# Mobile Security

## 14-829 – Fall 2013

Patrick Tague

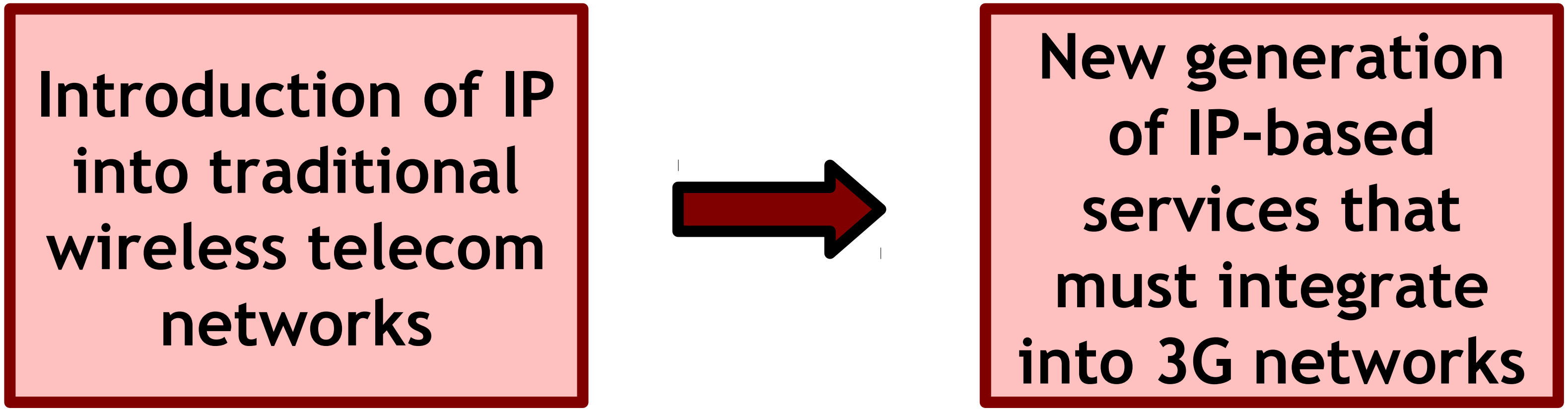
Class #4 – Telecom System Security

Carnegie Mellon University
Silicon Valley

# General Vulnerabilities

- Service interruption vulnerabilities
  - Due to increased capacity offered by high speed communication technologies
- Natural threats
  - Severe damage resulting from climatic, geological, or seismic events
- Handset vulnerabilities
  - Limited security features: more weaknesses
- Radio link protection-only vulnerabilities
  - Weak point in message transmission (lack of end-to-end security)
- Application-based (content-based) threats

# Cross Network Services



Introduction of IP into traditional wireless telecom networks

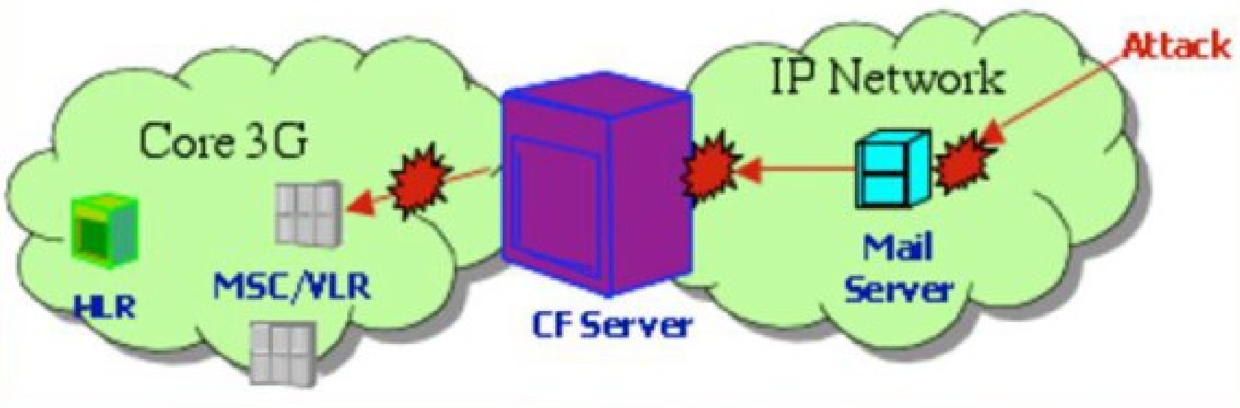
New generation of IP-based services that must integrate into 3G networks

Cross-Network Services

**Combination of Internet-based data and wireless telecom network data to provide enhanced services to the subscriber**

New Threats

# Cross Network Vulnerabilities



Example: Attack in a Call Forwarding Service where the attacker takes advantage of a breach in an IP network component to damage a 3G network component

# Specific Attacks in 2G/2.5G Systems

# DoS via Request Spoofing

- User de-registration request spoofing
  - Attacker de-registers a victim from the network, leaving them unreachable
- Location update request spoofing
  - Attacker updates a victim as registered in an incorrect location, routing messages to the wrong place, leaving them unreachable

# Compromised BTS

- Leveraging BTS capabilities
  - A victim connected to a compromised BTS can be forced to bypass encryption or to use a compromised encryption key
  - Attacker can play man-in-the-middle, eavesdropping on intercepted calls
  - Attacker with proper credentials of the victim can impersonate the victim

# Identity Catching

- Passive ID catching
  - GSM networks sometimes force users to send their identity in the clear
  - Passive eavesdropping can expose user's identity
- Active ID catching
  - Requires a compromised BTS
  - Attacker attracts the user to connect to the compromised BTS, then request identity in clear

# Attack Taxonomy for 3G Systems

[Kotapati, Liu, Sun, and LaPorta, 2005]

# 3G Attack Taxonomy I

- Dimension I: Based on the level of physical access to the network
  - Level 1: access the air interface w/ physical device
  - Level 2: access cables connecting 3G network switches
  - Level 3: access sensitive components of 3G network
  - Level 4: access links connecting the Internet and the 3G network core
  - Level 5: access Internet Servers or Cross-Network Services connected to 3G networks

# 3G Attack Taxonomy II

- Dimension II: Attack categories
  - Interception
  - Fabrication / replay
  - Modification of resources
  - Denial of service
  - Interruption

# 3G Attack Taxonomy III

- Dimension III: Attack means
  - Data-based attacks
  - Message-based attacks
  - Attacks based on service logic

