Mobile Security
Fall 2015

Patrick Tague

#4: Telecom System Security Issues

Class #4

- Finish up our telecom security history lesson
- Interesting effects of telecom evolution
  - Analysis of SMS subsystem and interesting attacks
  - Rogue base stations and MitM attacks
- Discussion of first few project deliverables

Re-Design in 3G

- 3G security model builds on GSM
- Protection against active attacks
  - Integrity mechanisms to protect critical signaling
  - Enhanced (mutual) authentication w/ key freshness
- Enhanced encryption
  - Stronger (public) algorithm, longer keys
  - Encryption deeper into the network
- Core security – signaling protection
- Potential for secure global roaming (3GPP auth)

Enhanced Auth. & Keying

SIM

MS

MSC VLR

HLR AUC

Authentication Request

RAND

K

SQNhe

3G Auth Suite

XRES CK IK AUTN

{RAND, XRES, CK, IK, AUTN}

{RAND, AUTN}

RAND

K

AUTN

SQNms

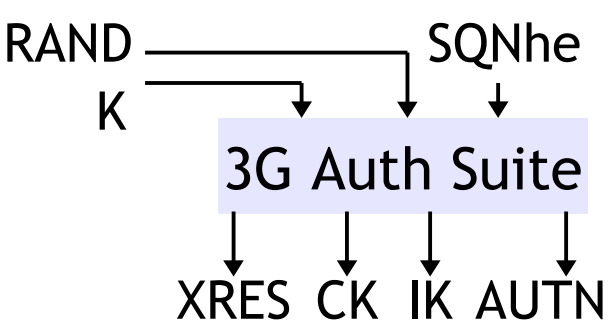
3G Auth Suite

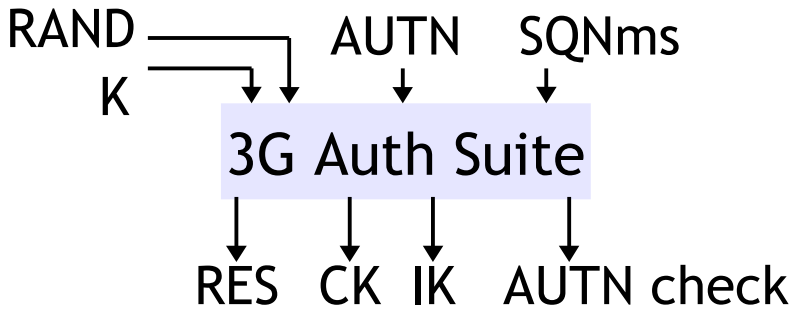
RES CK IK AUTN check

RES, Auth FAIL, or SQN FAIL

RES = XRES ?

Enhanced Auth. & Keying





3G Auth Suite = { F1 , F2 , F3 , F4 , F5 , ... }

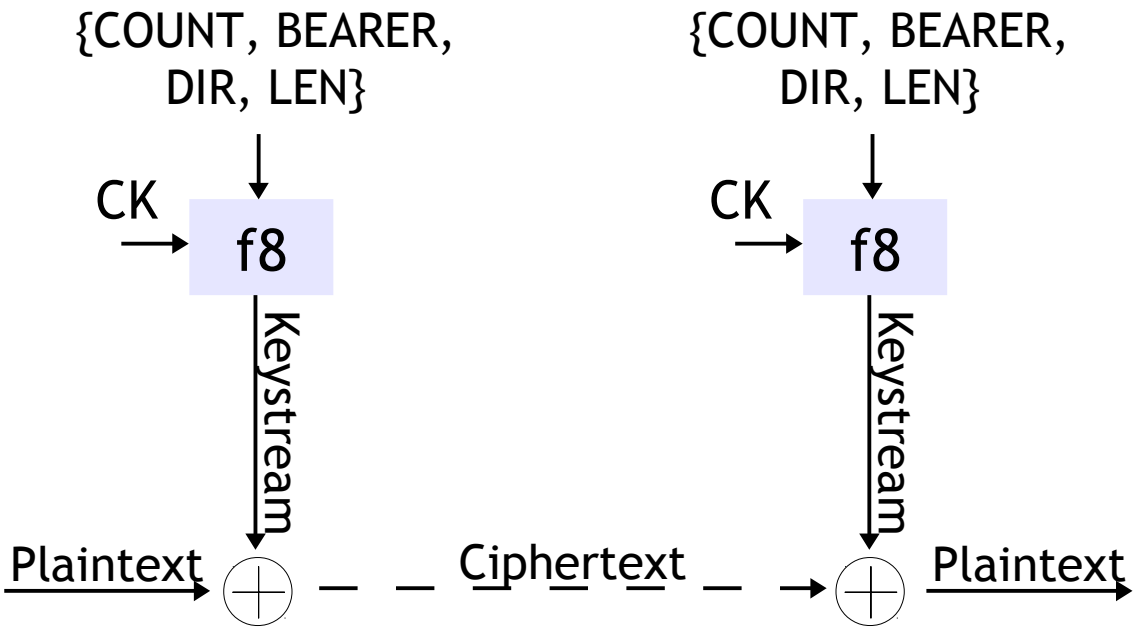
$XMAC = F1_K(RAND \mid SQN \mid AMF)$
$XRES = F2_K(RAND)$
$CK = F3_K(RAND)$
$IK = F4_K(RAND)$
$AK = F5_K(RAND)$

