Wireless Phone GSM tracking

Denis Foo Kune,

John Koelndorfer, Nick Hopper,
Yongdae Kim

UNIVERSITY OF MINNESOTA

Can someone track your phone?

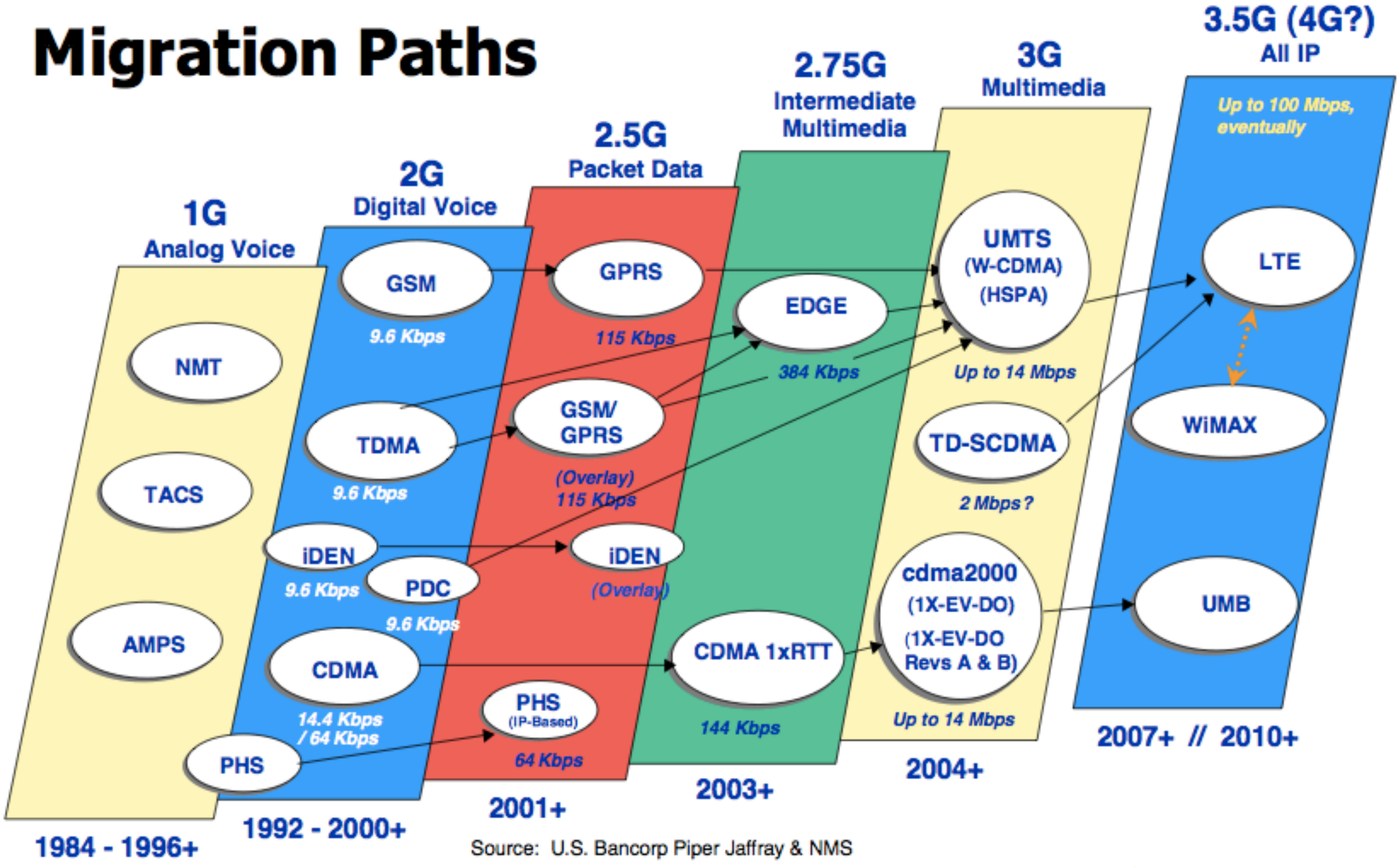
- GPS
  - Need access to phone
- Cell network trilateration/triangulation
  - Multiple base stations measure the RSSI for a phone
  - Estimate location from signal strength
  - Need access to service provider database
- WiFi
  - Trilateration works
  - A laptop can measure signal strength of broadcast messages
  - A commercially available WiFi card can listen to those messages
  - Need to know IEEE MAC address

What about the cell towers?

- Large array of towers broadcasting messages
  - Can those messages reveal a phone's location?
- Given a person's phone number
  - can we locate the tower they are attached to in a GSM network?
- No collaboration from the service provider.
- No support from apps.
- No GPS, trilateration or WiFi

- GSM: dominant protocol worldwide
  - Analysis of layer 2/3 messages only.

Cellular network timeline



Source: U.S. Bancorp Piper Jaffray & NMS

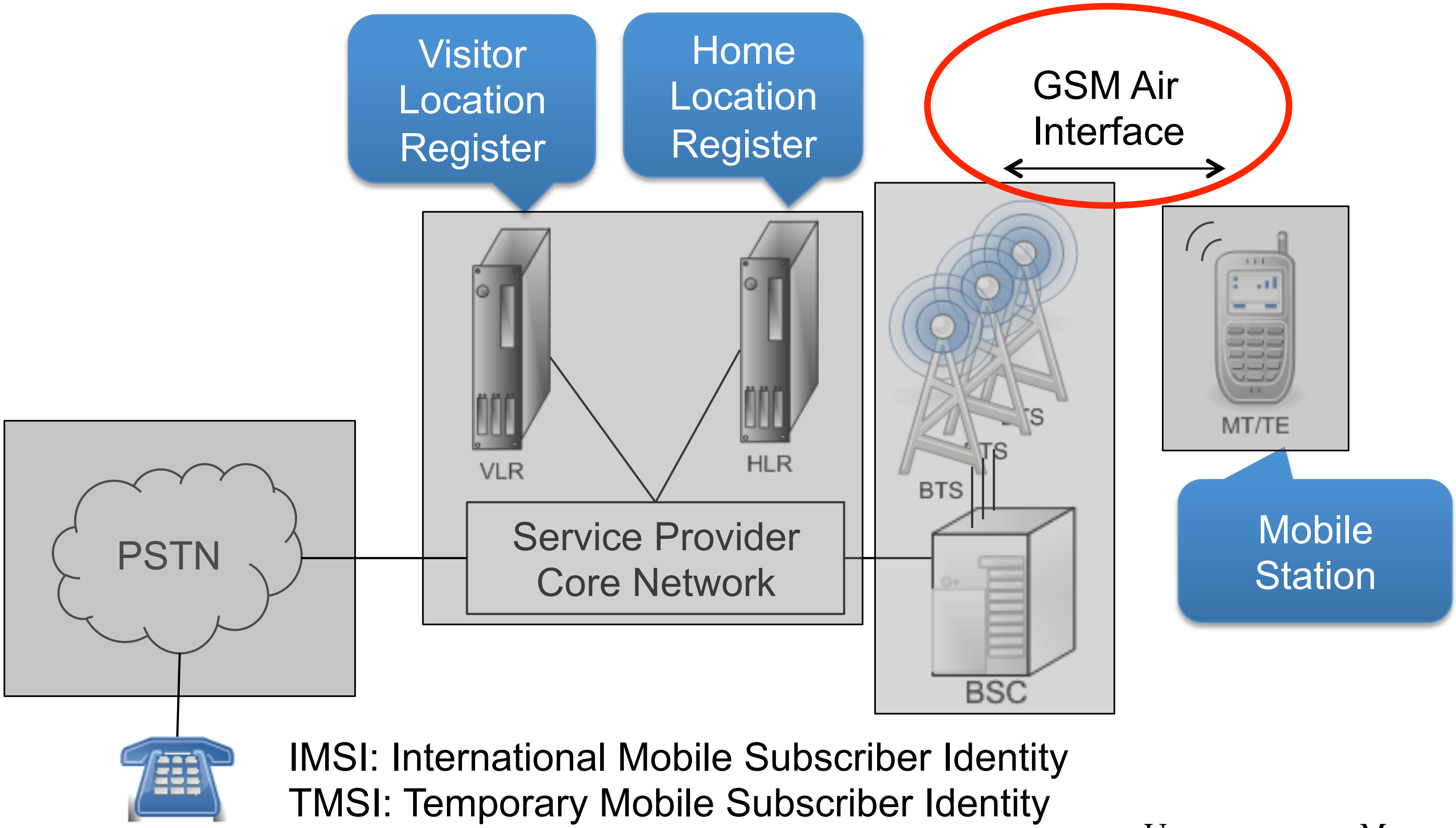
GSM Today

- 4.2 Billion worldwide users in 2010
  - United Nations NTU estimate
  - 5.3 Billion mobile users total
    - Includes users on CDMA, UMTS, LTE.
- Dominant protocol outside of the US
- Still widely used worldwide (including US)