# Specific Attacks in 3G Systems

# GTP Protocol and Attacks

- GTP is the GPRS IP communication protocol suite
  - (1) Creates and destroys user sessions, (2) Handles quality of service parameters, (3) Updates sessions for users in new locations, and more...
- Anomaly attacks:
  - Incorrect “message type” or “length” fields can cause memory exhaustion or buffer overflow
  - Recursive GTP encapsulation can cause packet or session spoofing
- Resource starvation:
  - Packet data protocol (PDP) Create Context flood, similar to a TCP SYN flood

# Possible Attacks in 4G Systems

# 4G Challenges

- 4G requires an open, heterogeneous, all IP-based (IPv6) environment
- VoIP – all packet switched, no circuits
- Service providers must share resources
- Interoperability
- Multicarrier
- Better QoS requirements

# Attacks in 4G

- Eavesdropping possible in unencrypted SIP
- Any attacks possible in the Internet (DoS, spam, spoofing, etc.) are possible in 4G
  - And many more will likely emerge and evolve
  - Yet to be seen if openness will help
- Forged billing (replay, MitM attacks)
- Tracking (e.g., statistical traffic analysis like in SIP protocols)

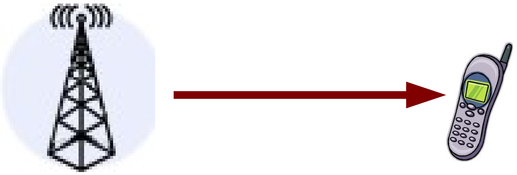
# Enabling Attacks

- What make so many attacks possible?
  - Availability of off-the-shelf mobile testing equipment
  - Integration of the Internet into mobile services and networks
    - Internet is open and easily manipulated
    - Increases the attack surface of mobile networks
  - Protocol weaknesses

# SMS, Packet Data, and DoS

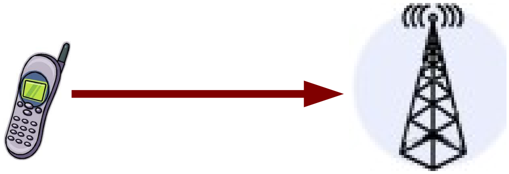
# Short Messaging Service

- Original SMS standard (1985) outlined three types of functionality:
  - Short message mobile terminated