AUTN = SQN [xor AK] | AMF | XMAC
SQN > SQNhe

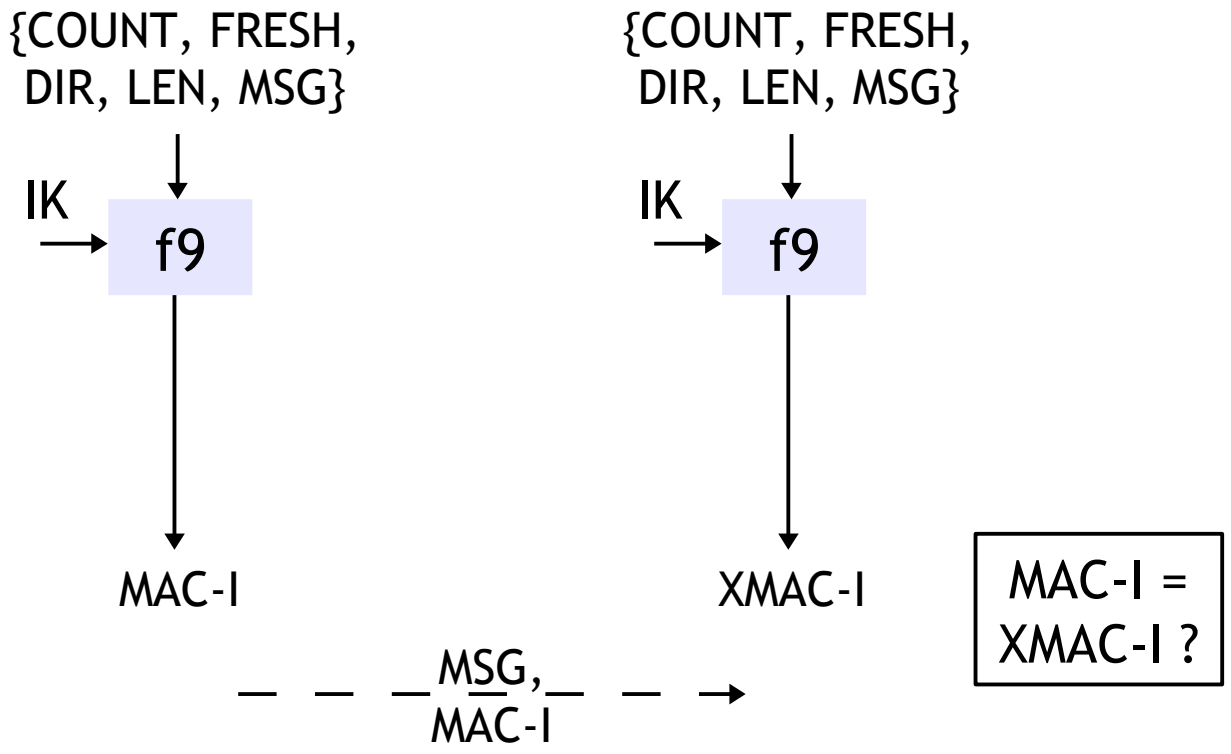
$MAC = F1_K(RAND \mid SQN \mid AMF)$
$RES = F2_K(RAND)$
$CK = F3_K(RAND)$
$IK = F4_K(RAND)$
$AK = F5_K(RAND)$

XMAC = MAC ?
SQN > SQNms ?

Enhanced Confidentiality



Enhanced Integrity



Algorithm Implementation

- KASUMI
  - Based on MISTY block cipher (Mitsubishi)
  - Two operational modes
    - f8 for encryption
    - f9 for integrity
  - Externally reviewed (positively)
  - Published
  - Broken
    - Dunkelman, Keller, and Shamir – January 2010
    - Interestingly, MISTY isn't affected by this technique...

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, III

- Dimension II: Attack categories
  - Interception
  - Fabrication / replay
  - Modification of resources
  - Denial of service
  - Interruption
- Dimension III: Attack means
  - Data-based attacks
  - Message-based attacks
  - Attacks based on service logic

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

From 3G to "4G" to 4G

- 4G represents the next generation in cellular communication
  - ITU-R standard: 1Gbps fixed, 100Mbps @ 100kph
  - WiMAX Release 2, LTE-Advanced
    - WiMAX and LTE are not really 4G, but "4G"
    - Verizon, Sprint, AT&T use LTE; T-Mobile, AT&T use HSPA+
    - Most provide ~20Mbps fixed
- "4G is a combination of marketing speak and future tech" [Warren, Mashable 02/2011]
  - Current "4G" systems are actually 3.75G or 3.9G, but they'll be upgraded to real 4G in the future

"It is difficult to quantify the security risks of 4G when it has yet to be developed, however it is essential that developers find a definable way to find a balance between practical applications and the necessary security levels involved with the network."