Recent works and attacks on GSM

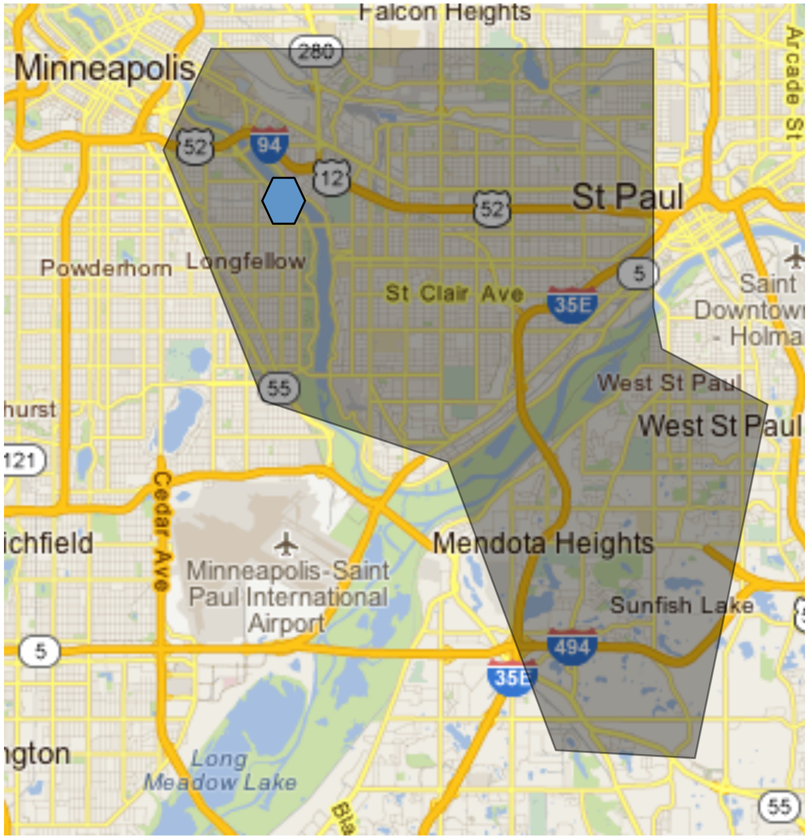
- Security of GSM, Nohl ‘09, ‘10, ‘11
  - Breaking the A5/1 cipher (2009)
  - Intercepting GSM call (2010)
  - Impersonating a mobile station (2011)
- Flooding attack using the SMS protocol
  - Traynor ‘05
- SMS of death, Muliner ‘11
- Location Based Services
  - Application layer of smart platforms, Cheng ‘06, Kalnis ’07
- Location information from service provider
  - Triangulation/trilateration, Caffery-Stuber ’98
- IP layer location information inference
  - Might not work for large networks behind NATs, Krishnamurthi ‘04

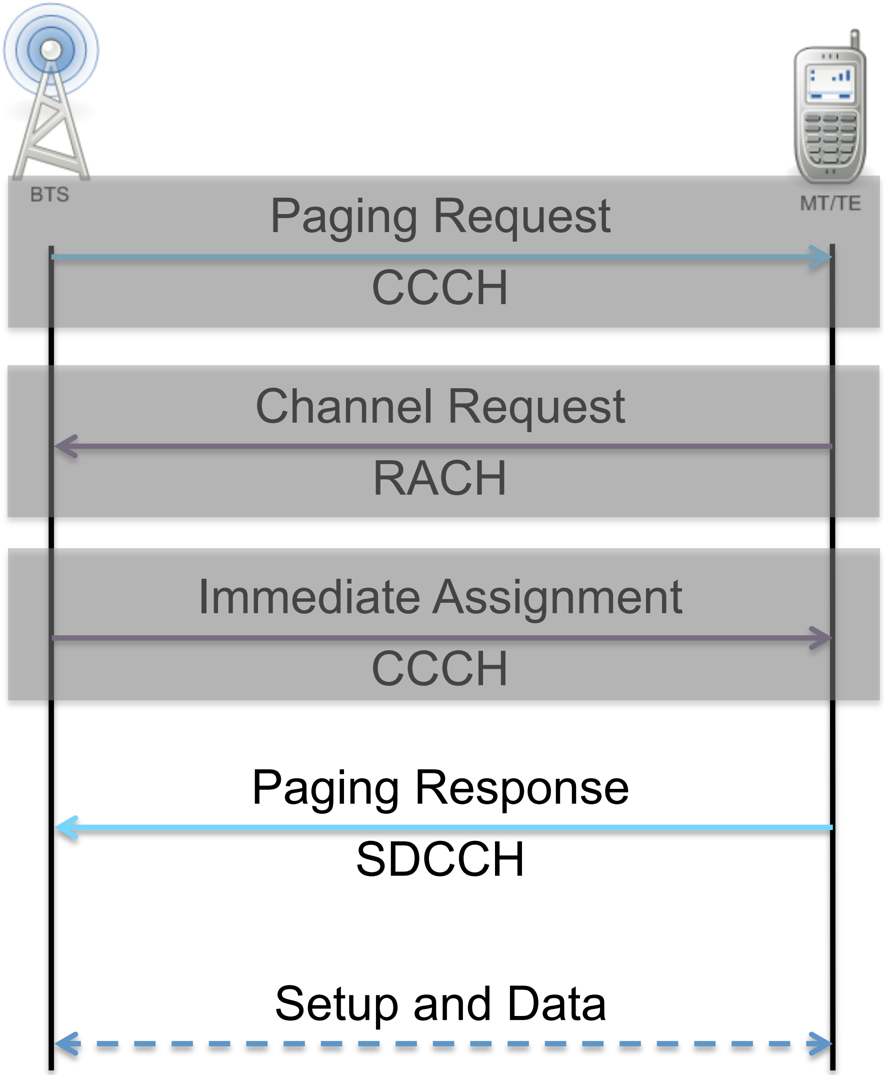
Cellular network architecture



IMSI: International Mobile Subscriber Identity
TMSI: Temporary Mobile Subscriber Identity

The GSM paging procedure





Paging Request

CCCH

Channel Request

RACH

Immediate Assignment

CCCH

Paging Response

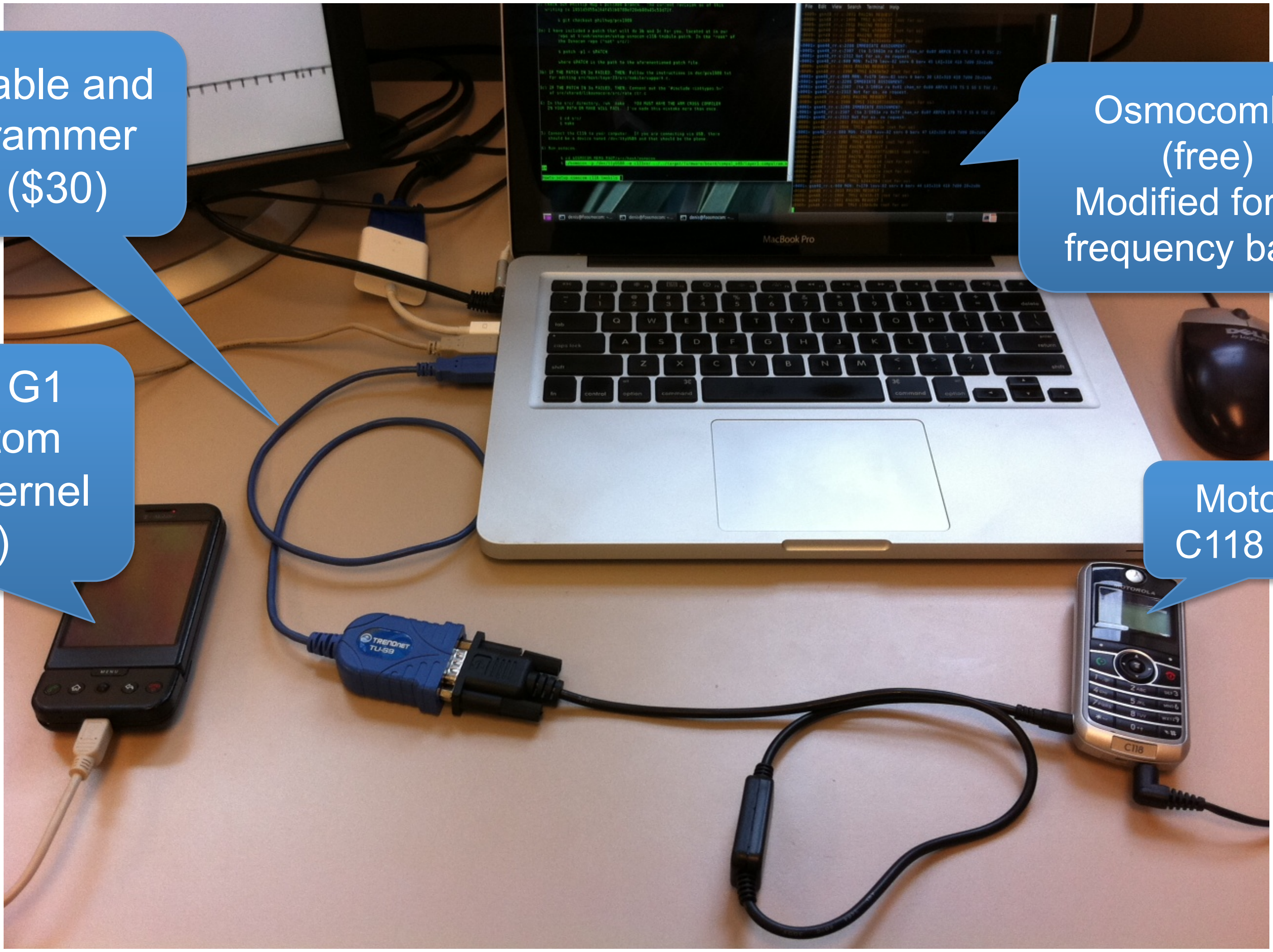
SDCCH

Setup and Data

UNIVERSITY OF MINNESOTA

Driven to Discover℠

Building the measurement platform



Serial cable and reprogrammer cable ($30)

OsmocomBB (free)
Modified for US frequency bands

T-Mobile G1 with custom Android Kernel ($100)

Motorola C118 ($30)

OsmocomBB (Open Source Mobile Communication Baseband)

- http://bb.osmocom.org
- Open source software -- free GSM implementation
- Served as the base for our location leak attack
    - Allows us to see paging & immediate assignment messages on frequencies of our choosing
- Custom firmware handles OSI layer 1 on phone, layers 2 and 3 handled on laptop
- Targetted for European users.