1992: 1st SMS message

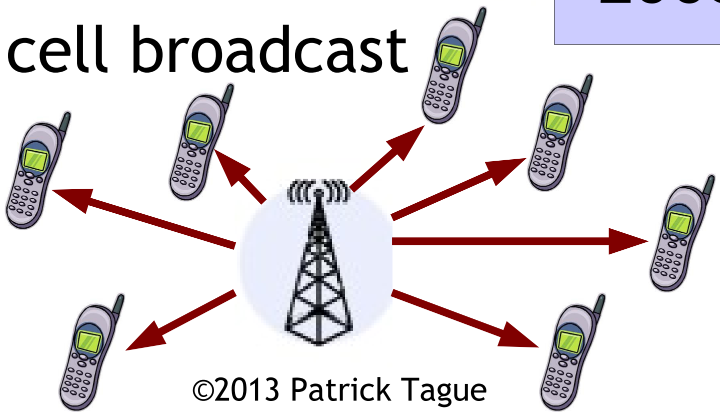
  - Short message mobile originated



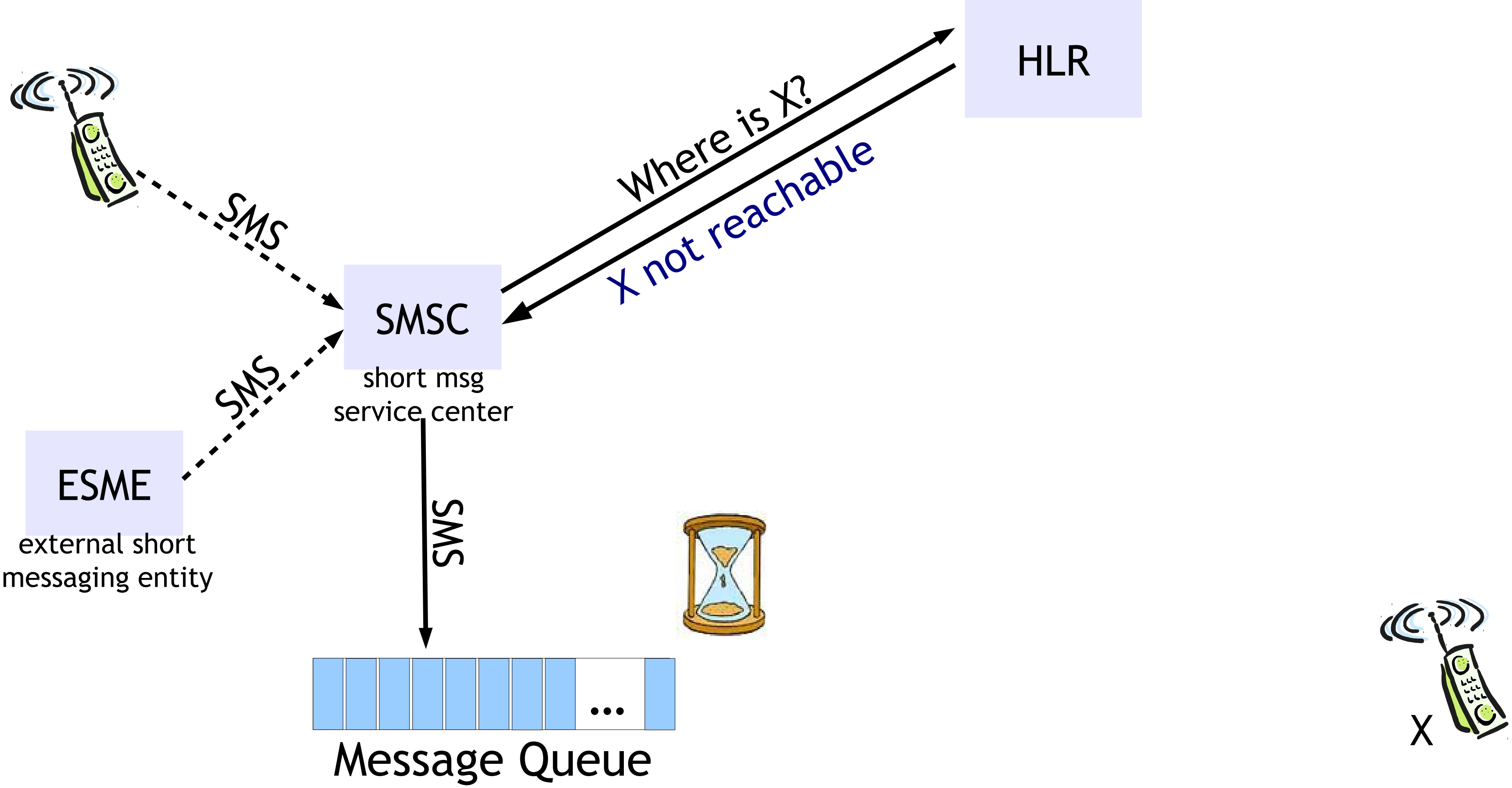
2000: 5x$10^9$ SMS/month

2005: $10^{12}$ SMS/month

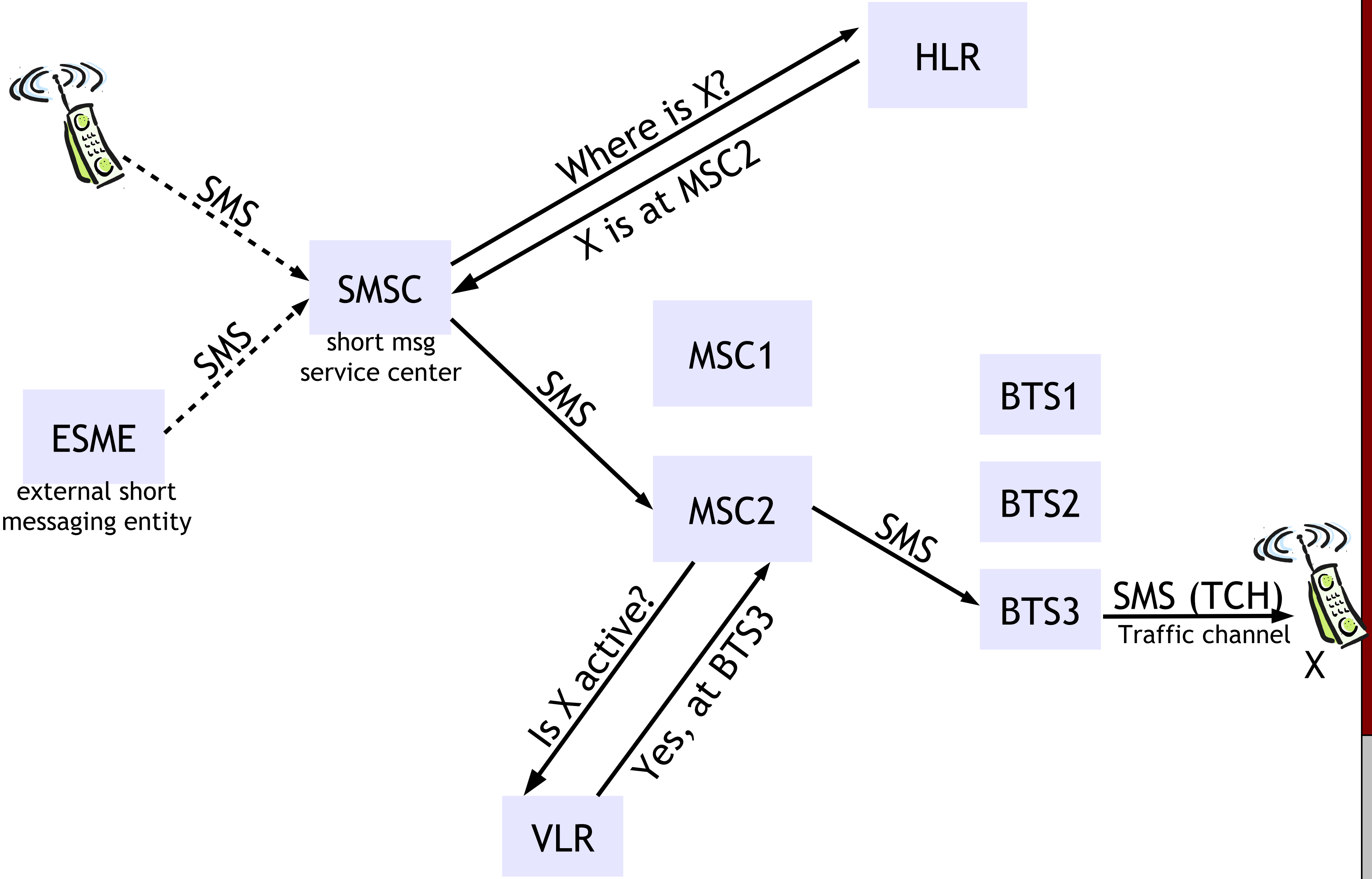
  - Short message cell broadcast



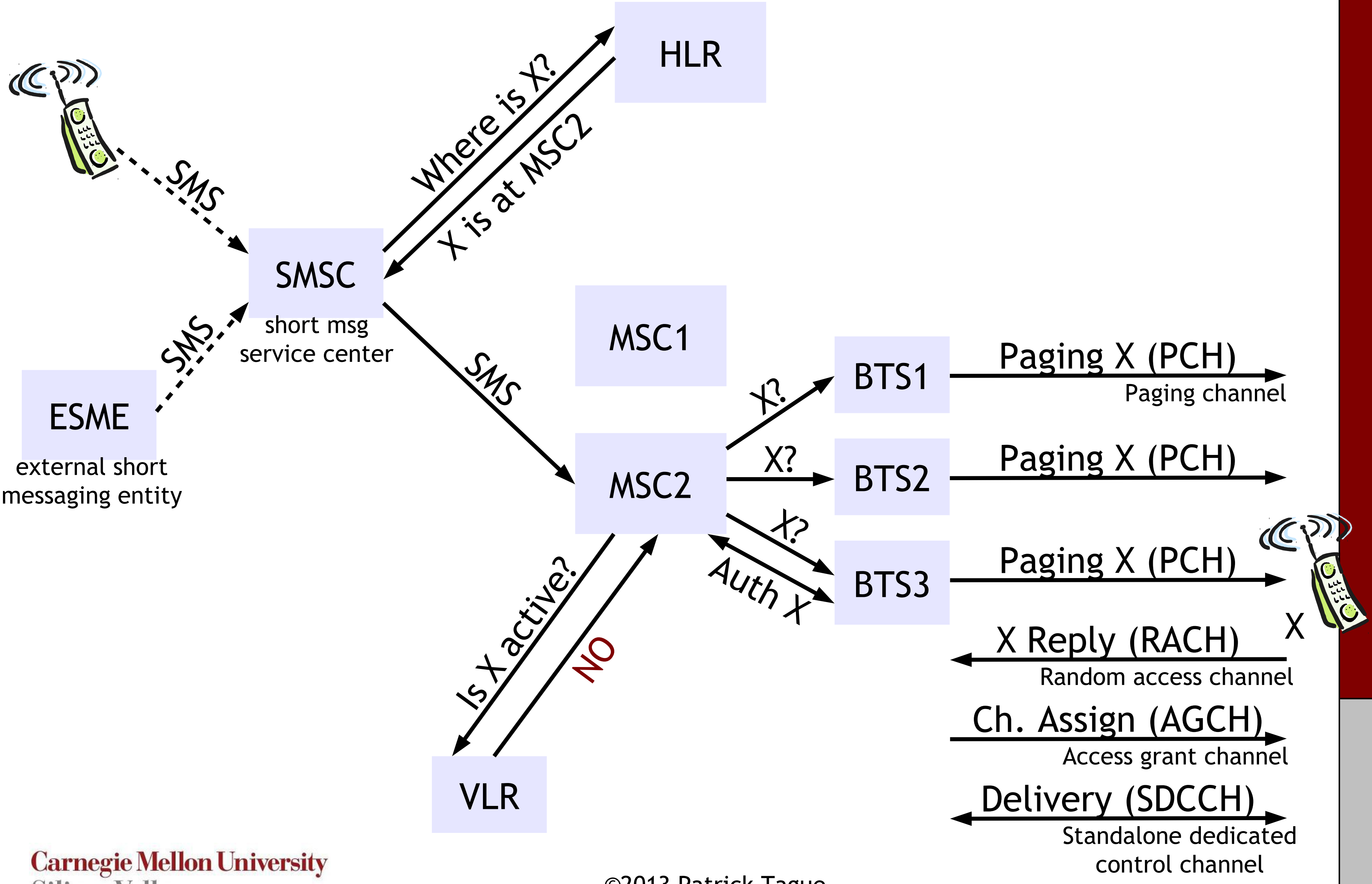
# Message Delivery



# Message Delivery



# Message Delivery



Carnegie Mellon University
Silicon Valley

# SMS Queuing

- At the SMSC:
  - Queues are finite
  - Messages can be lost
  - Dropping/overflow management varies by carrier
    - For details, see [Traynor et al., JSC 2008]

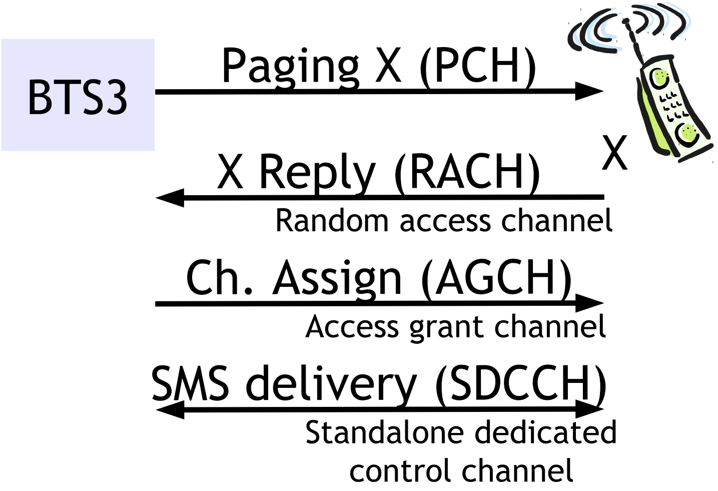