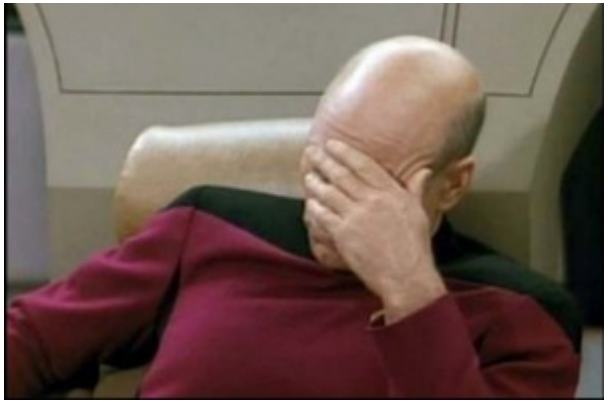
- Kevin Rio, Krio Media blog

Attacks on 4G Components

- 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)

Still in Use Today

- Nearly all of us are using protocols based on the 3G standard today
  - Many of those systems were upgraded from 2G and are still backward compatible (many voice calls are still handled by the 2G subsystems)
  - Security protocols known to be broken are still supported by most systems



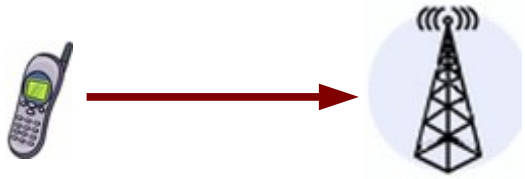
SMS, Packet Data, and DoS

Short Messaging Service

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

1992: 1st SMS message

  - Short message mobile originated



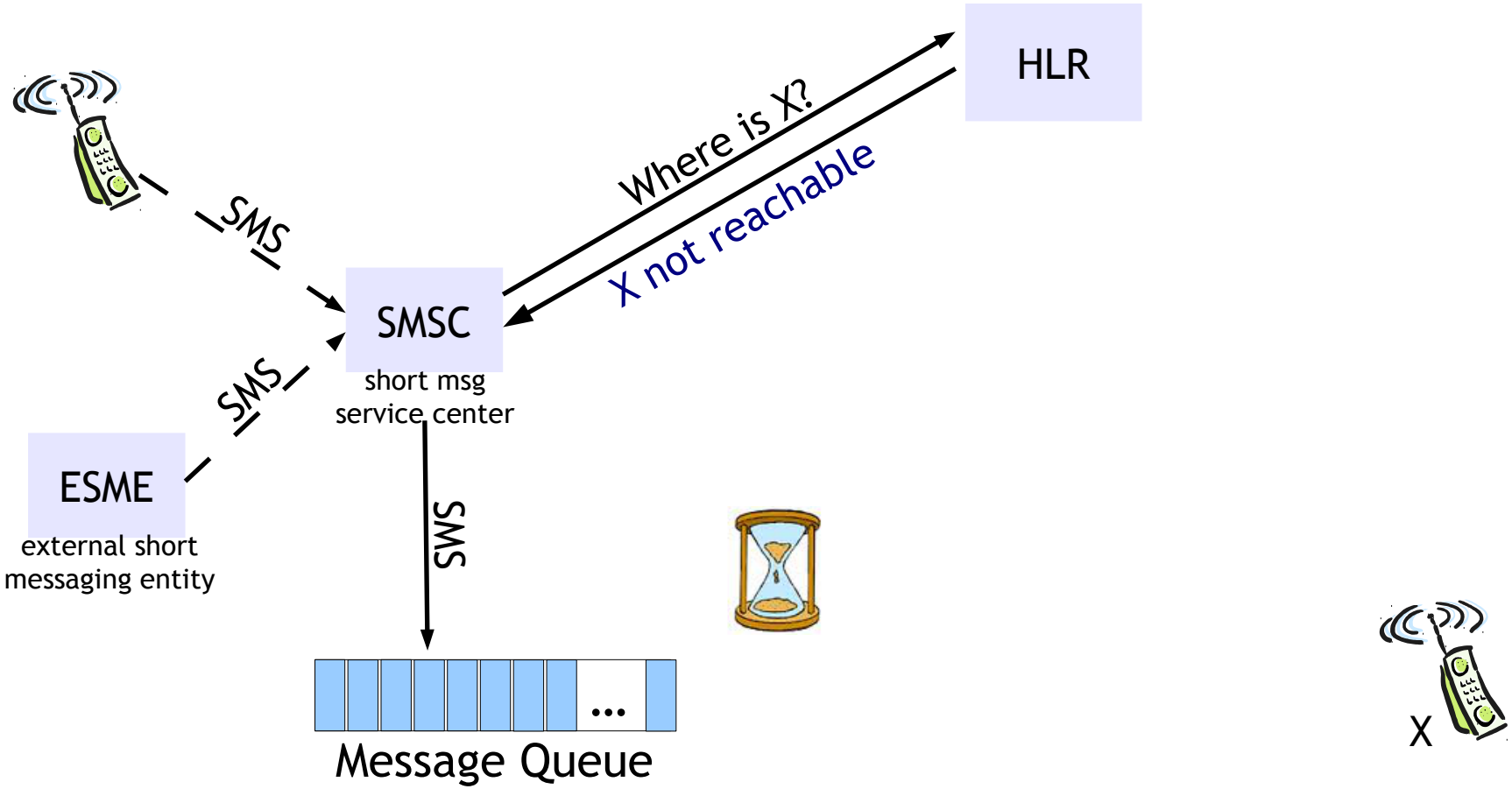
2000: 10^7 SMS/month

  - Short message cell broadcast

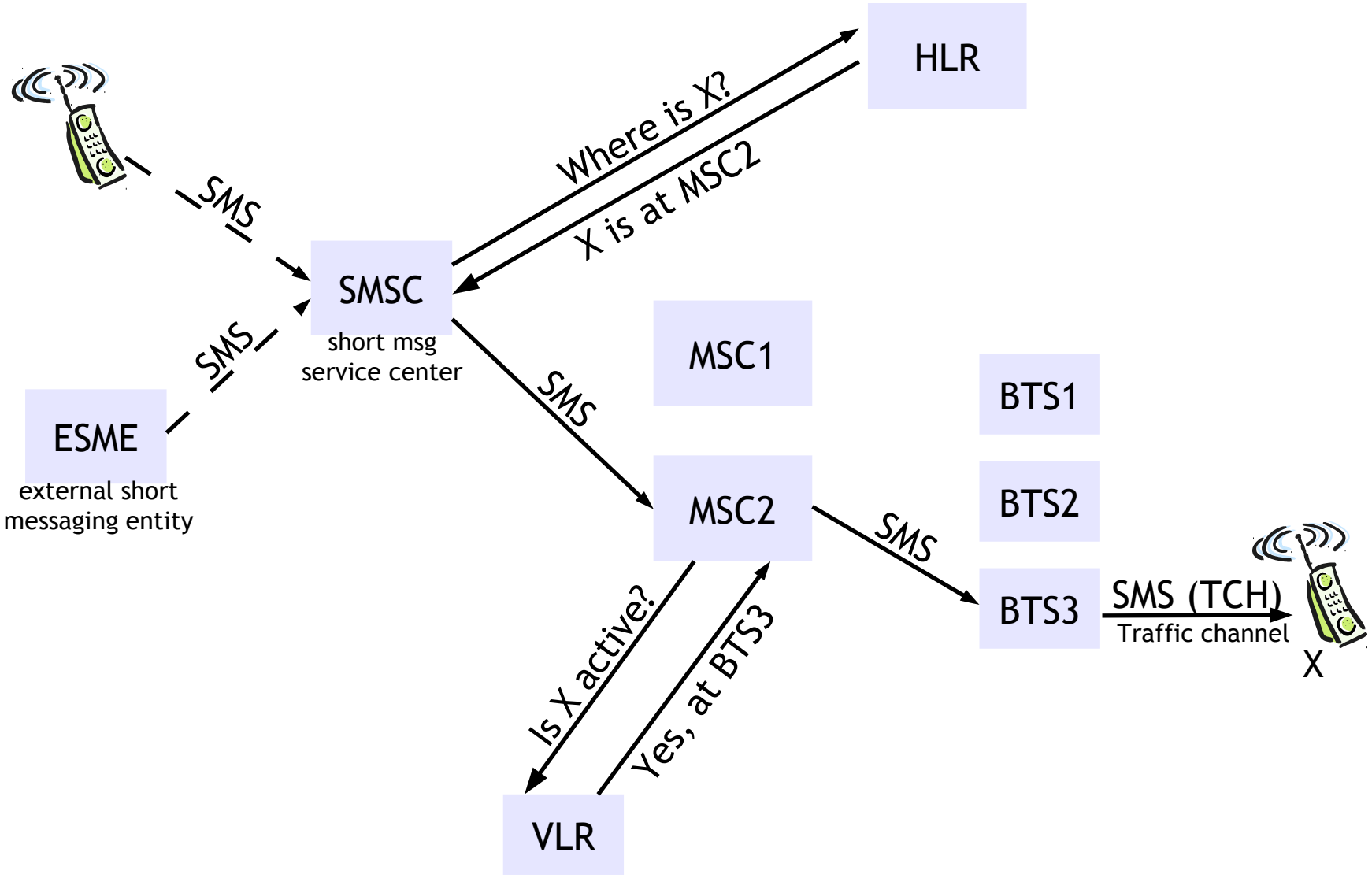
