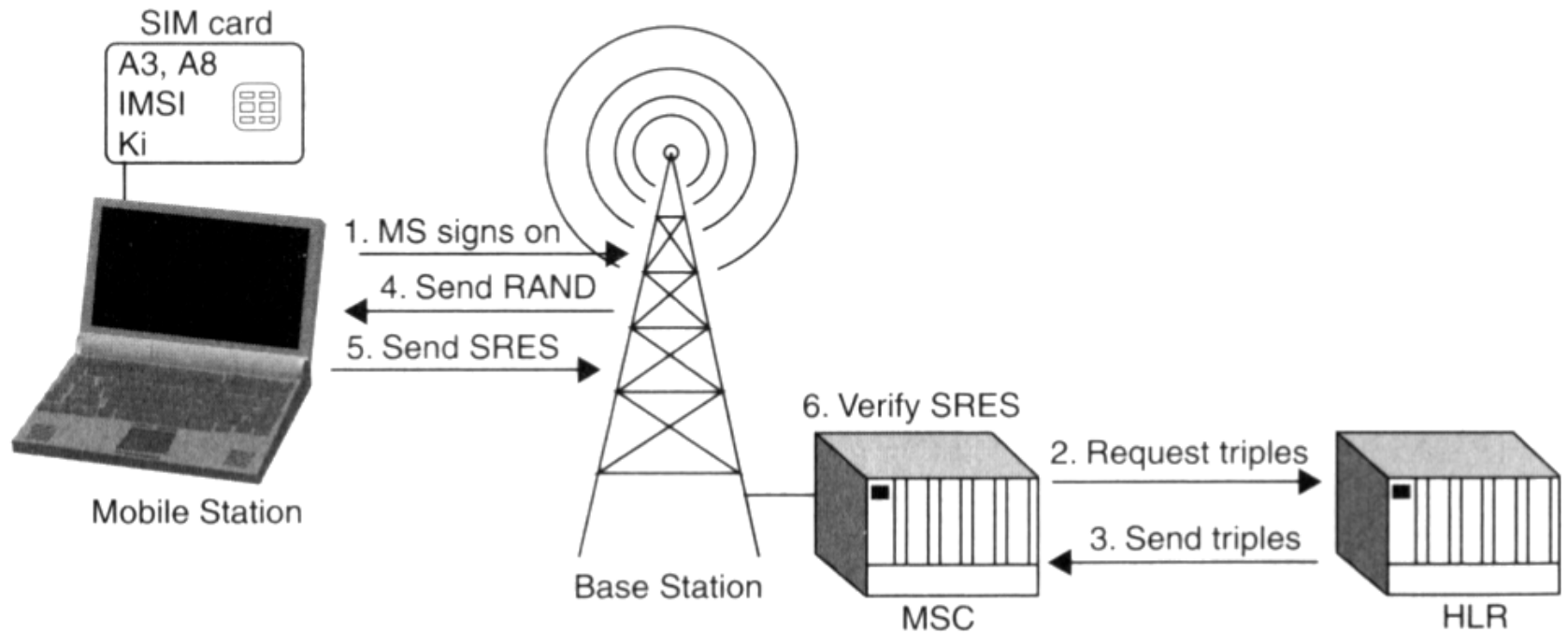
- Samsung Mobile (13 Oct 09) polled 300 people in 25 metropolitan areas...
  - *38% of women nationally would rather give up sex for a year than give up their cell phone for the same period*
    - 18% of men would do the same
- 1 in 7 Americans use only their cell phone and do not have a landline
  - *Harris Poll #36, 4 April 2009*
- 15% of Japanese do not carry a wallet, cash or credit cards; only a mobile phone
  - *Forrester Research, 12 August 2009*

# Points of Attack



**Figure 1.29** Potential attack points of intruders.

# GSM (2G) Registration and Authentication



**Figure 6.2: GSM Authentication**



- One-way authentication gave rise to rogue BTS attacks
  - Phone registers with strongest BTS signal
- Once a phone has registered with a rogue BTS, the rogue BTS can...
  - Turn off encryption
  - Relay call to legitimate BTS thus acting as MITM
  - Enable GPS
  - Conduct DoS (by not forwarding calls)
  - Other nasty things



*UMTS (3G) fixed this with  
two-way authentication,*

*but...*



*IEEE  
Spectrum  
July 2007*

**CRIME**

## THE ATHENS AFFAIR

**HOW SOME EXTREMELY SMART HACKERS PULLED OFF THE MOST AUDACIOUS CELL-NETWORK BREAK-IN EVER**

By Vassilis Prevelakis & Diomidis Spinellis

**ON 9 MARCH 2005,** a 38-year-old Greek electrical engineer named Costas Tsalikidis was found hanged in his Athens loft apartment, an apparent suicide. It would prove to be merely the first public news of a scandal that would roil Greece

known as Vodafone Greece, the country's largest cellular service provider; Tsalikidis was in charge of network planning at the company. A connection seemed obvious. Given the