- At the MS:
  - Queues are finite, batteries are small
  - If MS queue is full, HLR tells SMSC it is unavailable
  - Batteries can be drained...

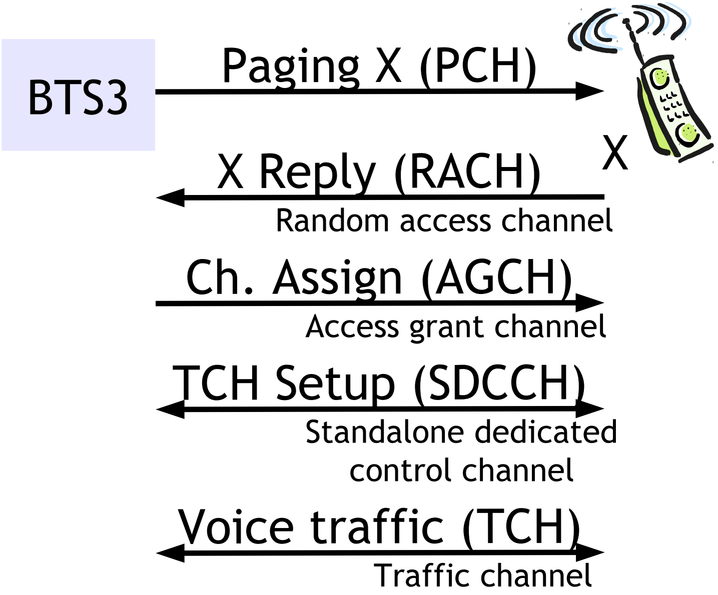
# Targeted SMS DoS

- Flooding a user with SMS messages:
  1. Buffer (@ MS or SMSC) overflow
     - With enough flooding, SMSC will drop valid messages
     - Some devices auto-delete previously read messages when they run out of storage
  2. Valid messages are delayed beyond useful lifetime
     - Ex: meeting reminders are useless after the meeting
  3. Valid messages are buried in the SMS flood

- Also a battery-depletion attack...