2006: 10^{10} SMS/month

2014: 5×10^{11} SMS/month

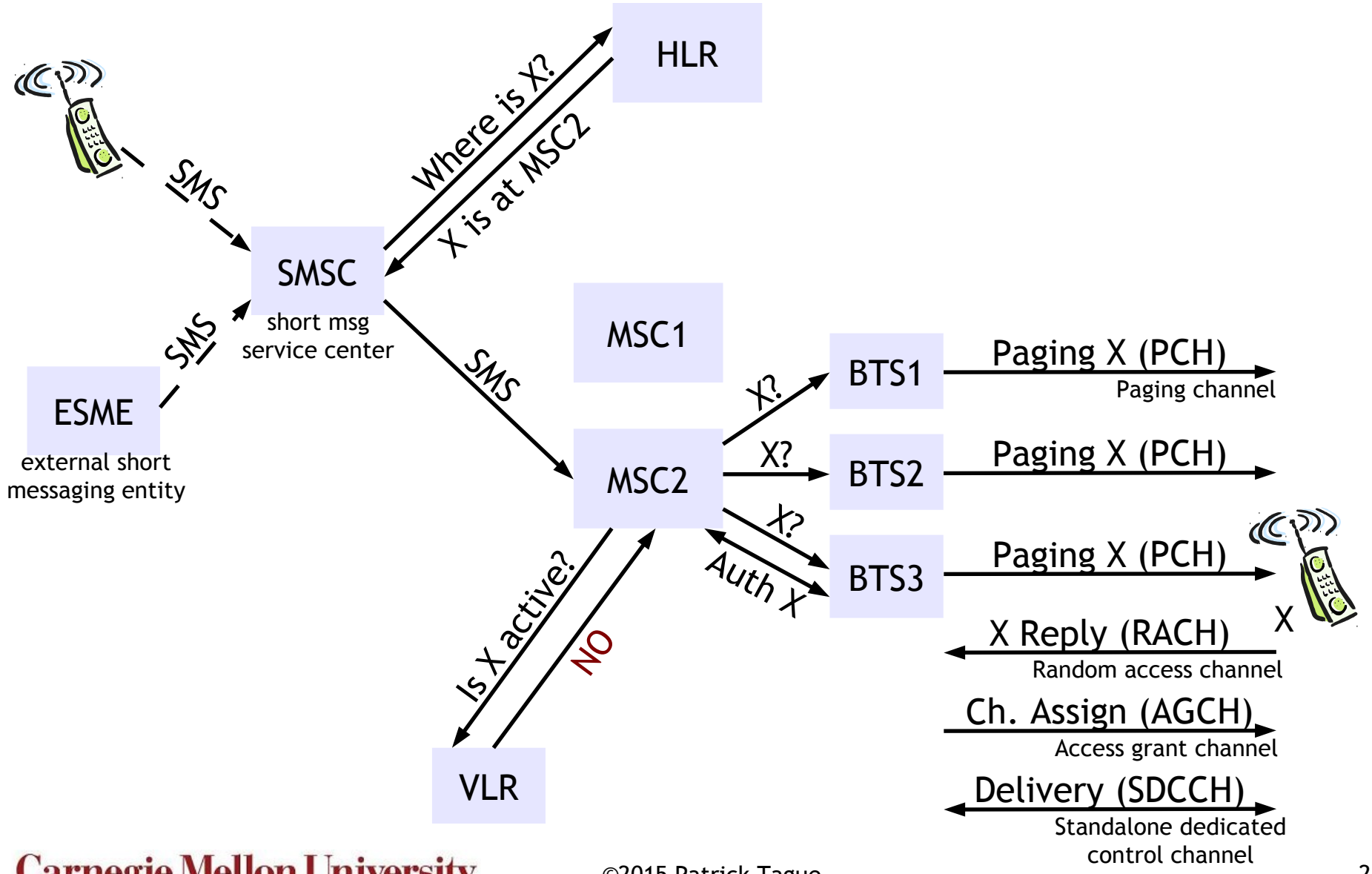
Message Delivery



Message Delivery



Message Delivery



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]

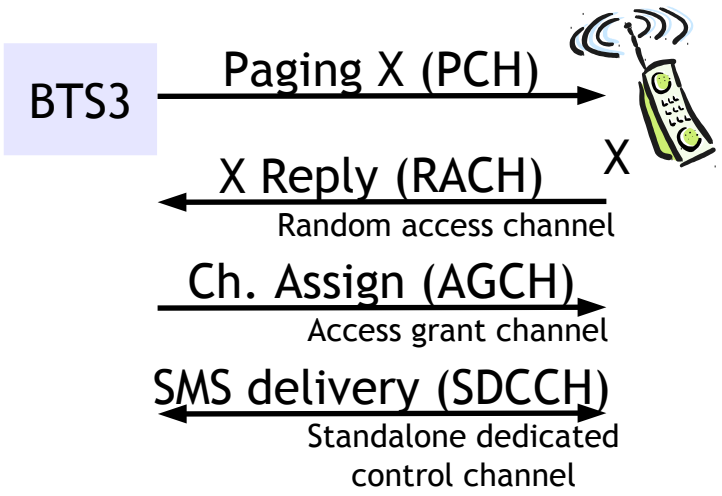
- At the MS:
  - Queues are finite, batteries are small
  - If MS queue is full, HLR tells SMSC it is unavailable
  - Batteries can be drained...