Basic mods on OsmocomBB

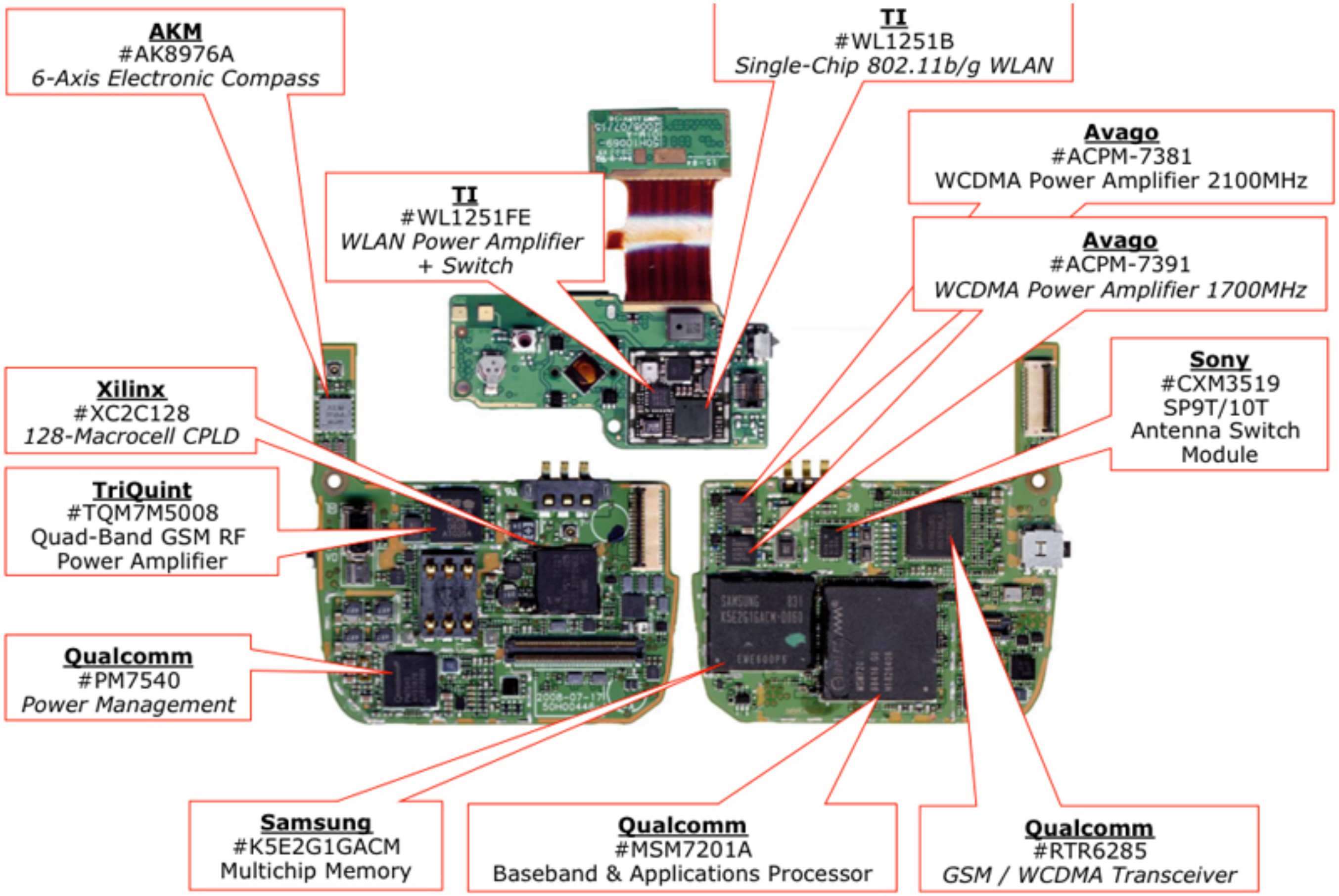
- Mods based on Phil Hug and Silvain Munaut
- PCS protocol on the 1900 MHz band
  - Frequencies in use in the U.S.
- SIM reader
  - allows reading network information from SIM card
- Uplink sniffing
  - Switch to uplink frequencies and wait for burst indication

Custom mods

- 100 lines of code changed to get Osmocom working
  - Minimal changes from the attacker
- Other nice changes
  - High resolution timestamp for output
  - Following specific immediate assignments
  - Sending uplink data to Wireshark for examination
- Heavy lifting with Perl scripts
  - Scanning frequencies with directional antenna
  - TMSI deanonymization

OsmocomBB live

The TMobile G1



AKM
#AK8976A
6-Axis Electronic Compass

TI
#WL1251B
Single-Chip 802.11b/g WLAN

TI
#WL1251FE
WLAN Power Amplifier + Switch

Avago
#ACPM-7381
WCDMA Power Amplifier 2100MHz

Avago
#ACPM-7391
WCDMA Power Amplifier 1700MHz

Xilinx
#XC2C128
128-Macrocell CPLD

Sony
#CXM3519
SP9T/10T
Antenna Switch Module

TriQuint
#TQM7M5008
Quad-Band GSM RF Power Amplifier

Qualcomm
#PM7540
Power Management

Samsung
#K5E2G1GACM
Multichip Memory

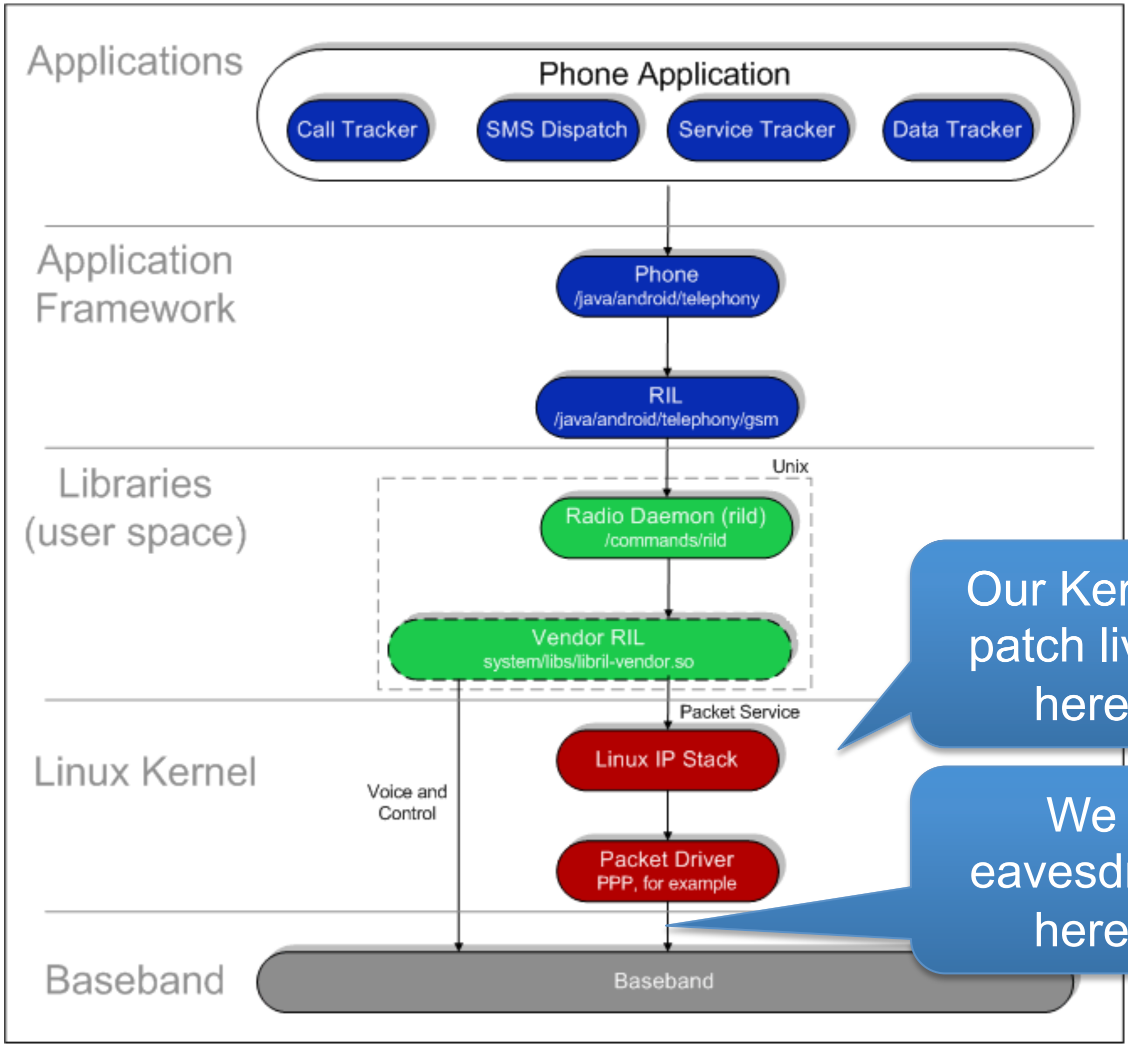
Qualcomm
#MSM7201A
Baseband & Applications Processor