# Voice & SMS Sharing

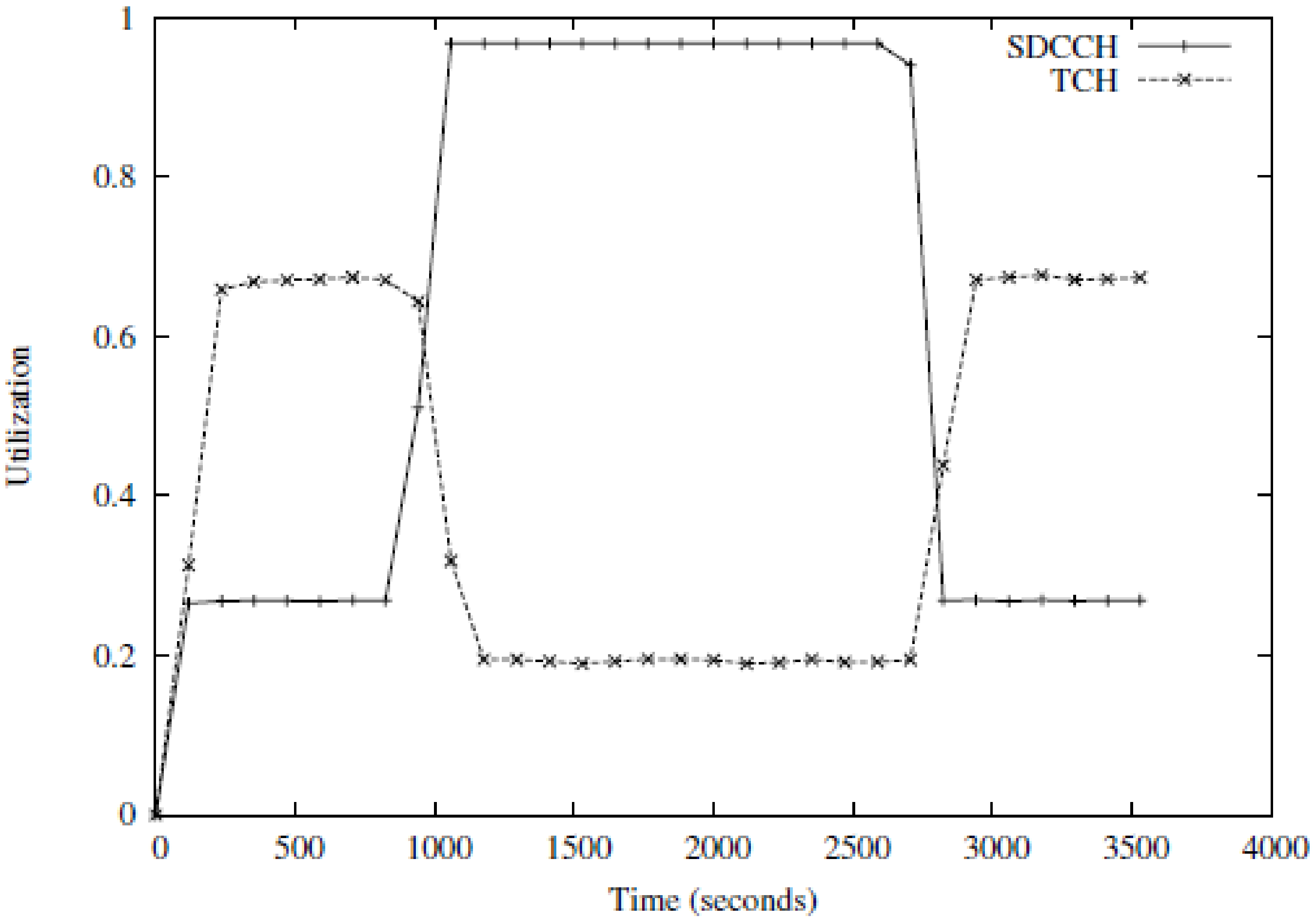




- Voice & SMS Resources
  - TCH is not used for SMS
  - Both SMS and voice init. use RACH, AGCH, and SDCCH

**SMS flooding also works as DoS against voice calls!**

# Voice & SMS Sharing



From [Traynor et al., “Security for Telecommunications Networks”, 2008]

# How to DoS a City...

- How much SMS traffic must be sent to saturate the SDCCHs in a large metro area?

SMS Capacity ~ (#Cell Towers) * (#Sectors/Tower)

* (#SDCCH/Sector) * (Capacity/SDCCH)

- Ex: Washington DC
  - 40 cell towers, 3 sectors/tower
  - Either 8, 12, or 24 SDCCH/Sector
  - Each SDCCH supports ~ 900 msgs/hour

SMS Capacity ~ 240 msgs/sec (for 8 SDCCH/sector) ~ 2.8 Mbps

# How to DDoS a Country...

- How much SMS traffic must be sent to saturate the SDCCHs in a large country?

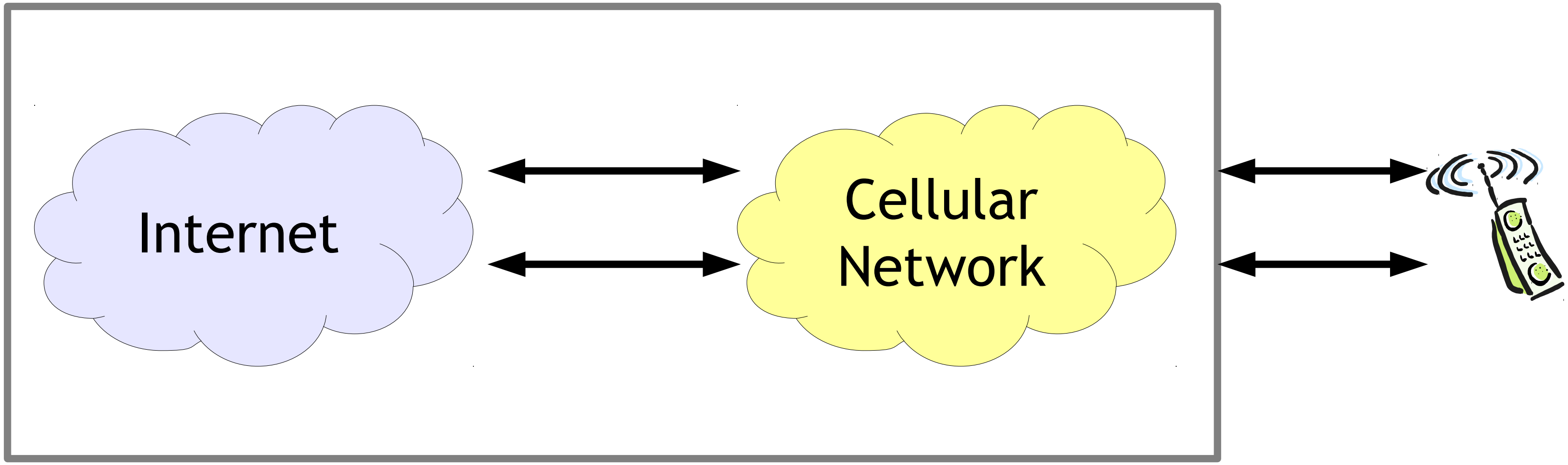
SMS Capacity ~ (Eff. Sector Density) * (Urban pop. Area)