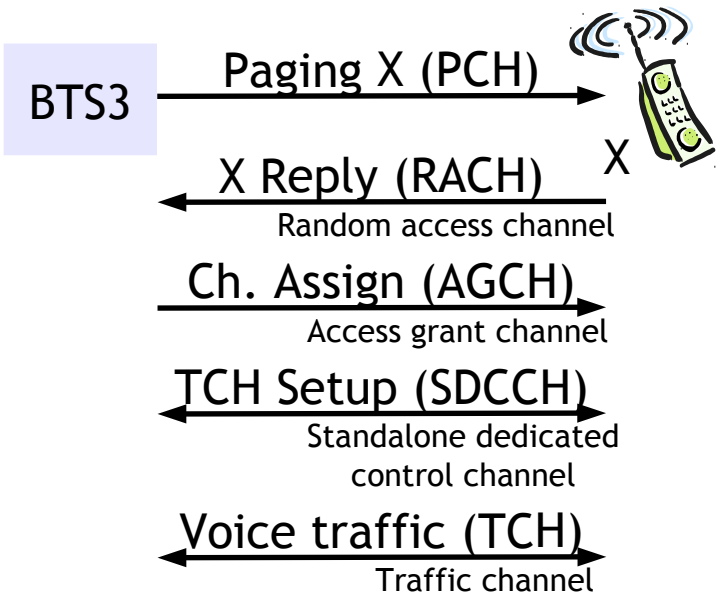
Targeted SMS DoS

- 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

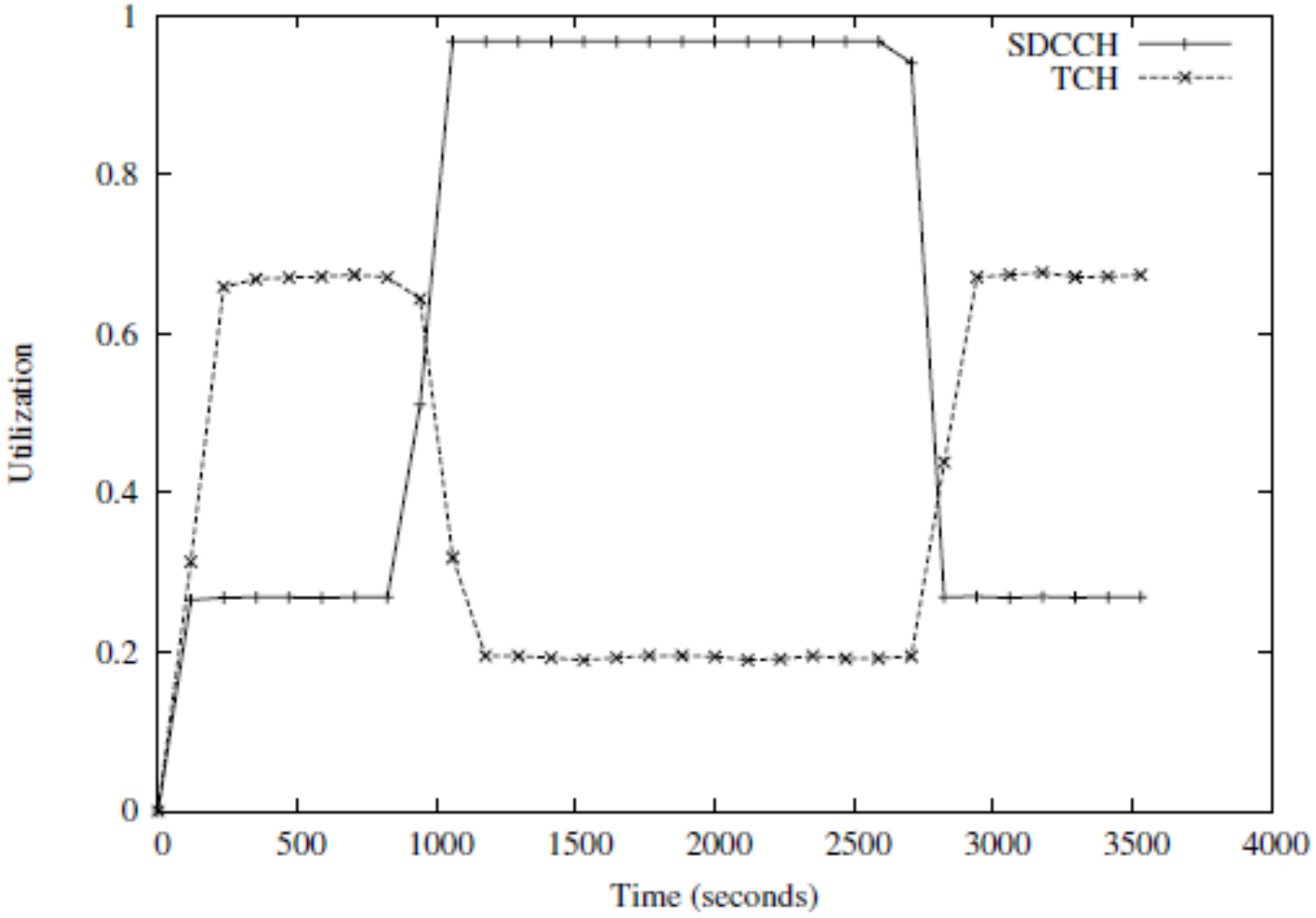




- Voice & SMS Resources
  - TCH is not used for SMS