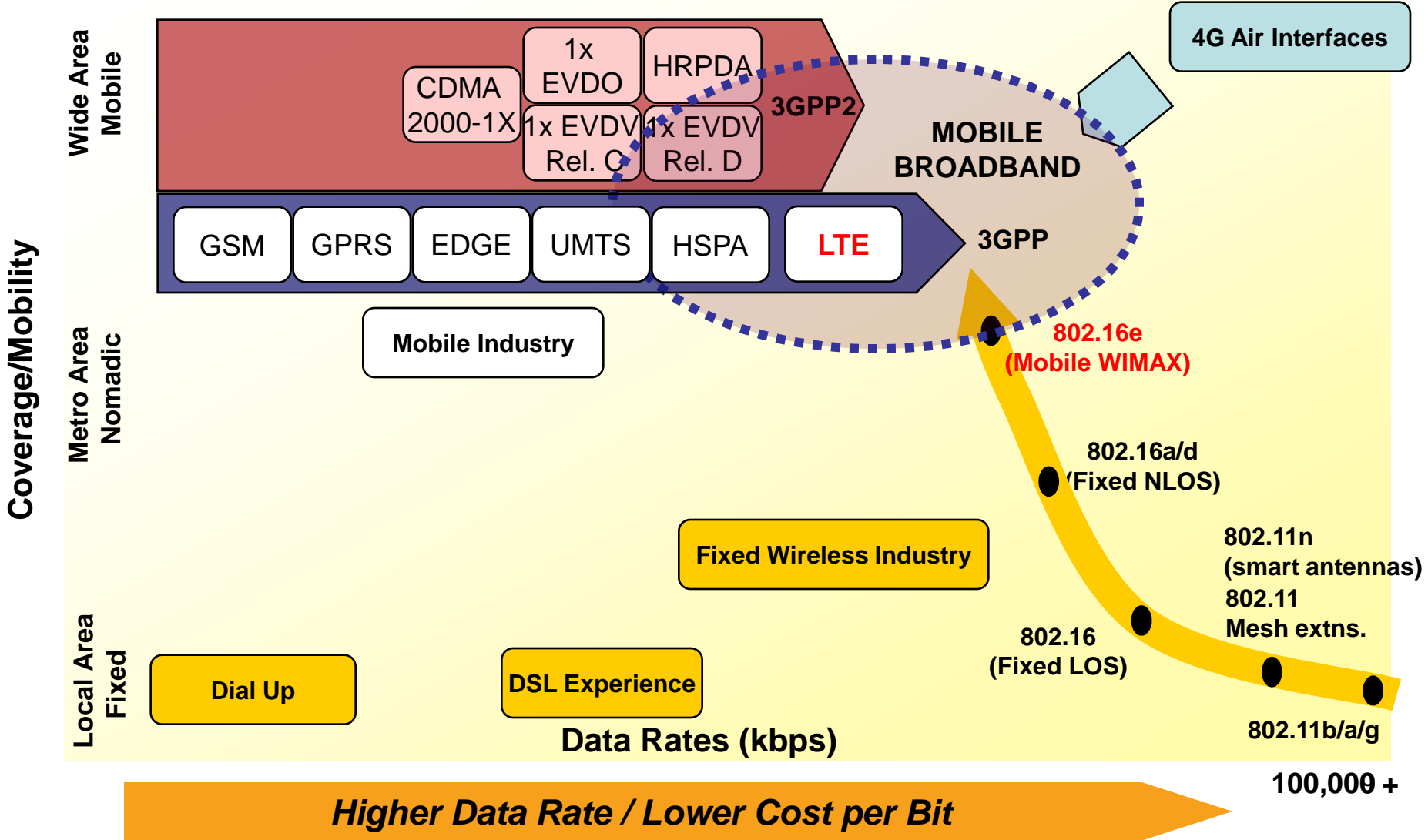
NAVAL  
POSTGRADUATE  
SCHOOL

**Where is the mobile industry  
going?**





# Two Key technologies are evolving to meet the Wireless Broadband Requirements





# WMAX/LTE Common Themes

## Radio Access Network

- + OFDMA Technology
- + Downlink 100Mbps+
- + Uplink 20-50Mbps+
- + User <10msec latency
  
- + Flexible spectrum –  
1.25-20MHz
- + FDD and TDD
  
- + VoIP ~3x time  
UMTS architecture
  
- + MIMO/Beamforming
- + E2E QOS

## Packet Core

- + New all IP collapsed  
architecture
  
- + Centralized mobility  
and application layer  
(IMS based)
  
- + E2E QOS
  
- + Access technology  
agnostic
  
- + Connect to legacy  
GSM/UMTS core (LTE)



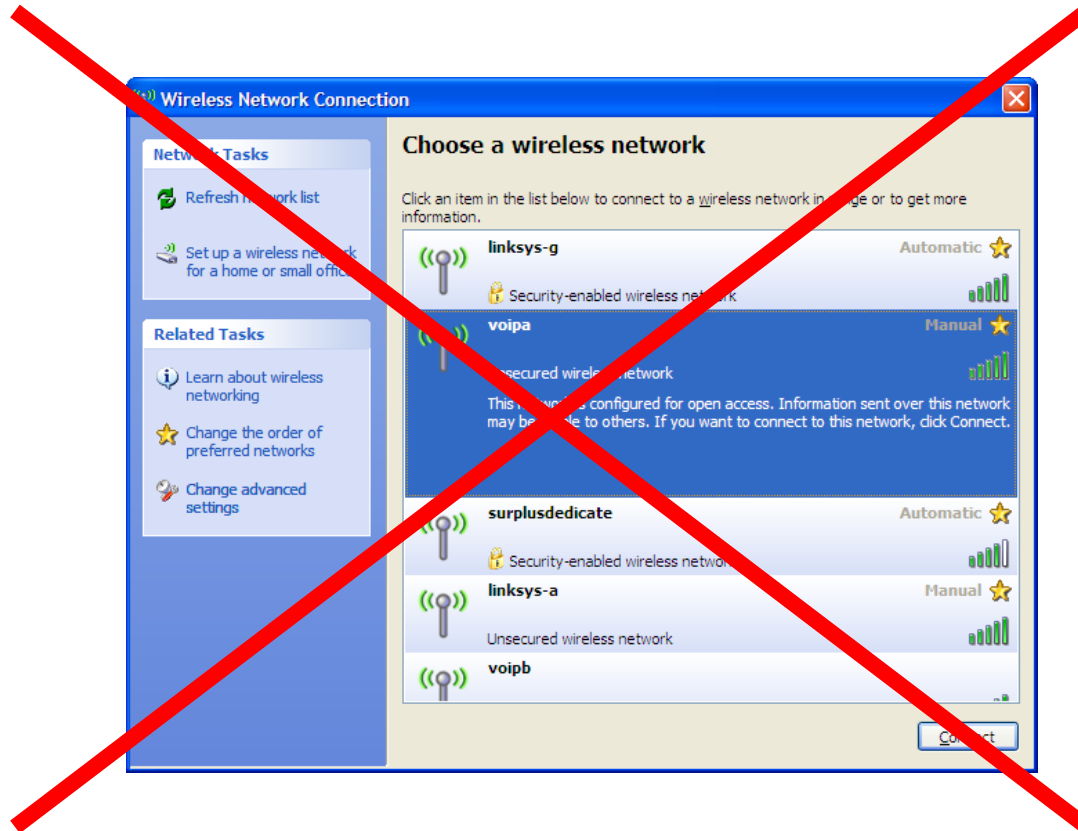
# *WiMax is not WiFi on steroids!*

<b>WiMax</b>	<b>WiFi</b>
Synchronous framing	Asynchronous framing
No specified carrier frequency (License dependent from 2 – 10GHz)	Standardized carrier frequencies in 2.4 GHz and 5.8 GHz spectra
Variable bandwidths (3.5, 5, 7, 10 MHz and more)	22.5 MHz bandwidth
100s of users	10's of users
State-driven control	Event-driven control

# If you don't know what you're looking for...



## ...finding a WiMax network is not easy!





- Envisioned as a 4G cell phone replacement technology (data first)
- Provides Corporate/Residential/Mobile broadband wireless access
  - ~3-70 Mbps (modulation/code rate dependent)
    - Think of as Wireless Cable Modem for residential customers
  - Coverage area of a few km (density dependent)
  - Mobility support ~60kmph (802.16e-2005)
  - ~100's of “active” subscribers
- Large network structures similar to those in current cellular deployments
- Attractive for developing countries without wired infrastructure
  - Rapidly deployable
  - Relatively low deployment cost

# Sprint makes \$3B bet on WiMax

## Value Proposition



- Complement existing services
- Expand mobile broadband market
- Low Cost nationwide service
- Full Mobility
- CE devices, Portable Multimedia Users

## Target Segments



- Residential
- Enterprise
- SoHo
- CE Devices Users

## Differentiators



- First-to-Market
- Nationwide Coverage
- Anywhere broadband for CE devices
- Dual Mode (WiMAX/CDMA) handsets

## Services Offered



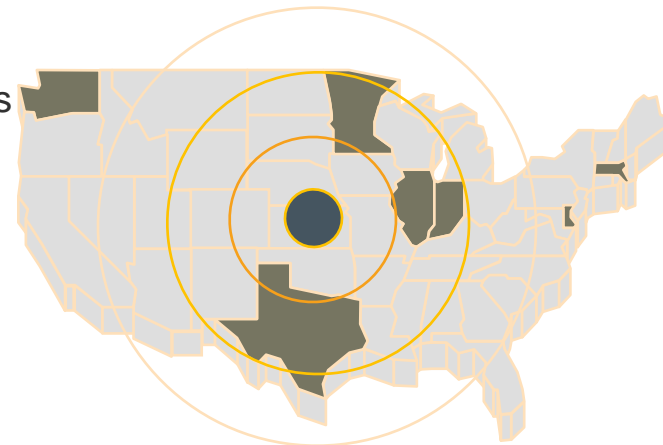
- Home/SoHo Broadband
- Visual centric Portable Multimedia
- Interactive Applications
- CE Devices support

## Major Competitors



- Incumbent Wireless Operators
- Incumbent Cable Operators

**First-to-Market  
Nationwide  
WiMAX 16e Mobile  
Network  
In the USA**





## Turbocharge your Now connection. Get 4G speeds up to 10x faster than 3G.

### Sprint 3G/4G USB Modem U300

- Blazing-fast speed, faster than any wireless service available from AT&T or Verizon
- Instantly send or download mammoth files and huge videos on 4G
- 4G lets you videoconference live without the lag
- Access 3G speeds nationwide
- Get moving with GPS services on the 3G network
- Be fast and fearless with top-notch security features
- Check out our [4G cities](#)



First and only wireless 4G network from a national carrier.