* (#SDCCH/Sector) * (Capacity/SDCCH)

- Ex: USA
  - ~1.75 sectors / sq. mile
  - 8 SDCCH/Sector
  - Each SDCCH supports ~ 900 msgs/hour

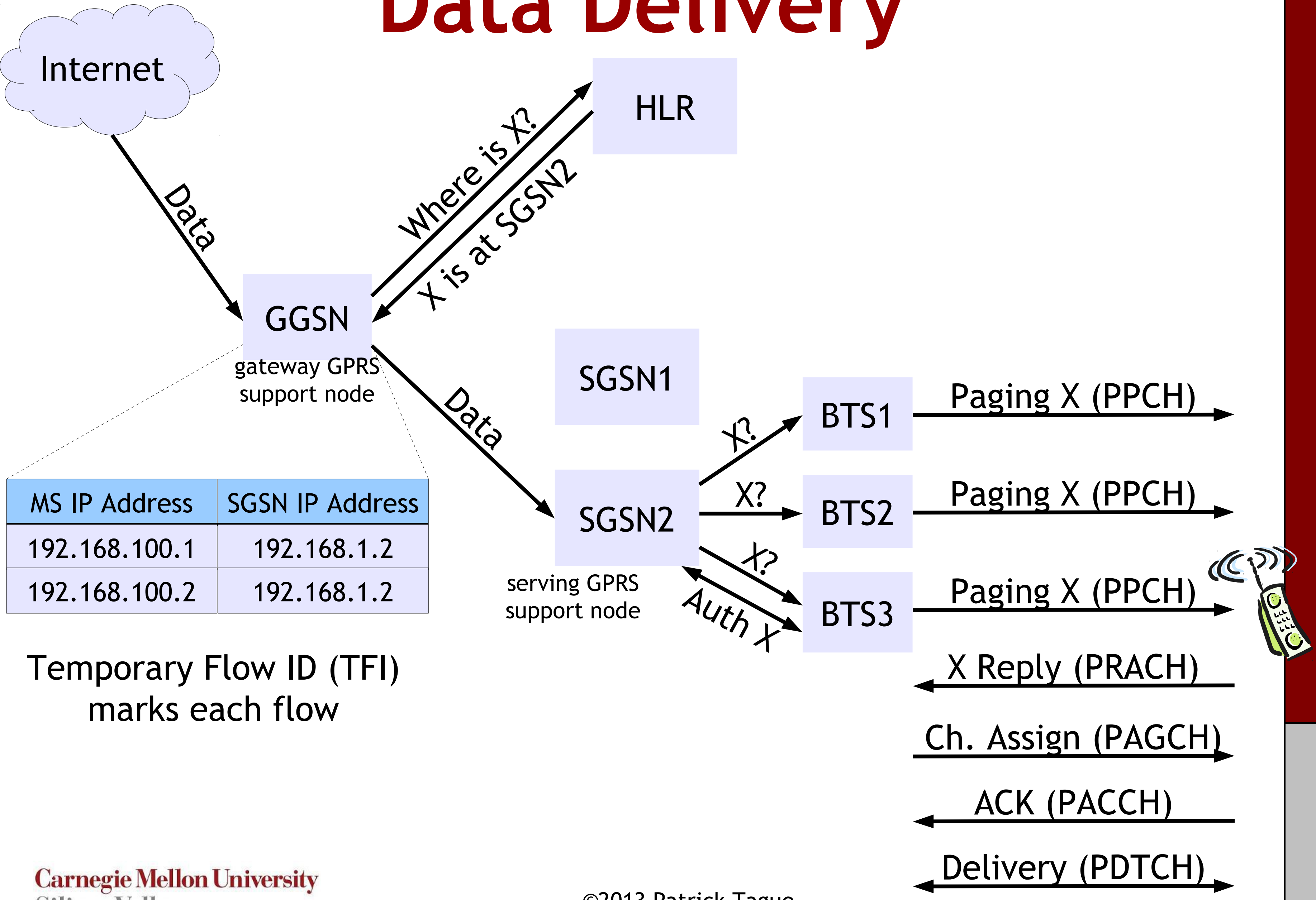
SMS Capacity ~ 325.5 Kmsgs/sec ~ 3.8 Gbps
Or ~ 380 Mbps for 10x multi-recipient messaging

# Cellular Data Service



- Cellular data service acts as a gateway to the Internet
  - Connecting to an “open” network through a “closed” network?

# Data Delivery



| MS IP Address | SGSN IP Address |
|---|---|
| 192.168.100.1 | 192.168.1.2 |
| 192.168.100.2 | 192.168.1.2 |

Temporary Flow ID (TFI)
marks each flow

Carnegie Mellon University
Silicon Valley

# Data-Based DoS Attacks

- Establishing a data connection is costly!
  - Timeouts are typically delayed to prevent frequent reallocation and reestablishment due to minor variation
  - Timers ~ 5 seconds
  - TFI field is 5 bits → If an adversary establishes 32 data sessions in a sector, DoS to everyone else!

$$\text{Capacity} \sim \frac{(\#\text{Sectors}) * (\#\text{Msgs/Sector}) * (\text{Bytes/Msg})}{\text{Timer duration}}$$

  - Ex: Washington DC: 120 sectors, 41 B/Msg → 252 kbps
    - Order of magnitude less work to deny data traffic compared to SMS DoS attack on voice

# Rogue Base Stations & MitM Attacks

Carnegie Mellon University
Silicon Valley

# Rogue BTS

- An adversary can deploy a rogue BTS that attempts to spoof the service provided by a valid BTS, attracting users for various reasons
- Possible to launch a MitM attack on 2G/3G mobile connections
- Applies to GPRS, EDGE, UMTS, and HSPA capable devices
- Cheap

# Lack of Authentication

- GPRS and EDGE use 2G GSM authentication
  - Devices are required to prove their identity to the BTS
  - BTS is NOT required to prove its identity to the device