  - Both SMS and voice init. use RACH, AGCH, and SDCCH

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?

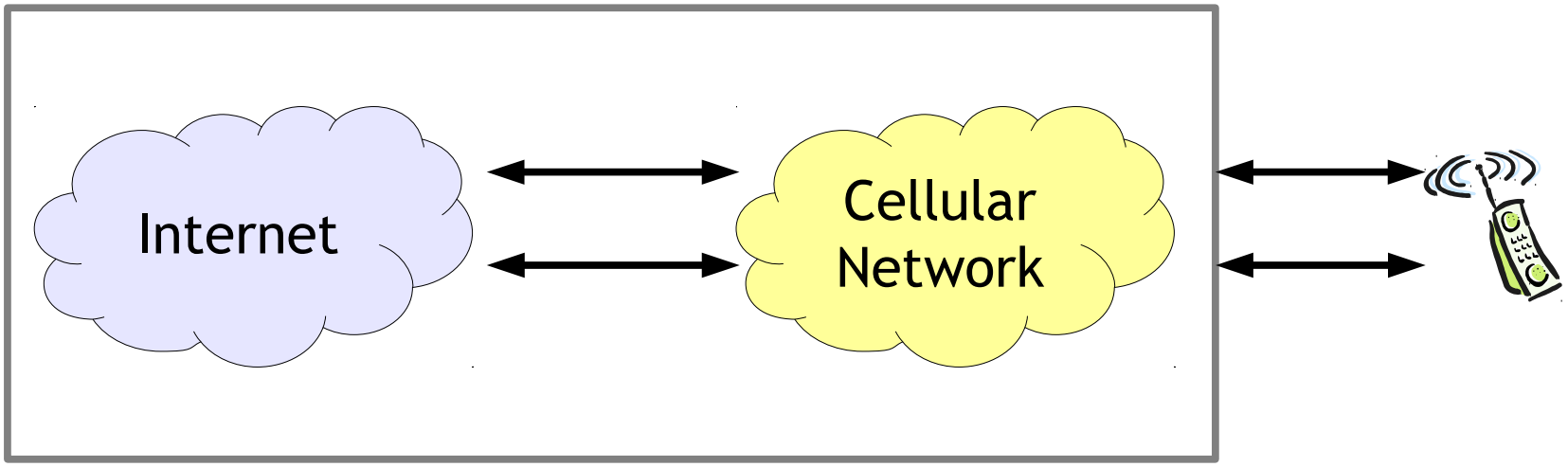
SMS Capacity ~ (#Cell Towers) * (#Sectors/Tower)