Qualcomm
#RTR6285
GSM / WCDMA Transceiver

Hacking the Android Kernel

- Great tool to measure the layout of cell towers
- Custom kernel driver, output to a serial device
- Intercept messages to / from the baseband chip in the kernel.
- Findings:
  - Possible to intercept network traffic from OSI layer 3 and up
  - Baseband chips controlled by Hayes AT commands. GSM extensions. 3GPP TS 27.007

Android Radio Interface Layer



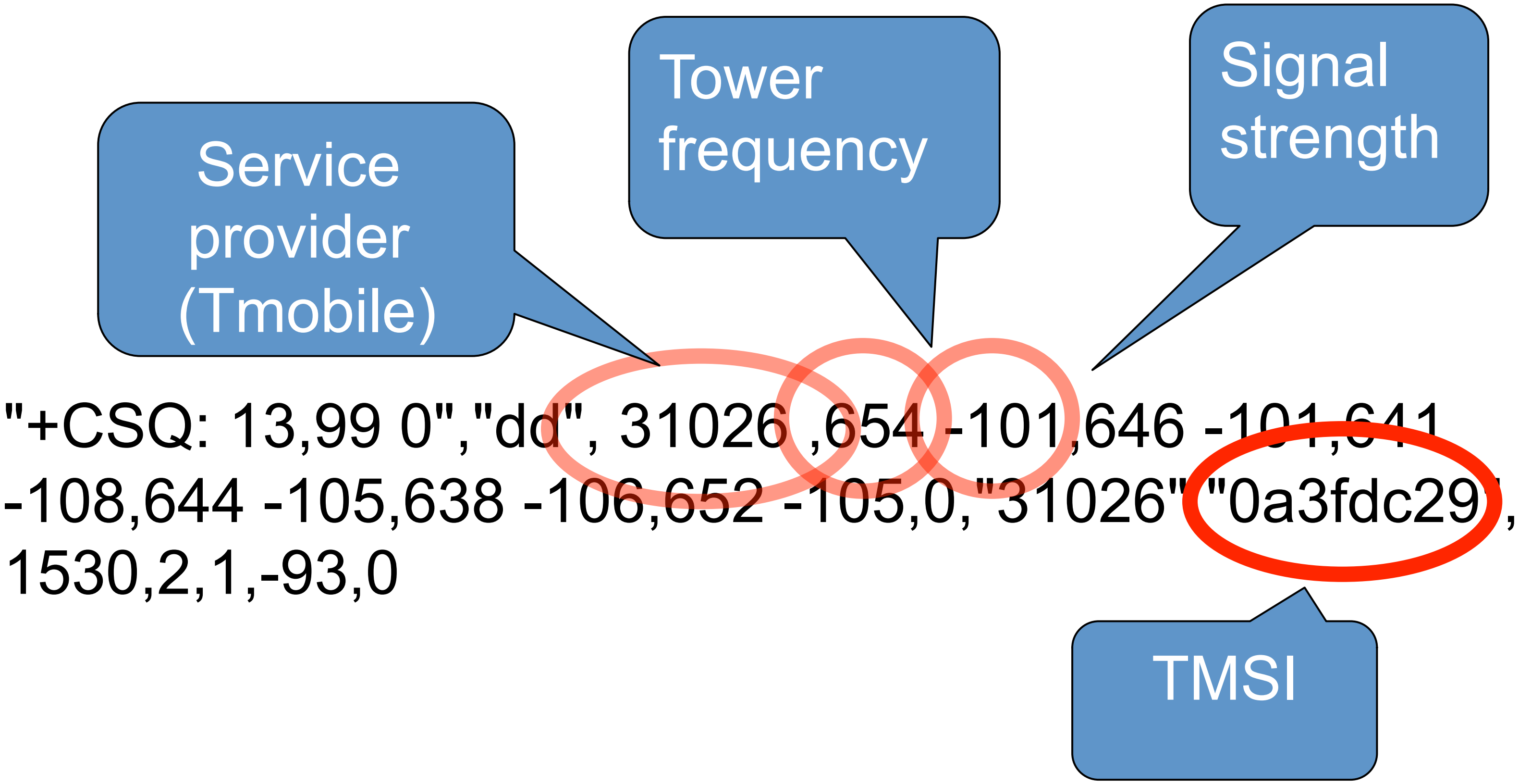
Our Kernel patch lives here

We eavesdrop here

Hayes AT Commands revived

- ATDT phone number
  - Calls that phone number
  - Just like old school modems
- Tmobile G1
  - Baseband 62.33.20.08H with Qualcomm RTR6785 transceiver
- iPhone 3G
  - Baseband 06.15.00 with Infeneon transceiver.
- Any other interesting commands?
  - AT+CSQ

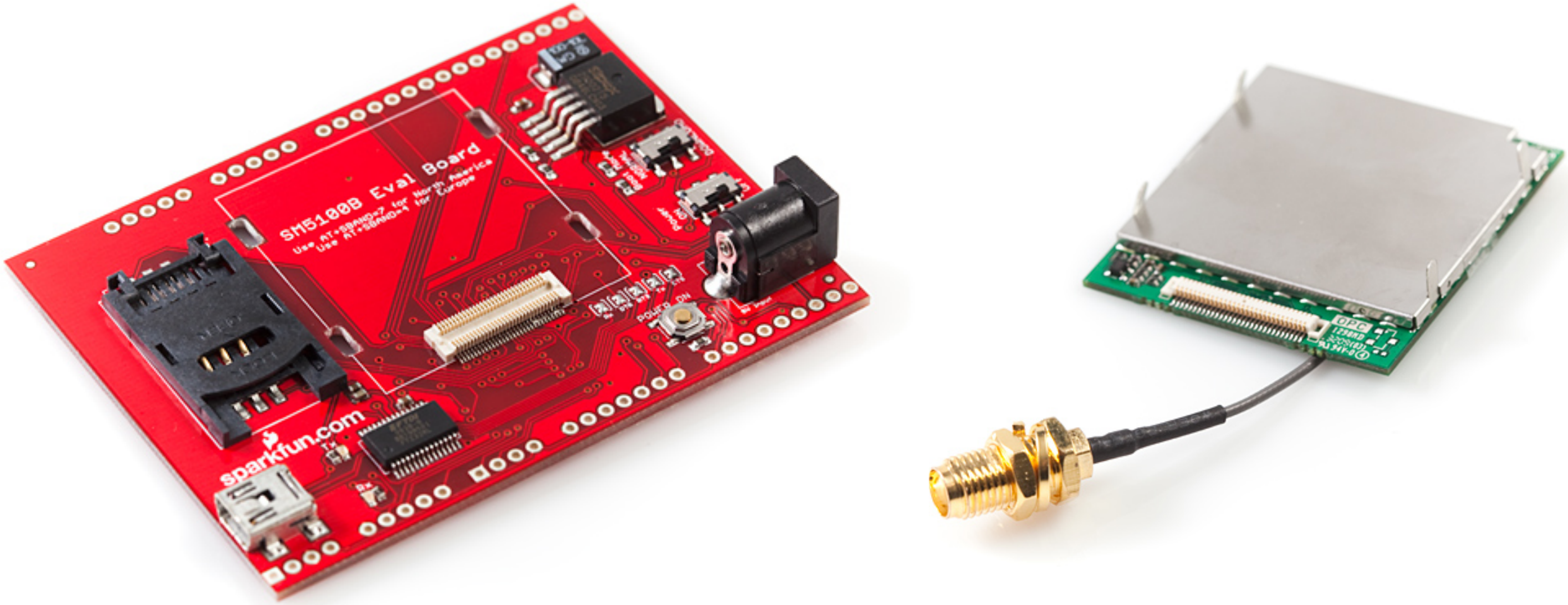
The AT+CSQ return message



```
"+CSQ: 13,99 0","dd", 31026 ,654 -101,646 -101,641
-108,644 -105,638 -106,652 -105,0,"31026","0a3fdc29",
1530,2,1,-93,0
```

Other development boards (Sparkfun)