# Free

For your business account.

# Free

For your non-business account.

After a \$50 mail-in rebate. Requires an eligible upgrade (or new-line activation) and a two-year agreement.

**Get it now** →

**Tell me when it's out** →

- Check coverage area
- Sprint 30-day guarantee

## PCWorld

Sprint tested as the most reliable 3G network overall among U.S. carriers in a 3G performance test conducted by PC World.

# Mobile WiMax Phones



Samsung

HTC



# Wateen : First nationwide WiMAX 16e deployment in the world

## Background



Division of Warid Telecom (Abu Dhabi)  
Nationwide WiMAX license (3.5 GHz) in Pakistan

## Value Proposition



Speedy Installation  
Low Cost replacement to DSL  
E2E network (IP NGN Core, IMS)  
Nationwide service footprint  
One Stop Triple Play

## Target Segments



Residential  
Enterprise  
SME  
SoHo

## Differentiators



Nationwide Coverage  
Untethered (Wireless)  
Fixed with evolution to Mobility

## Services Offered

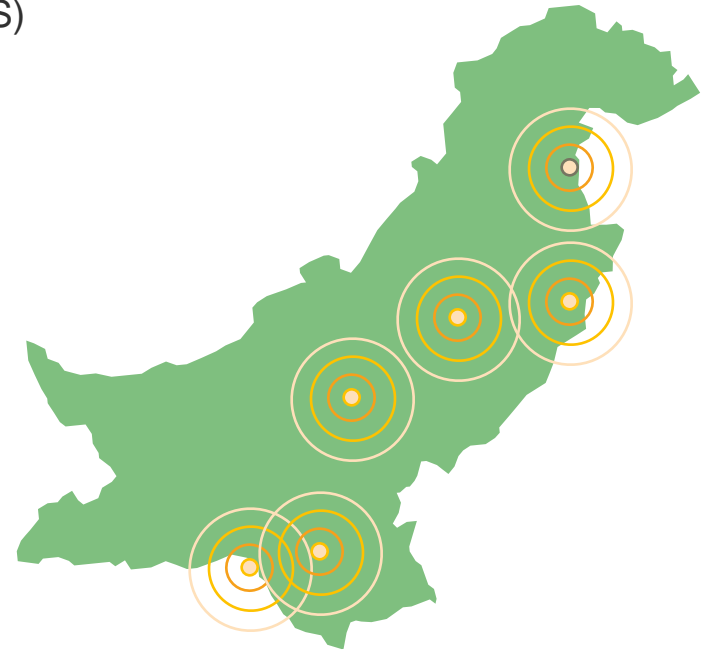


Internet Access  
VoIP  
VPN

## Major Competitors



Incumbent Fixed Operators



# Worldwide Deployment

- Worldwide use of Wireless Broadband Networks



 Fixed WiMAX

 Mobile WiMAX



# 802.16-2004 Vulnerabilities Study

	Threat	Algorithm(s)	Likelihood	Impact	Risk
Availability - Physical Layer	Jamming		3	1	3
	Scrambling		2	1	2
Confidentiality	Eavesdropping management messages		3:3	2:1	6:3
	Eavesdropping traffic	DES-CBC, AES-CCM	1	1	1
Integrity Authentication Confidentiality	BS or MS masquerading	Device list	3	3	9
		X.509 dev. Auth.	2:1	3:2	6:2
		EAP	2:2	3:2	6:4
Integrity Non repudiation	Management message modification	No MAC	3	3	9
		SHA-1 MAC	2	3	6
		AES MAC	1	3	3
Integrity Non repudiation	Data traffic modification	Without AES	3	1	3
		With AES	1	1	1
Availability	DoS on BS or MS	EAP, SHA-1, AES MAC	3:3	3:2	9:6

-After [Barbeau]

## 802.16 2004 Vulnerabilities

		Rationale		
Criteria	Cases	Difficulty	Motivation	Rank
Likelihood	Unlikely	Strong	Low	1
	Possible	Solvable	Reasonable	2
	Likely	None	High	3
Impact	Low	User Annoyance	System Very limited outages	1
	Medium	Loss of service	Limited outages	2
	High	Long time loss of service	Long time outages	3
Risk	Minor	No need for countermeasures		1, 2
	Major	Threat need to be handled		3, 4
	Critical	High priority		6, 9