* (#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

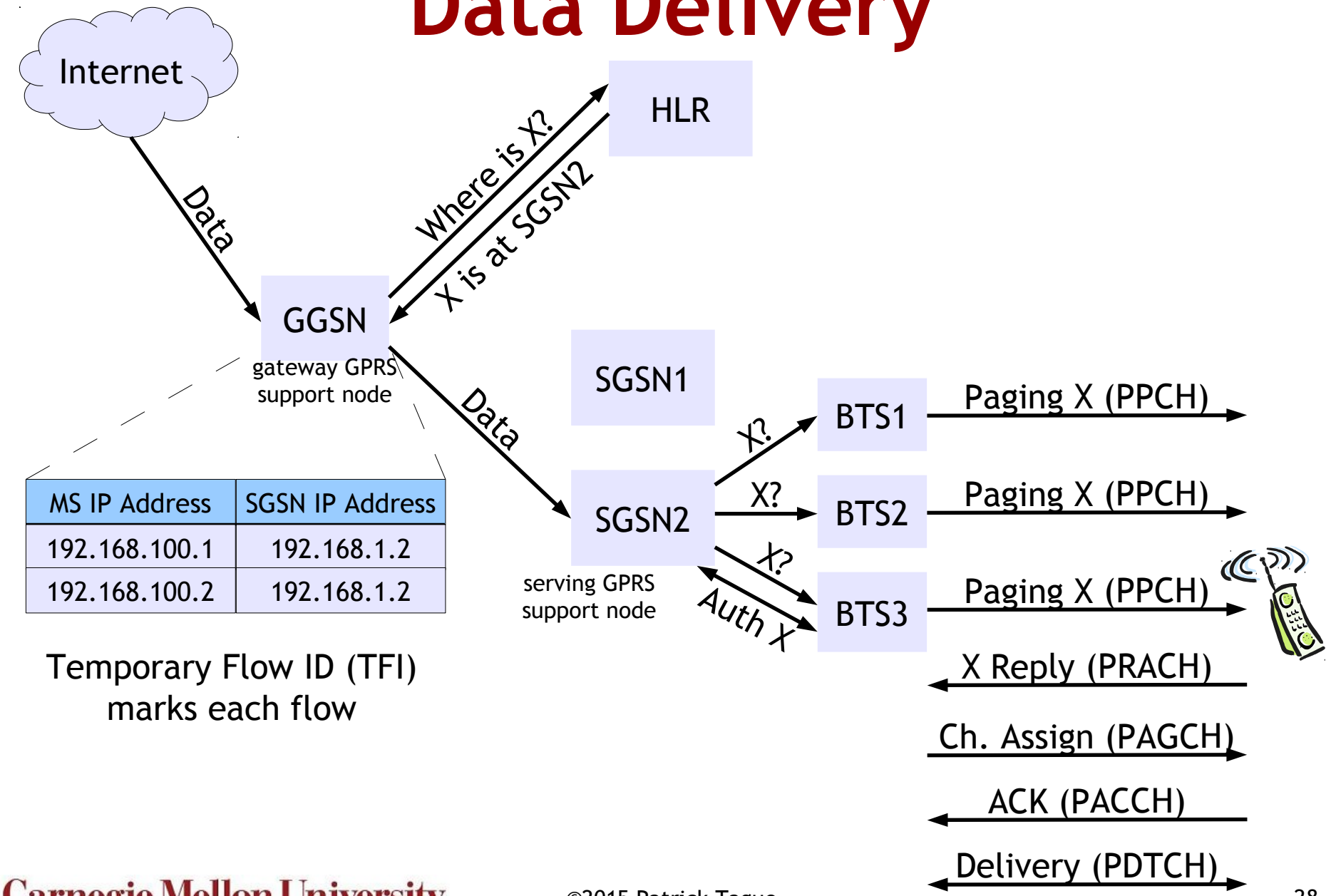
SMS Capacity ~ 240 msgs/sec (for 8 SDCCH/sector) ~ 2.8 Mbps

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

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

More about Projects

Project Goals

- The course project provides an opportunity to apply topics from class to an in-depth study of a specific topic area
  - Not just a broad survey of what has been done
  - A chance to do something novel and make a real contribution to advance the state of the art

- Experience with an end-to-end project
  - Ideation, hypothesis, experimentation, analysis, and presentation of process and results

Intro Presentation

- Presentation of project area, potential project topic, and background / related work
  - What is the broadly defined problem? Why is it interesting? What has been done so far? What questions have not yet been answered?
  - Presentation should include figures to illustrate the problem idea, approach, etc. in a straightforward way (i.e., not a lot of text)
  - Ideally, plan for 3-4 slides with a total duration around 10 minutes per team (including every team member)

Intro Template

Intro presentation template is available on Blackboard.

Project Title

Team Awesome
Jordan, Jon, Joey, Donnie, and Danny

Mobile Security, Fall 2015
Project Intro Presentation

Project Title

Team Awesome: Jordan, Jon, Joey, Donnie, and Danny

Full-slide figure – use the figure to describe your project area

Project Title

Team Awesome: Jordan, Jon, Joey, Donnie, and Danny

- Background work in this area
  - What previous work has been done that shapes the space?
  - What are the limitations of the previous work?
  - How are you hoping to extend upon or enhance what was done previously? *[not specifically what will you do, just ideas of what you could do]*
  - *Include references as appropriate*

Deliverable Grading

- Presentations:
  - Grade will be based on 1) whether you included everything that we asked you to include, 2) use of the time allotted, 3) balance of presenters across team, 4) clarity of presentation

- Reports:
  - Grade will be based on 1) clear presentation of project aspects, 2) inclusion of all necessary components, 3) use of figures, data, etc. as appropriate

Project Ideas

- We're posting various project ideas on Blackboard
- Any project posted there will have a “mentor” that you should contact about joining their team
- Have your own idea for a project? Please discuss with us before going forward

Sept 15:
Tutorial I: Android Tips & Tricks

Sept 17:
WiFi Security