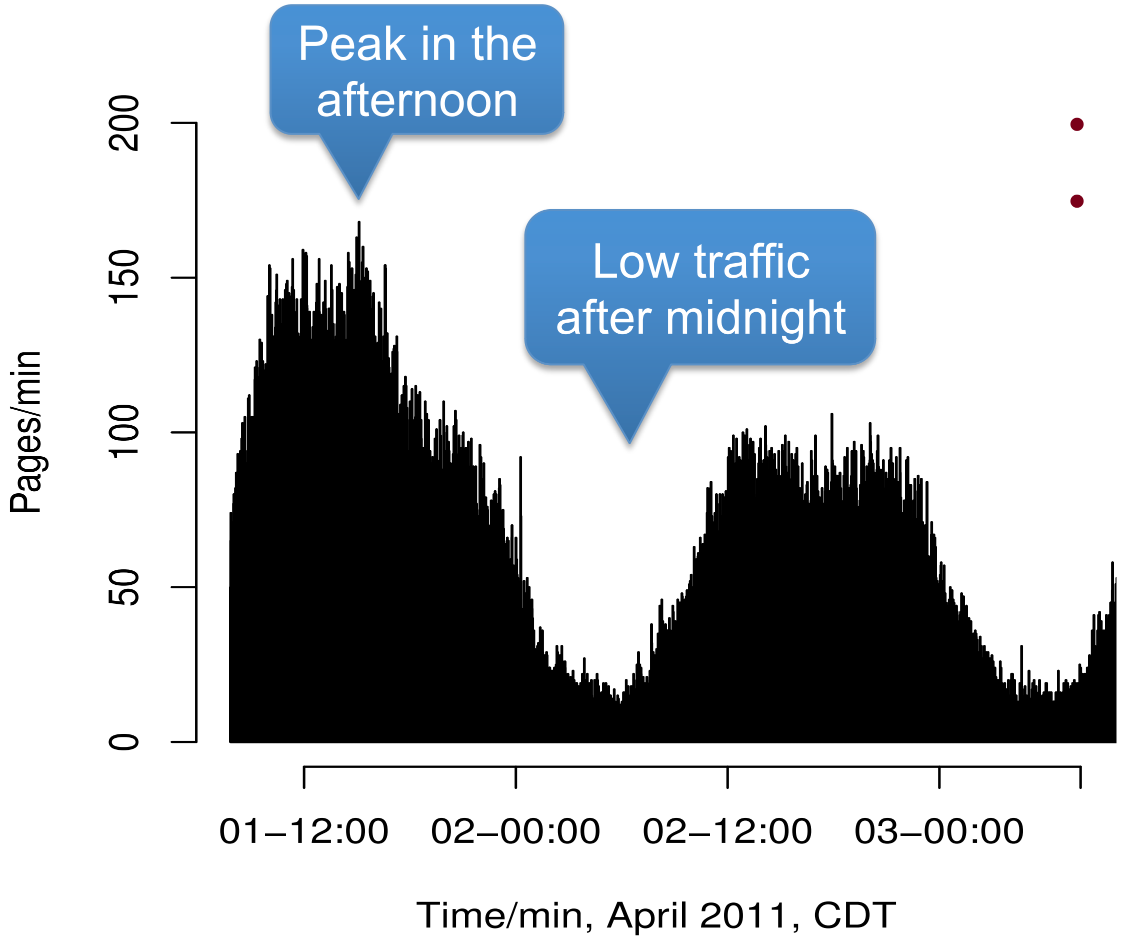
- Responds to AT commands from 3GPP TS 27.007



GSM paging channel observations

	T-Mobile LAC 747b	AT&T LAC 7d11
Paging Requests – IMSI	27,120	8,897
Paging Requests – TMSI	257,159	84,526
Paging Requests Type 1	284,279	91,539
Paging Requests Type 2	1,635	26
Paging Requests Type 3	0	1
Observation period	24 hours	24 hours