NAVAL  
POSTGRADUATE  
SCHOOL

# Recent WiMax Research Findings

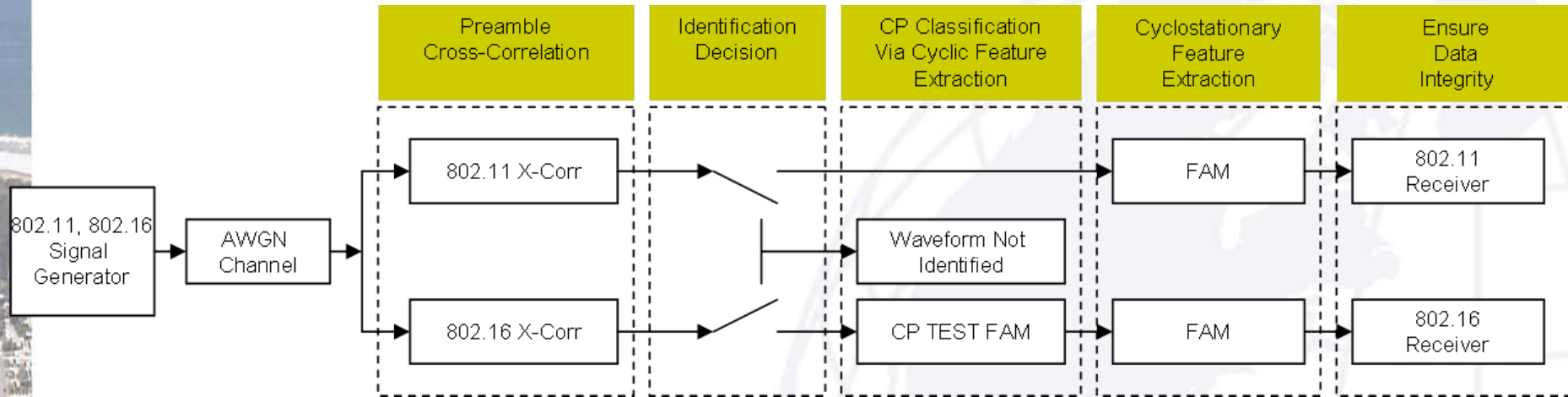




# WiMax Attack Methodology



- Functional diagram of implementation model



Major Steve Schnur, USMC, MSEE, Sep 2009

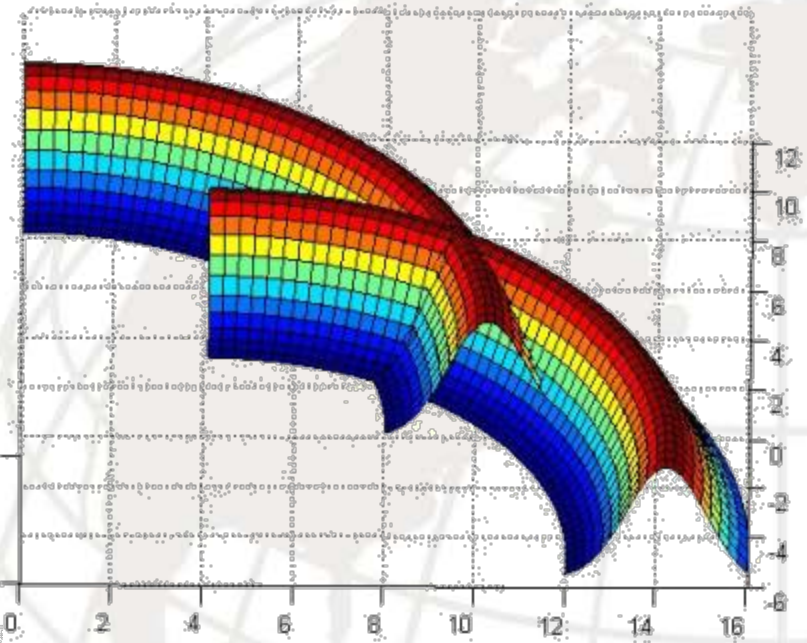
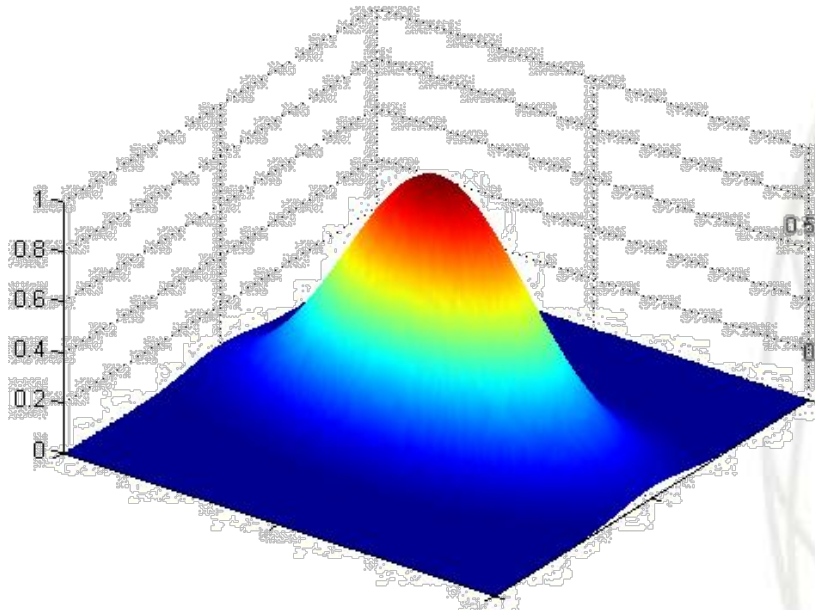
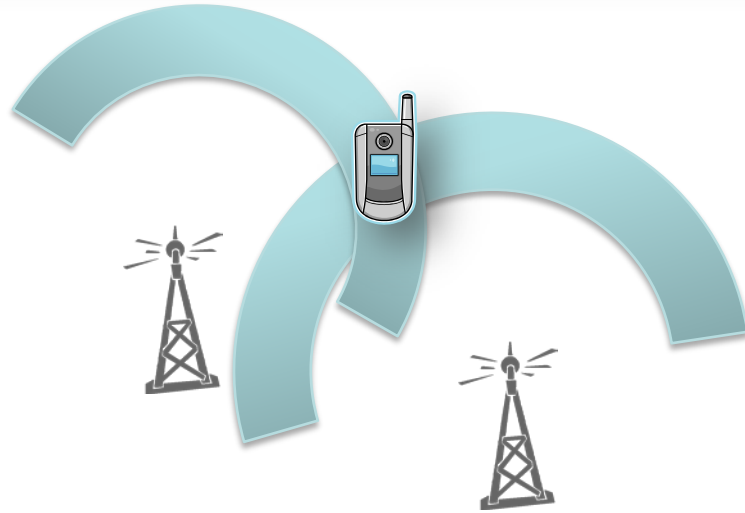