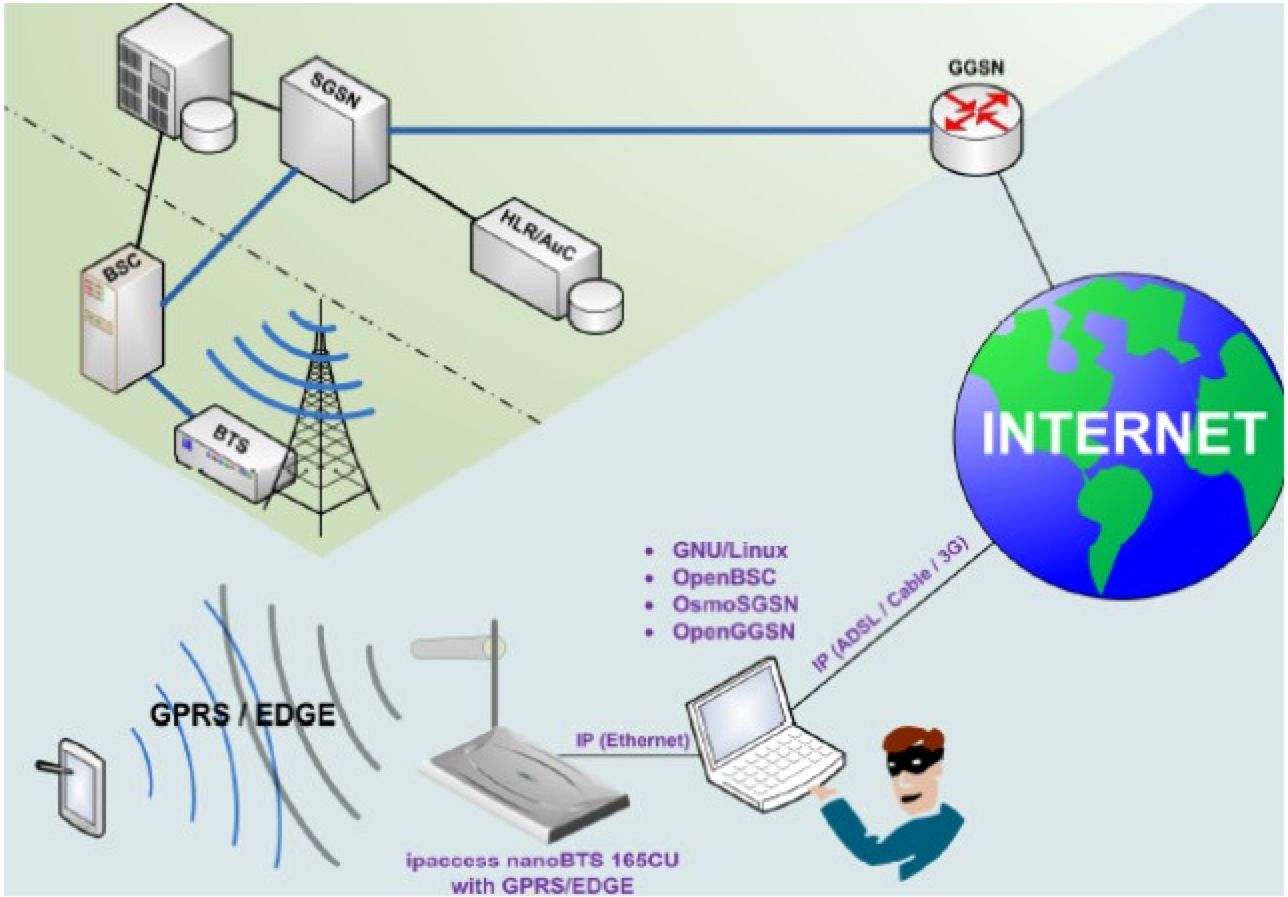
# Null Encryption Support

- GPRS / EDGE devices are required to support A5/0 null encryption (i.e., plaintext)
  - BTS can only offer to support null encryption
  - Most devices will accept the offer and send data in the clear

# Fallback Support

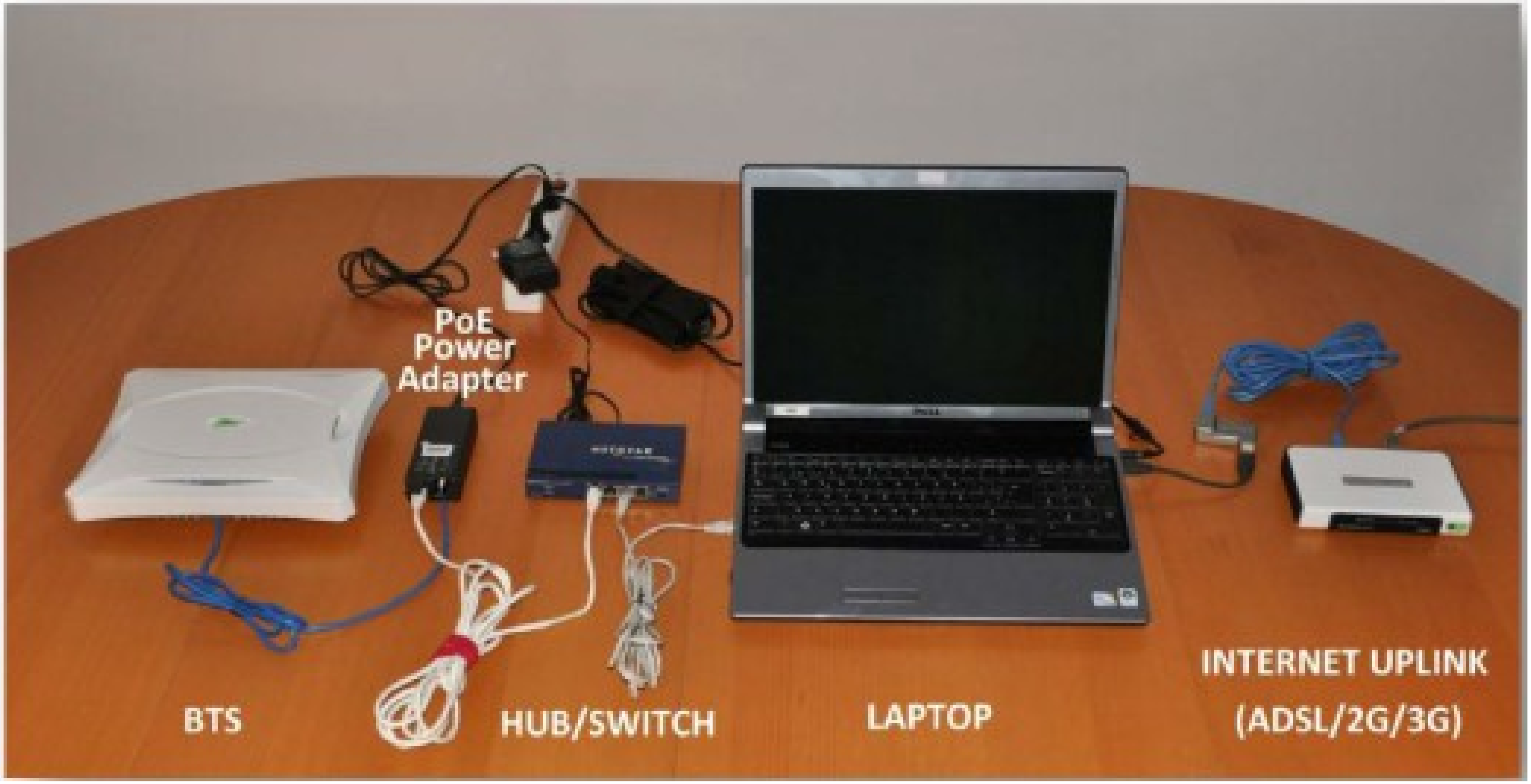
- Devices running UMTS/HSPA (3G/3.5G) are often configured to fall back to GPRS/EDGE if no UMTS/HSPA service is available
  - Sometimes occurs in network fringes, rural areas, etc.
  - Also, if someone is jamming the UMTS/HSPA frequencies or certain channels