Pages and human activity

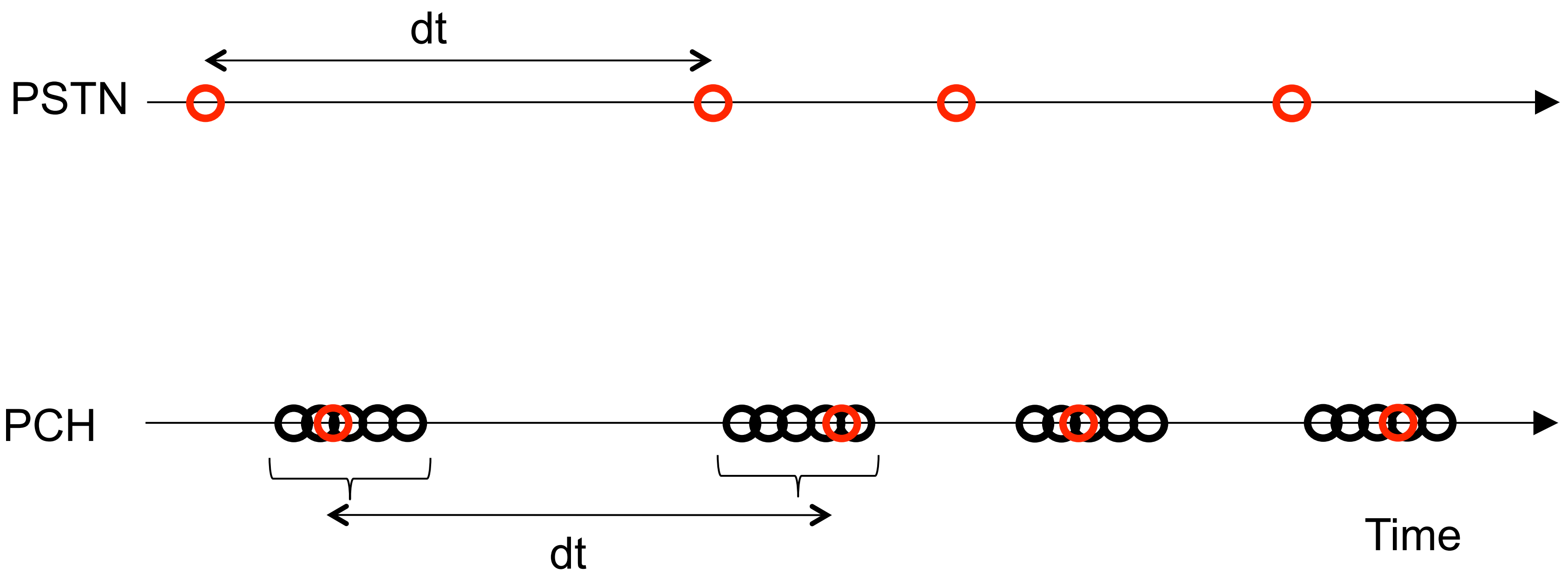


Peak in the afternoon

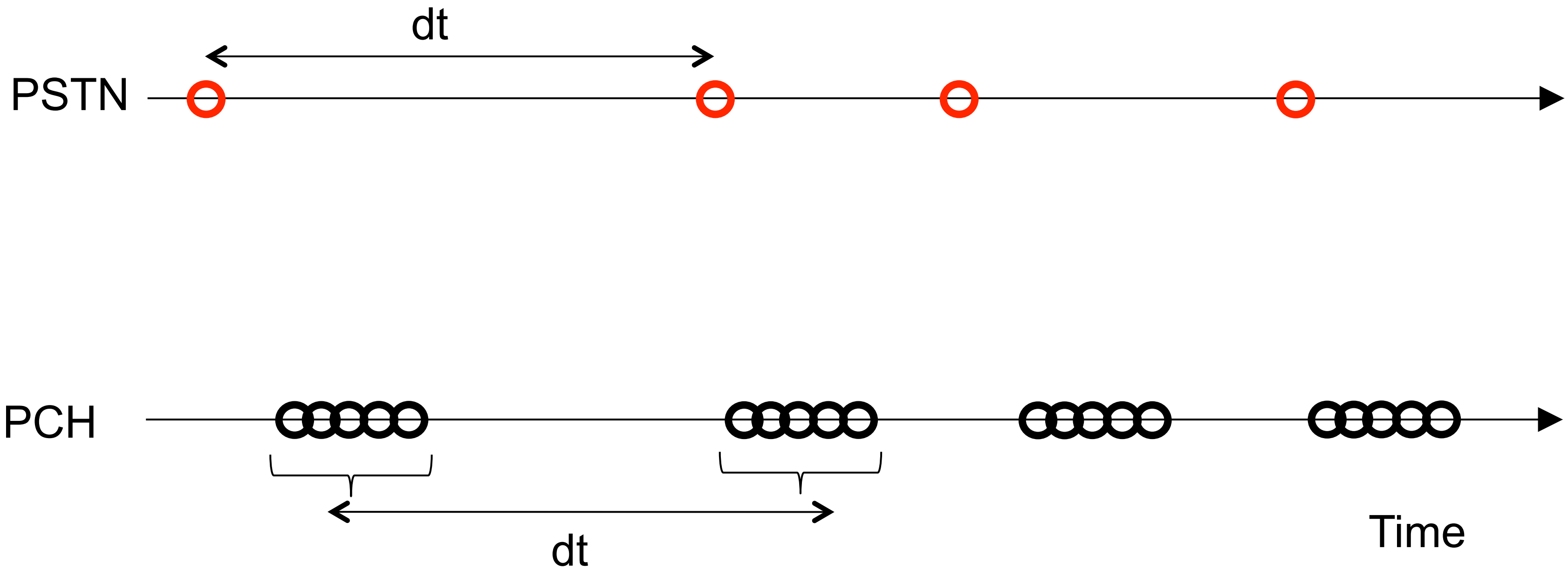
Low traffic after midnight

- University campus
- Day of the week during the semester

Phone number-TMSI mapping

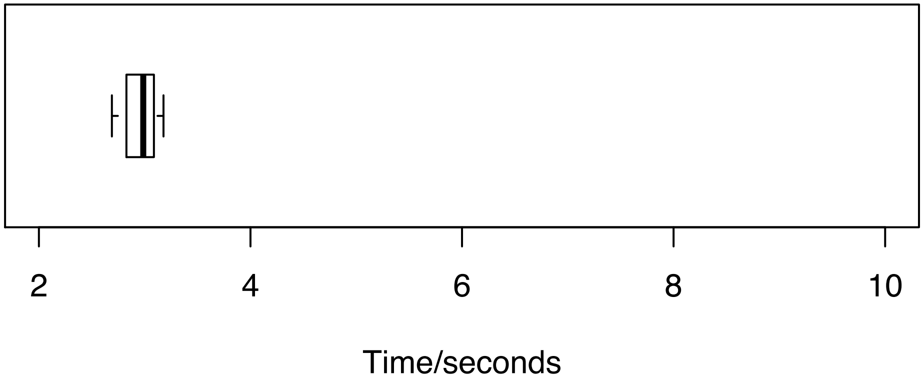


No recovered TMSI

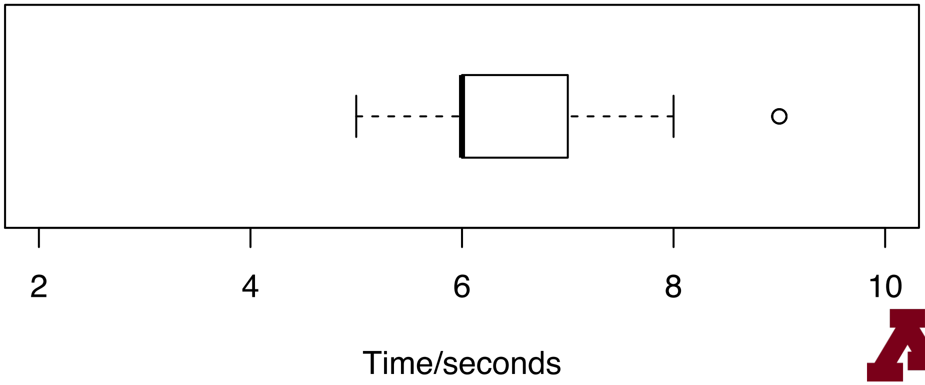


Silent paging

- Delay between the call initiation and the paging request
  - 3 seconds



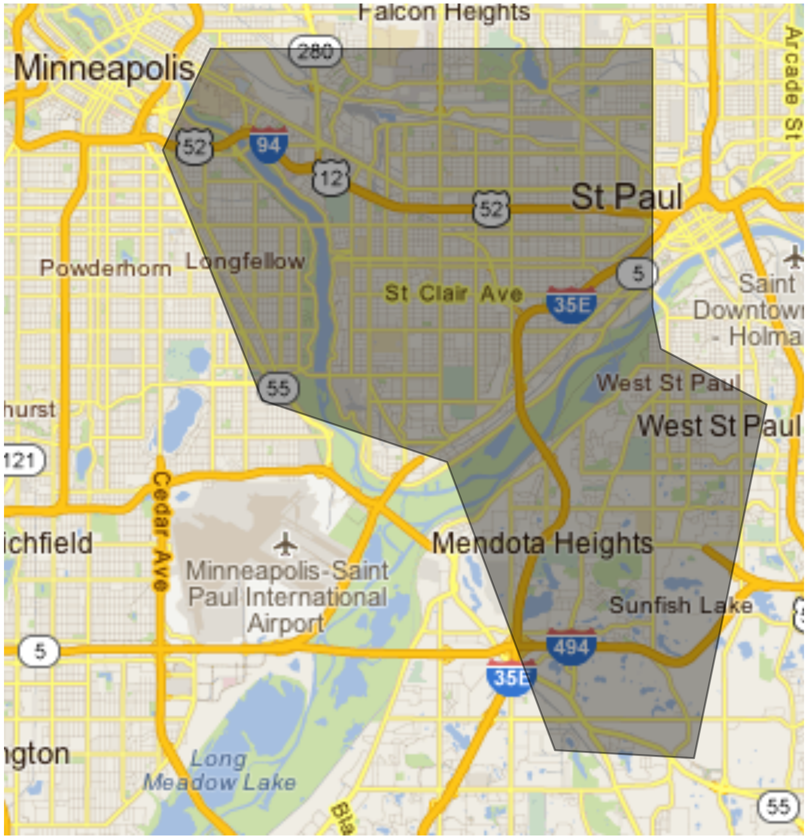
- Median delay between call initiation and ring
  - 6 seconds



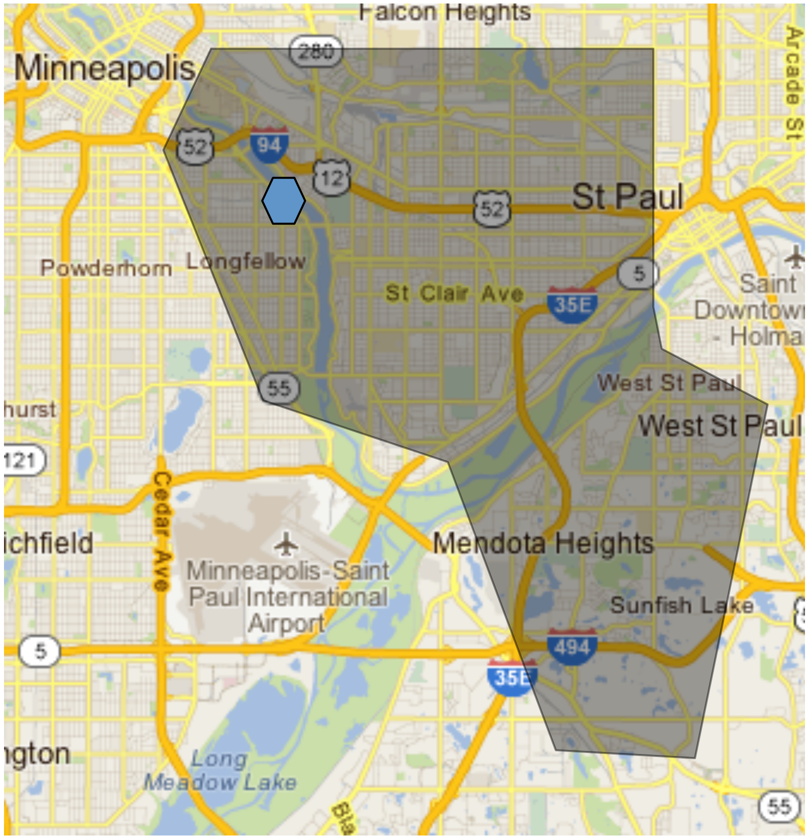
University of Minnesota
Driven to Discover℠

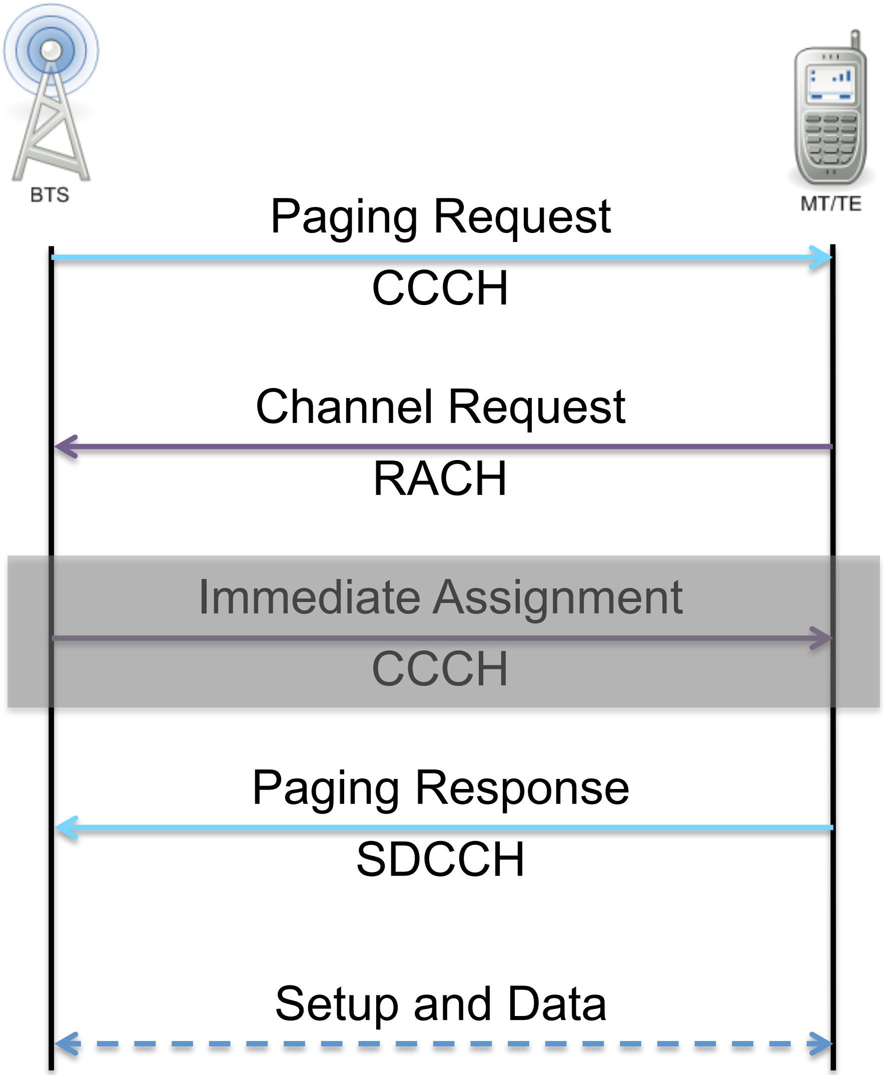
Bounding the LAC

- LACs can be very large.
  - T-Mobile LAC 747d: 100km^2
- Used a wall-following algorithm, road permitting.
- Call to MS on NW corner.
- Observed paging request on SE corner.