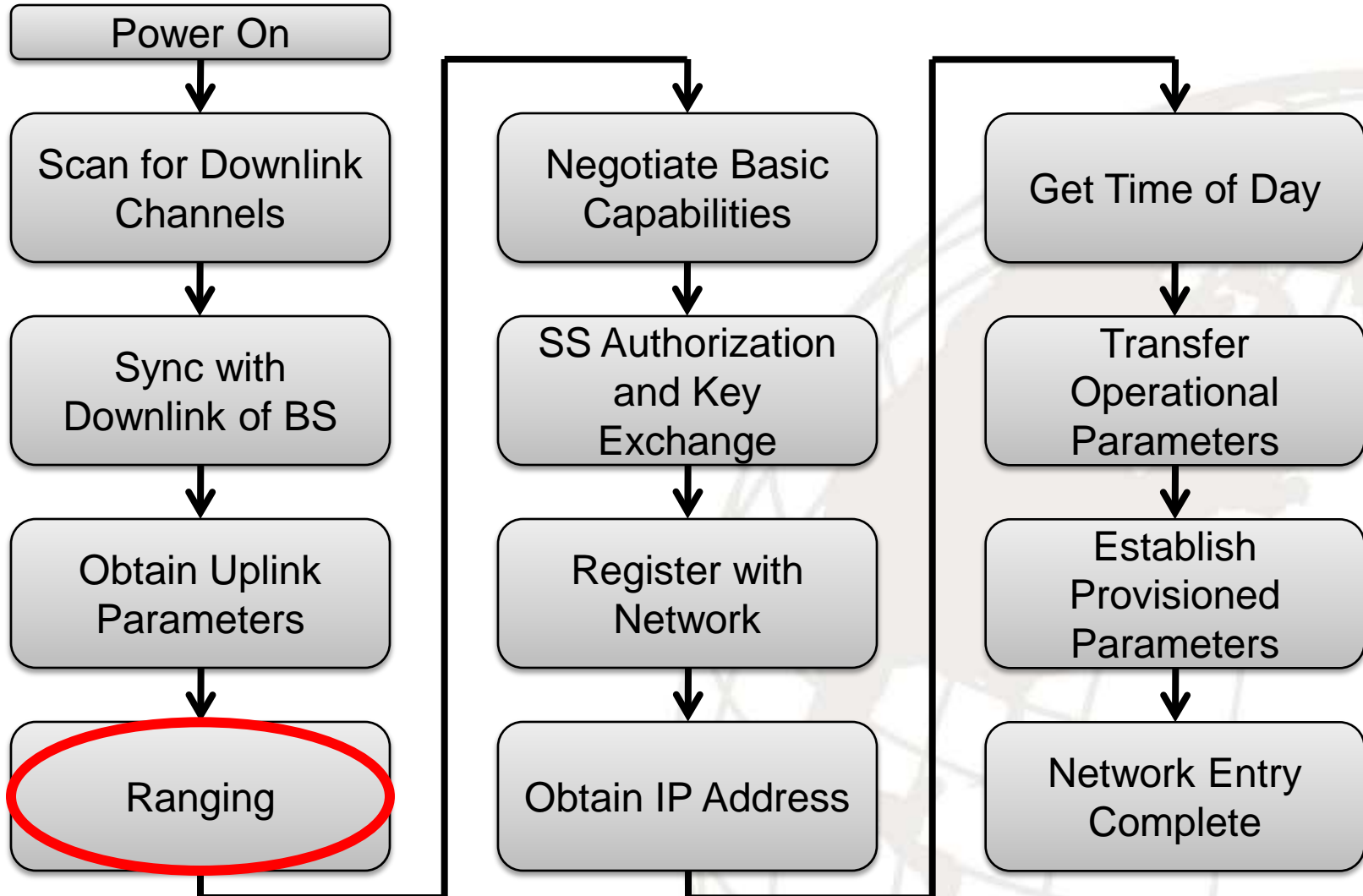
# Geolocation of WiMax Signals

- Received Signal Strength
- Angle of Arrival
- Frequency Difference of Arrival
- Time Difference of Arrival
- Signal Internals

LT Don Barber, USN, MSEE, Dec 2009

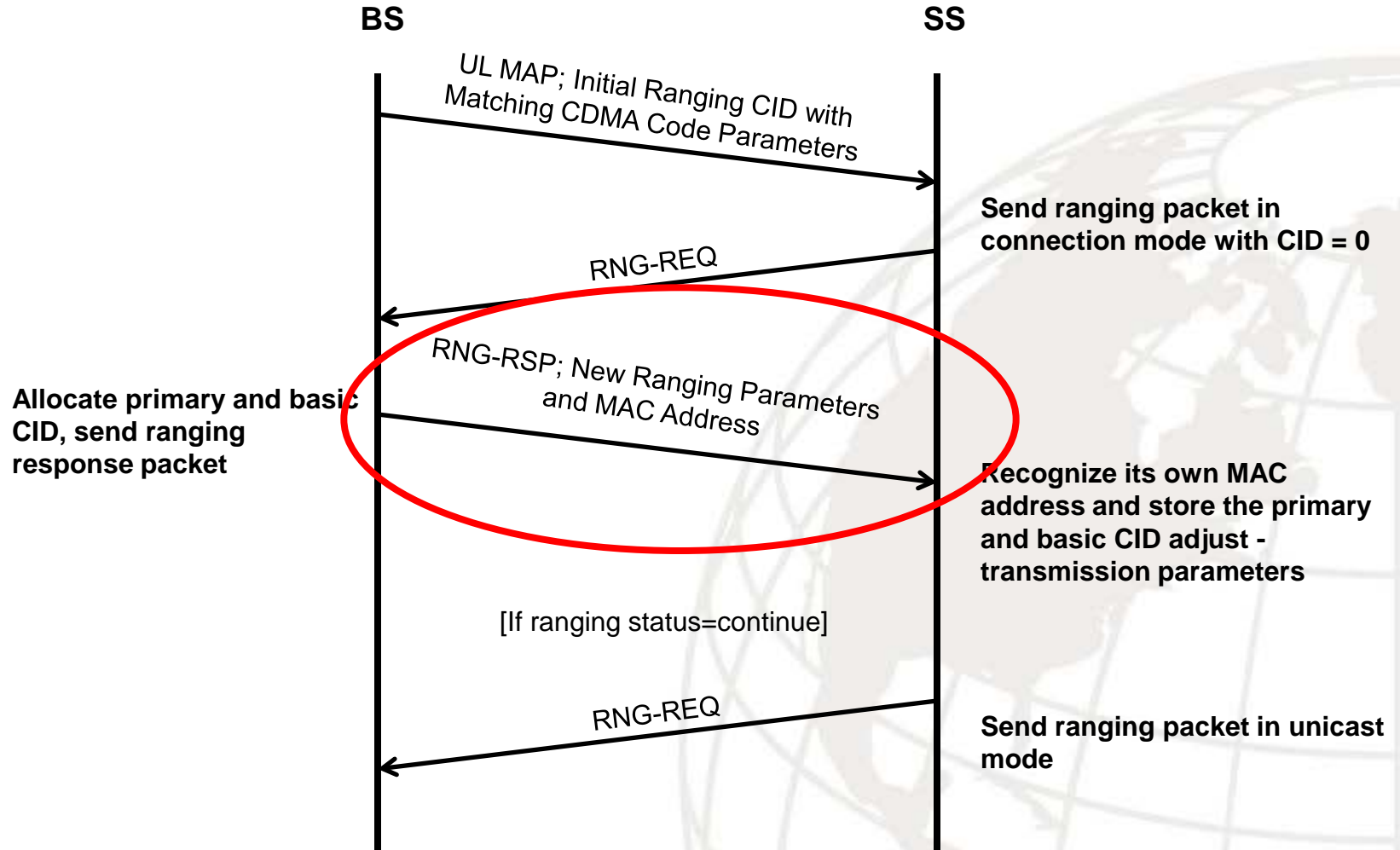
# Crossing Timing Ranges







# Ranging & Adjust Procedure





- Management Message Type (MMT) 5
- Ranging Status 1 “Continue”
- Later contiguous bits:

	Type	# Bytes	Values
Timing Adjust	01	04	FF FF FF BE
Power Level Adjust	02	01	EB
Offset Frequency Adjust	03	04	00 00 00 7A



# JavaScript Plotting Interface

OWL (Beta v9.07g)

**OFDM Wireless Locator**

Beta Version 9.07g

TA is set for  $F_s = 4$  MHz. Please enter latitude/longitude in decimal degrees ([converter](#)).

SITE 1 (Base Station) Lat:  Lng:  Offset:  TA:

SITE 2 (Collector) Lat:  Lng:   TA:

MARK (Subscriber) Lat:  Lng:       Details:

Map Satellite Hybrid Terrain

Done Computer | Protected Mode: Off 100%



- Potential for Better than 10x Improvement Over GSM TA Location Techniques
  - 40m for WiMax vs. 400m for GSM
- RNG-RSP Successfully Received in Traffic
- Small Timing Adjust Variance in Repeated Observations
- Fixed WiMAX Techniques Directly Applicable to Mobile WiMAX
- Periodic and Handoff Ranging Can Add to Location Accuracy