# MitM Attack



- Attacker positions BTS in range of the target
  - Range can be improved by using a high-gain directional antenna or amplifier

# Setting up a Rogue BTS



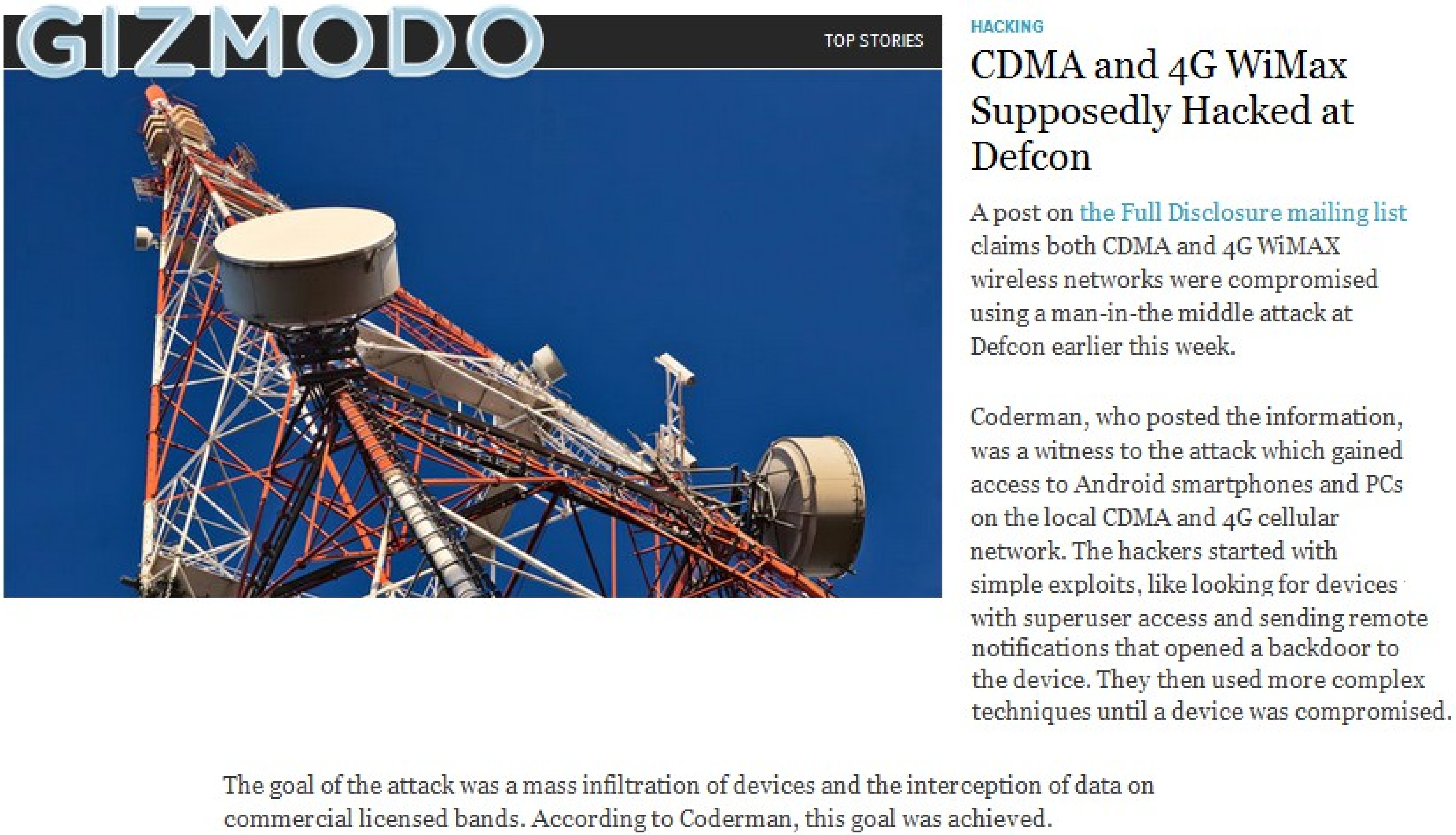
[Perez & Pico, BlackHat 2011]

# Defenses

- Major modifications would be needed to make GSM/GPRS/EDGE secure against rogue BTS
- Higher level protections can be used to secure data against MitM attack
- UMTS/HSPA devices can be configured to not fall back to 2G/2.5G

- 4G to the rescue?

# “4G” Not to the Rescue



HACKING

## CDMA and 4G WiMax Supposedly Hacked at Defcon

A post on the Full Disclosure mailing list claims both CDMA and 4G WiMAX wireless networks were compromised using a man-in-the middle attack at Defcon earlier this week.

Coderman, who posted the information, was a witness to the attack which gained access to Android smartphones and PCs on the local CDMA and 4G cellular network. The hackers started with simple exploits, like looking for devices with superuser access and sending remote notifications that opened a backdoor to the device. They then used more complex techniques until a device was compromised.

The goal of the attack was a mass infiltration of devices and the interception of data on commercial licensed bands. According to Coderman, this goal was achieved.

# Sept 11:
WiFi Security Basics

Carnegie Mellon University
Silicon Valley