The GSM paging procedure





Paging Request

CCCH

Channel Request

RACH

Immediate Assignment

CCCH

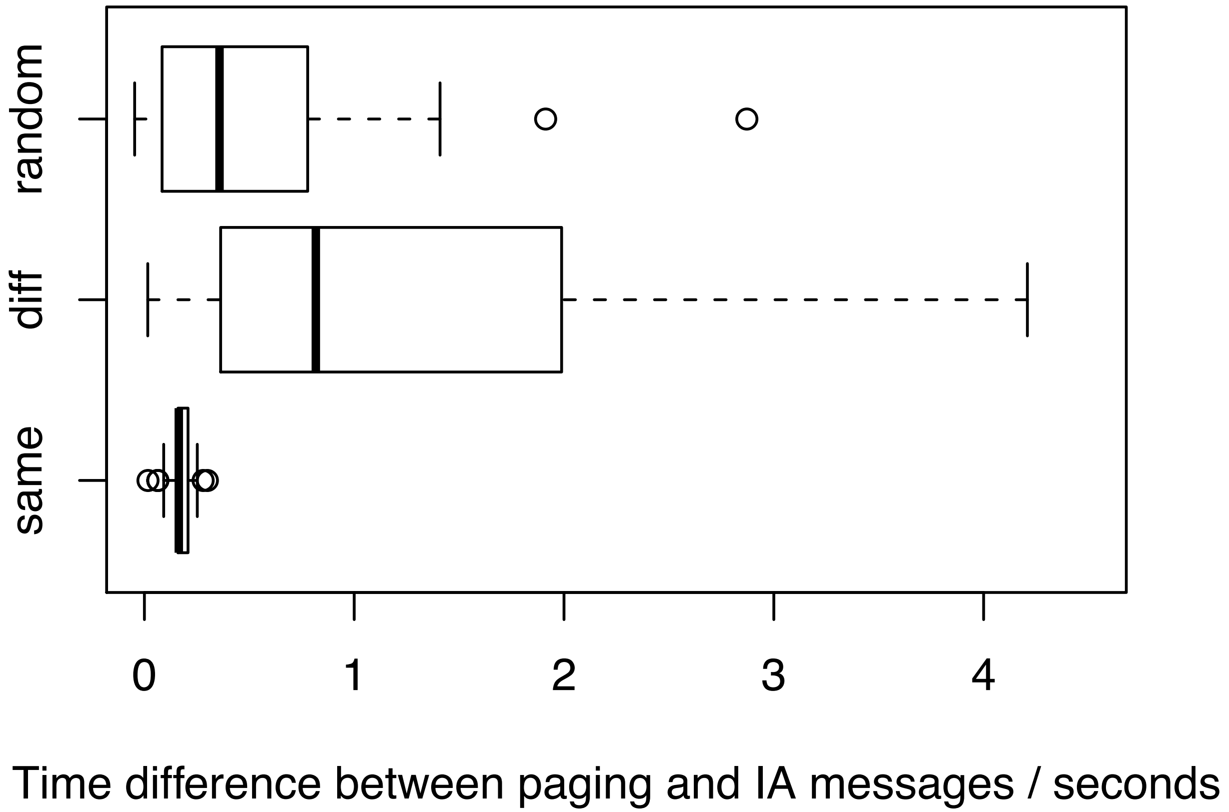
Paging Response

SDCCH

Setup and Data

Same tower test

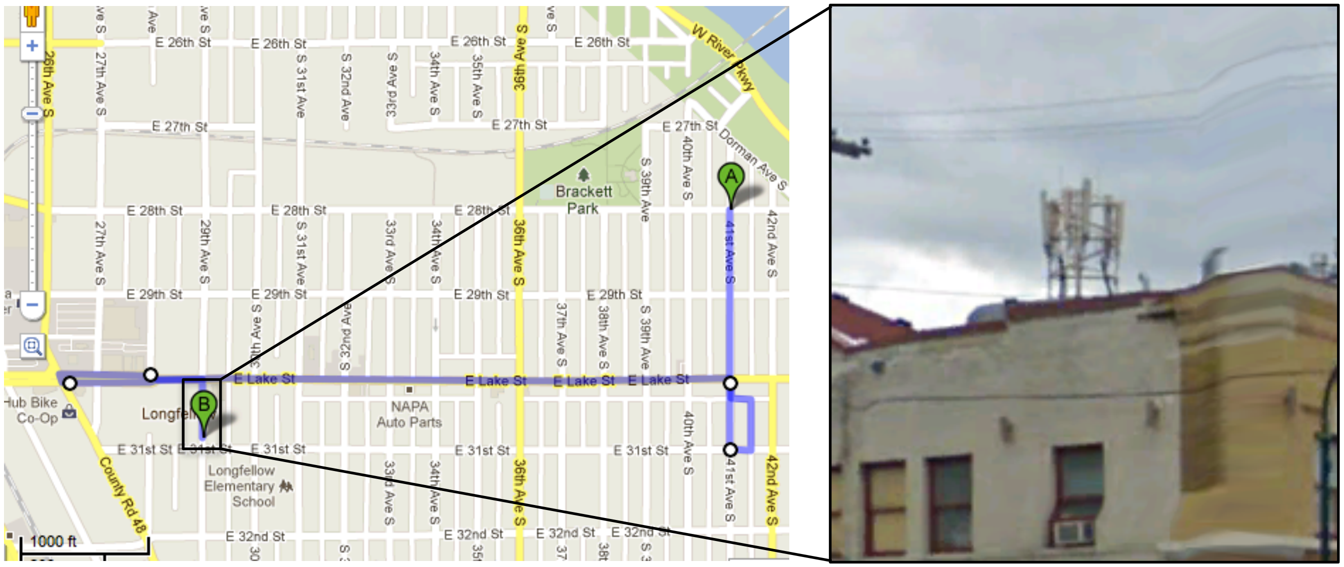
- Delay between the paging request and the immediate assignment message.



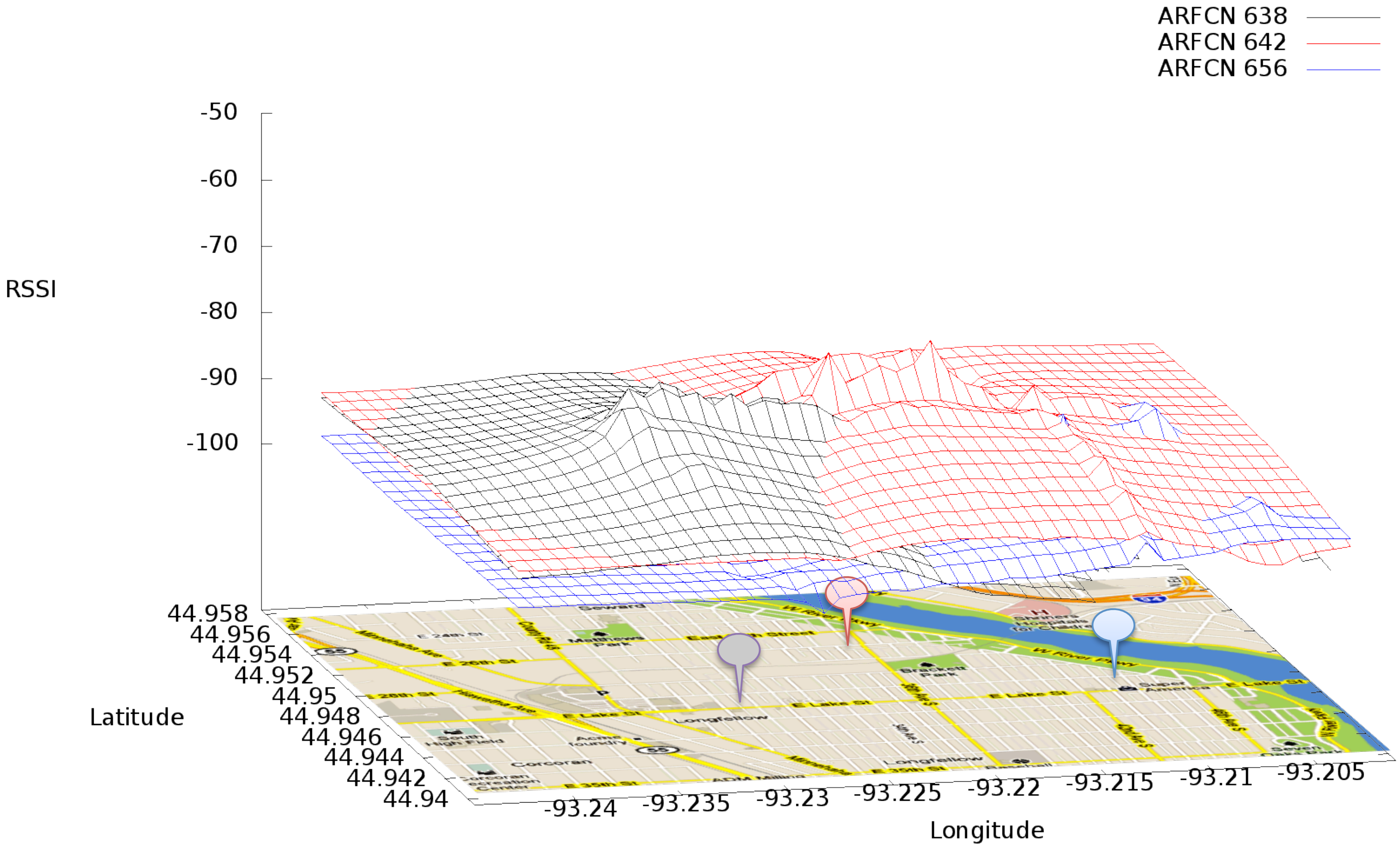
University of Minnesota
Driven to Discover℠