# WiMax Denial of Service

Major Devin Licklider, USMC, MSEE, Sep 2009



# Determine Timing



NAVAL  
POSTGRADUATE  
SCHOOL

# LPPD Jamming Signal Insertion





## Full DOS occurs at:

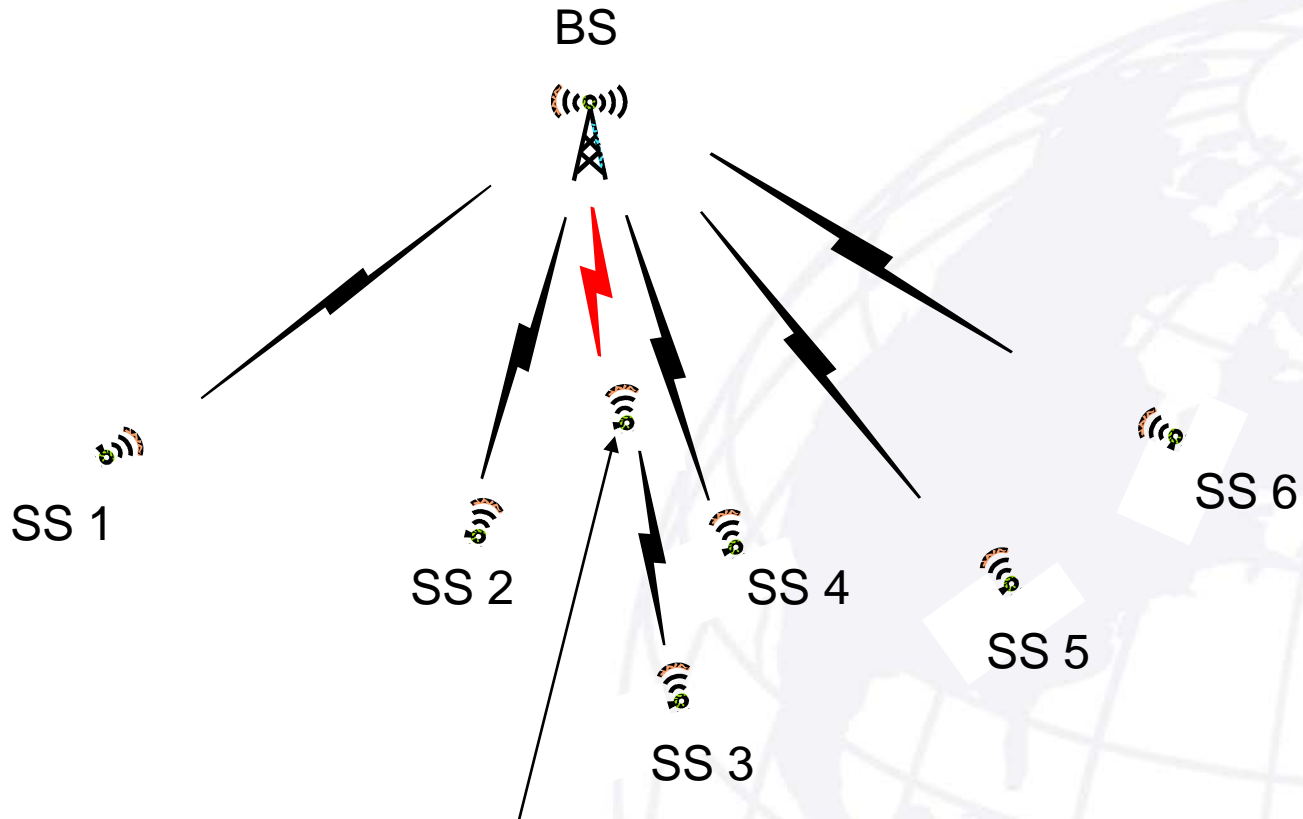
-23 dBm LPPD Collision  
technique

-10 dBm Continuous Jamming

At -23 dBm point LPPD  
requires only 13% of  
the energy required by  
continuous jamming



# Denial of Service Scenario Utilizing LPPD Collision Generation



## LPPD Collision Generator

-Ideally using a randomly changing combination of SSs 2, 3 and 4 to hide its signal in theirs.

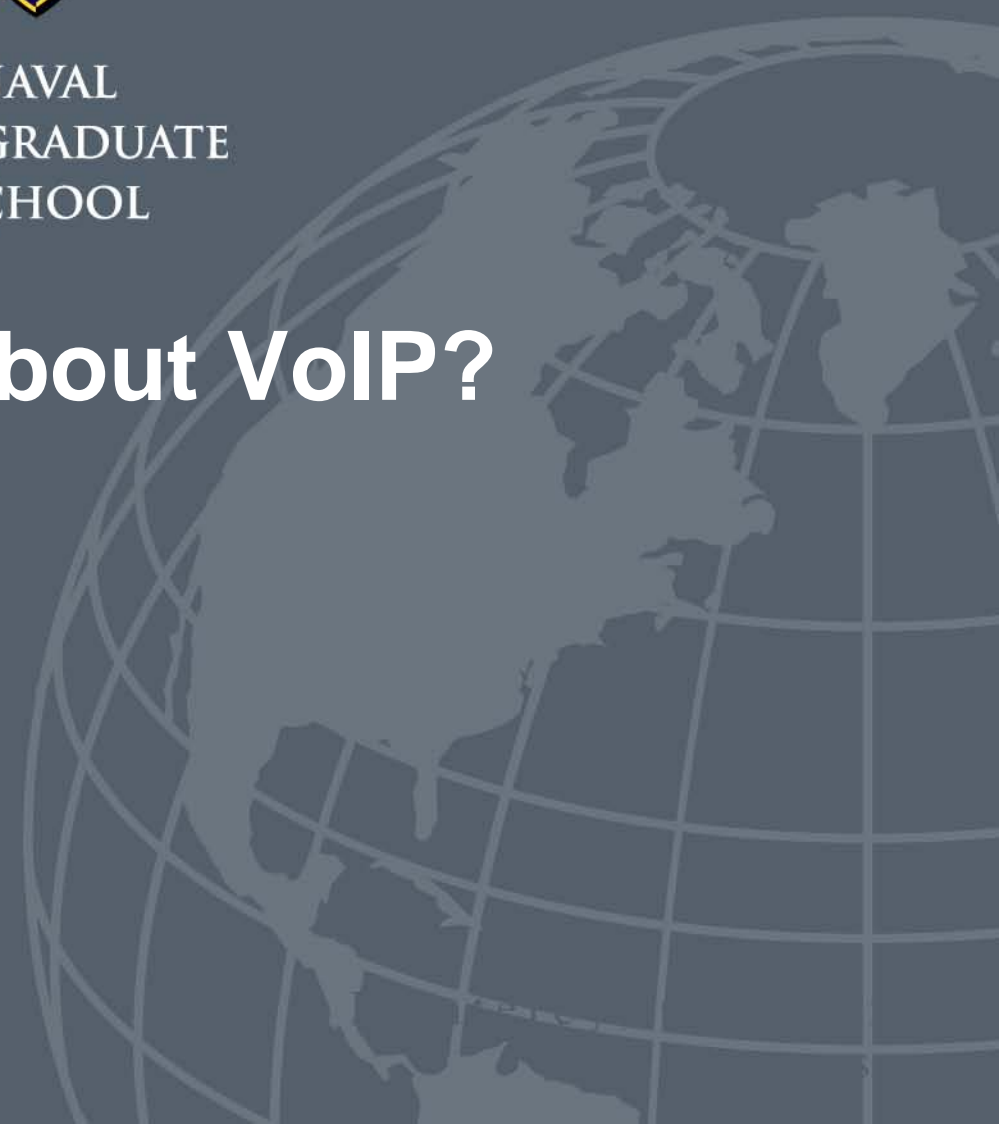


- Identified method for finding a WiMax user and keeping him off the network
- A wide variety of operational options
- Remaining research in implementation and integration



NAVAL  
POSTGRADUATE  
SCHOOL

**What about VoIP?**

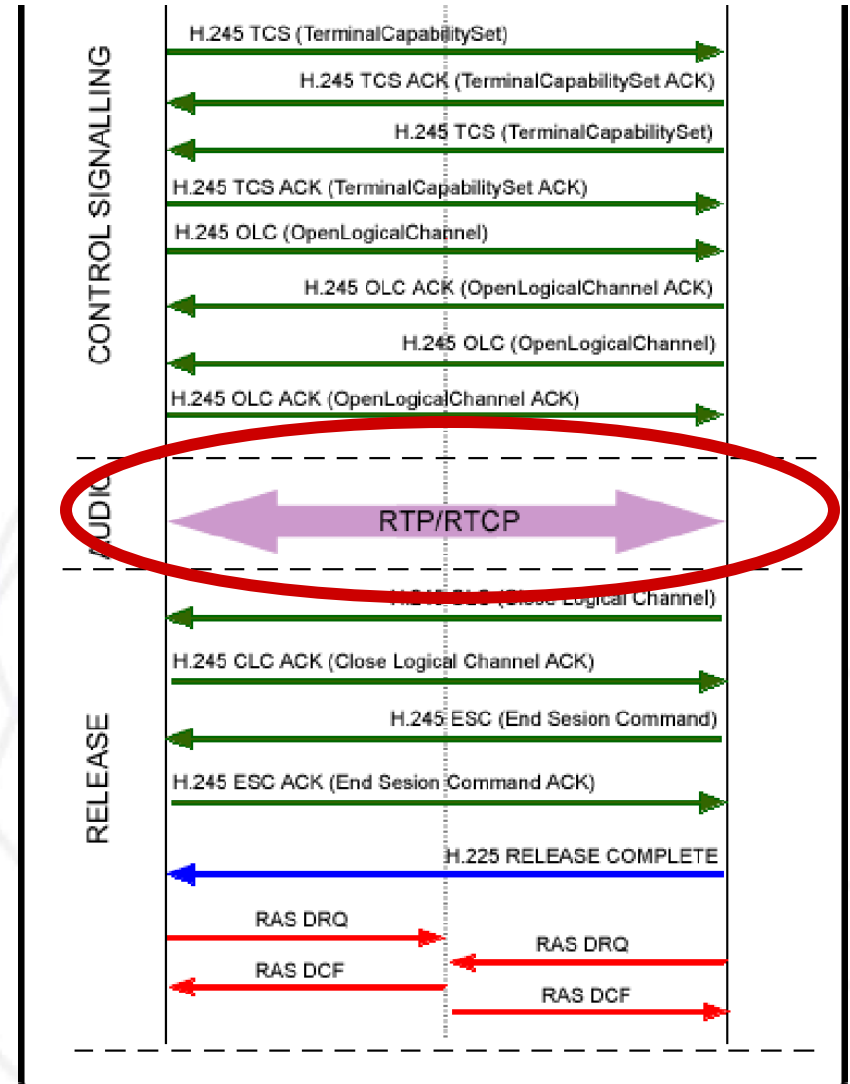
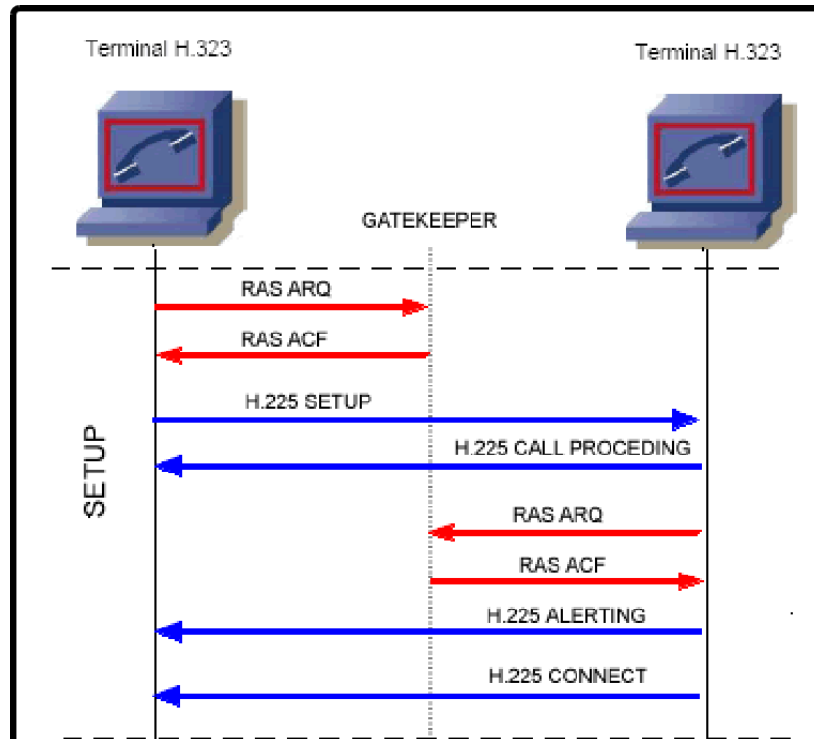


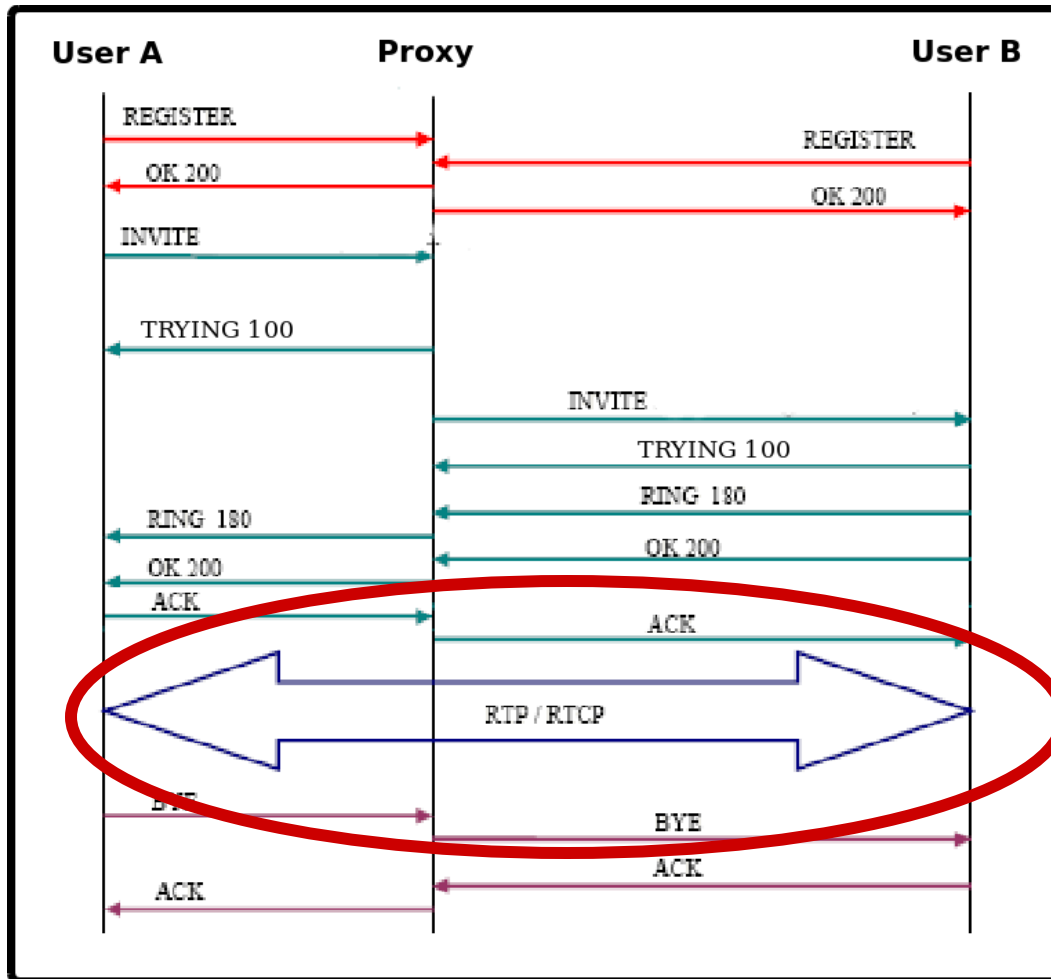


- 4G phones will use VoIP.
- With VoIP comes all of the security issues associated with TCP/IP networks
  - Moving from a highly controlled network (SS7) to a highly open network (Internet)
- Consequently, a myriad of attacks have been identified that are largely signaling standard-specific
  - H.323, SIP, MGCP, Skinny



**Is there anything common across  
all VoIP technologies?**







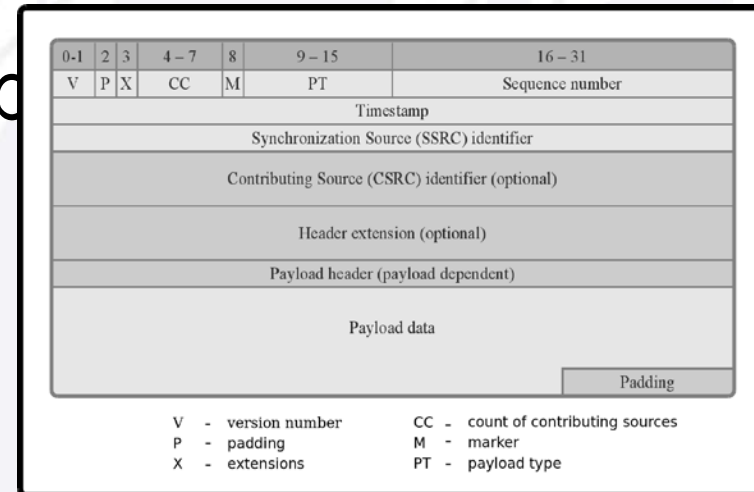
All VoIP Technologies use  
RTP for media transport

# RTP Packet Manipulation

- Substitute Payload
  - No checksum
- Vary RTP sequence number
  - No replay prevention
- Vary Timestamp
  - No replay prevention
- Signaling Protocol does not matter

bits	0 - 15	16 - 31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

(UDP checksum is only on header)





# What does varying the sequence number do?

- The sequence number indicates the order in which samples of voice were transmitted
- The receiver will discard any packets with sequence numbers older (less) than the last one received
- Attack vector: *Sending spoofed content with sequence numbers greater than the legitimate content will cause the spoofed content to be heard and the legitimate content ignored*

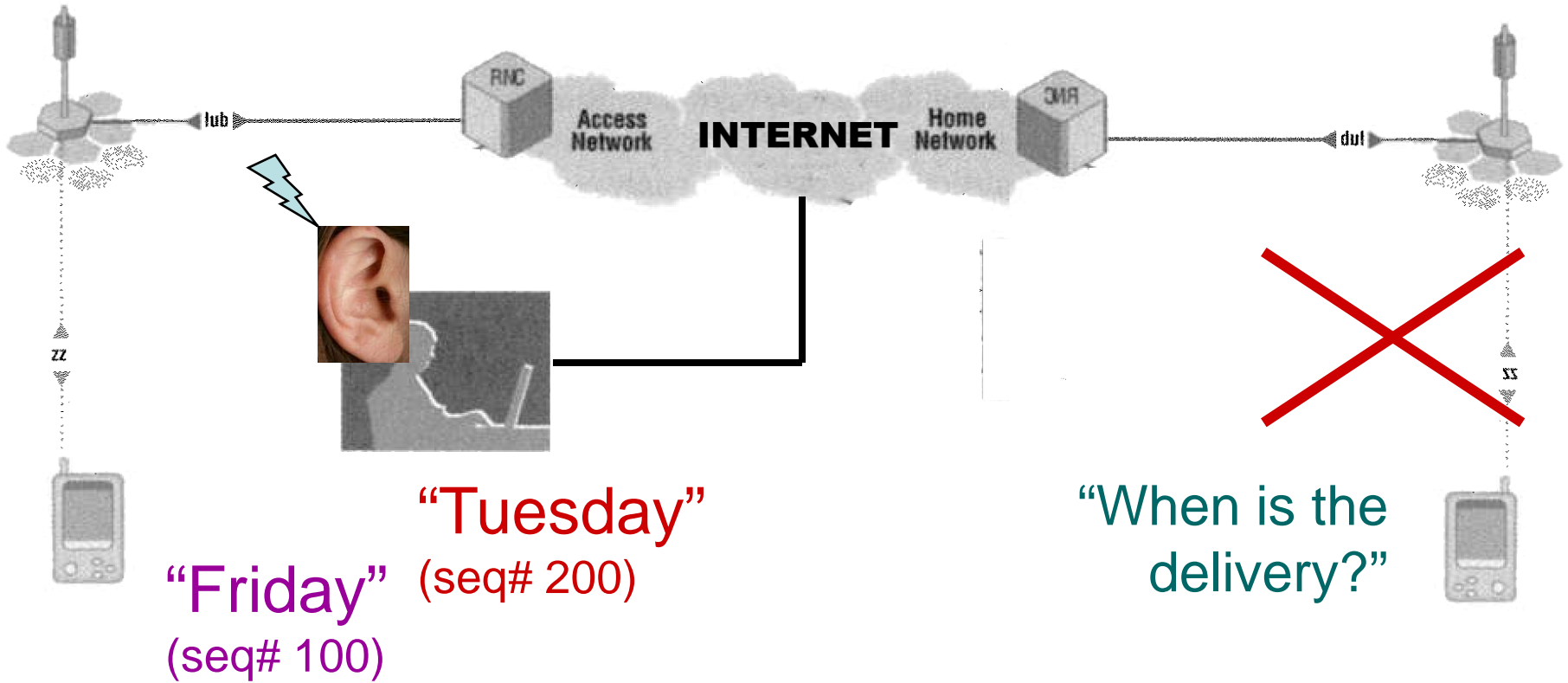


What does this mean in terms of 4G phones?

Inserting packets into a synchronous  
4G link is extremely difficult

Does the attacker need to insert  
the spoofed content into the 4G link though?

# Content Insertion Scenario





- Trend is for increasing reliance on our mobile device
- Legacy mobile standards have significant security issues
- Identified some issues with 4G standards
- Additionally, reliance on VoIP in 4G standards introduces a entirely new domain of vulnerabilities



# QUESTIONS?