Finding individual towers

- Find individual towers with a hill-climbing algorithm.
  - Non-uniform RF attenuation.
  - Overshoot by 50m to avoid local maximum.



Where is the phone likely to be?



Directional antenna

- Use existing OsmocomBB code to perform frequency scan
- Sort list of frequencies by RSSI
- Attempt to camp on each frequency
- Record which frequencies contain cells and in which direction the cell is located

Directional antenna experiments

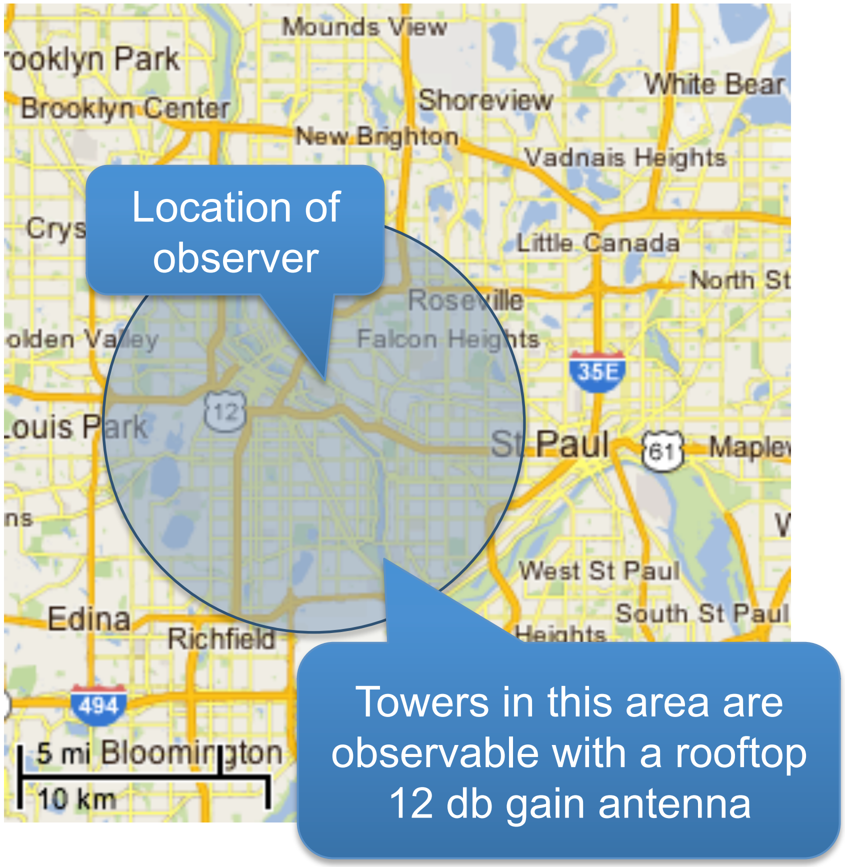
- Goal: determine how far we can hear cell broadcast messages
- Method: from a clear vantage point, scan through frequencies at intervals of 15 degrees to map nearby cells
- Findings: we are able to map cells in a 200km^2 area

Coverage with one antenna

Downtown Minneapolis

Yagi antenna 12dB gain

John’s new “haircut”



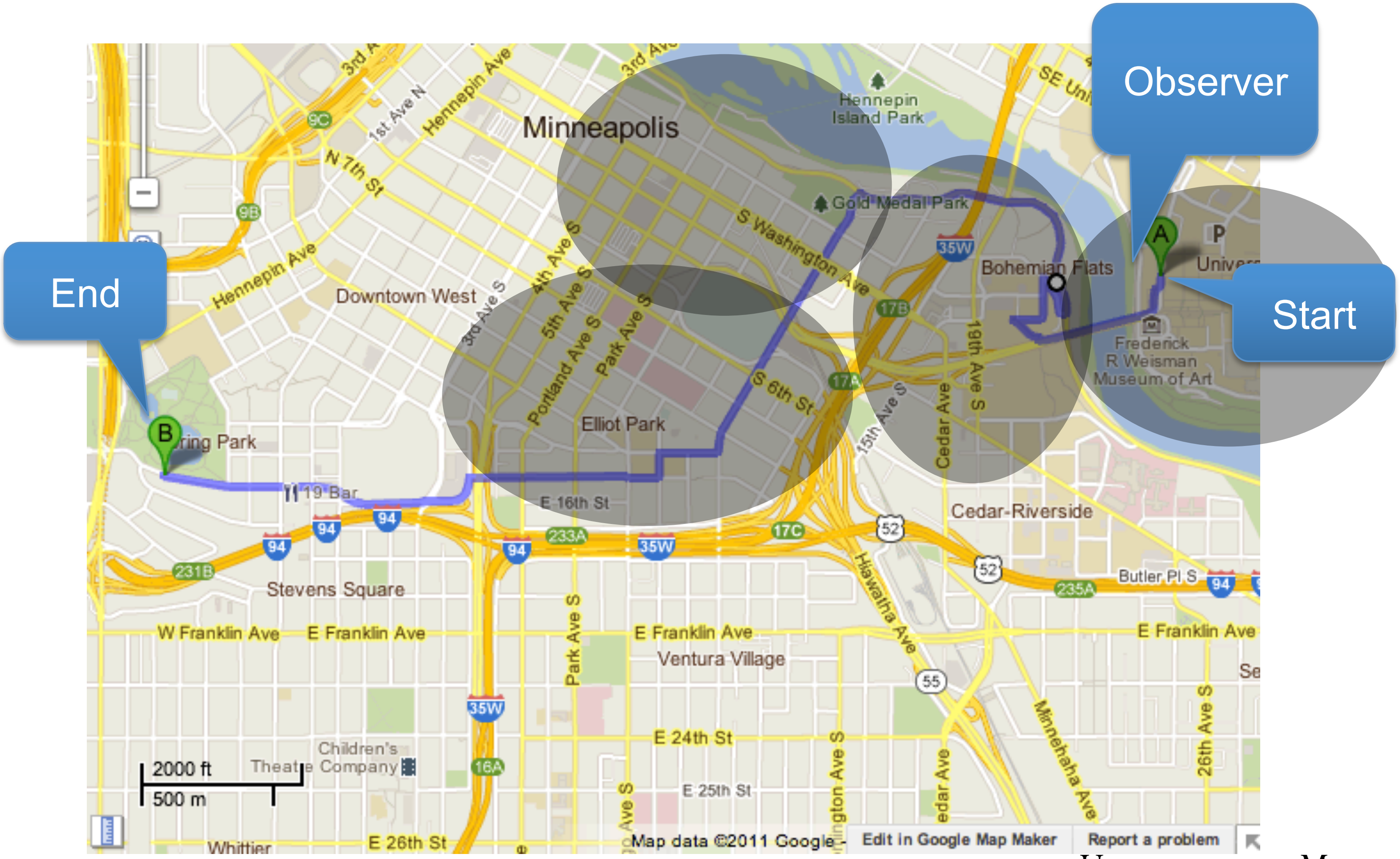
Location of observer

Towers in this area are observable with a rooftop 12 db gain antenna

Following a walking person

- Goal: determine if location testing is feasible on a moving target
- Method: using a directional antenna and high vantage point, follow the procedures for finding a victim's TMSI
- Findings: following a walking person is feasible; following a moving vehicle would be difficult
- Hard to follow a vehicle with only 1 antenna.

Tracking users in motion



Defenses

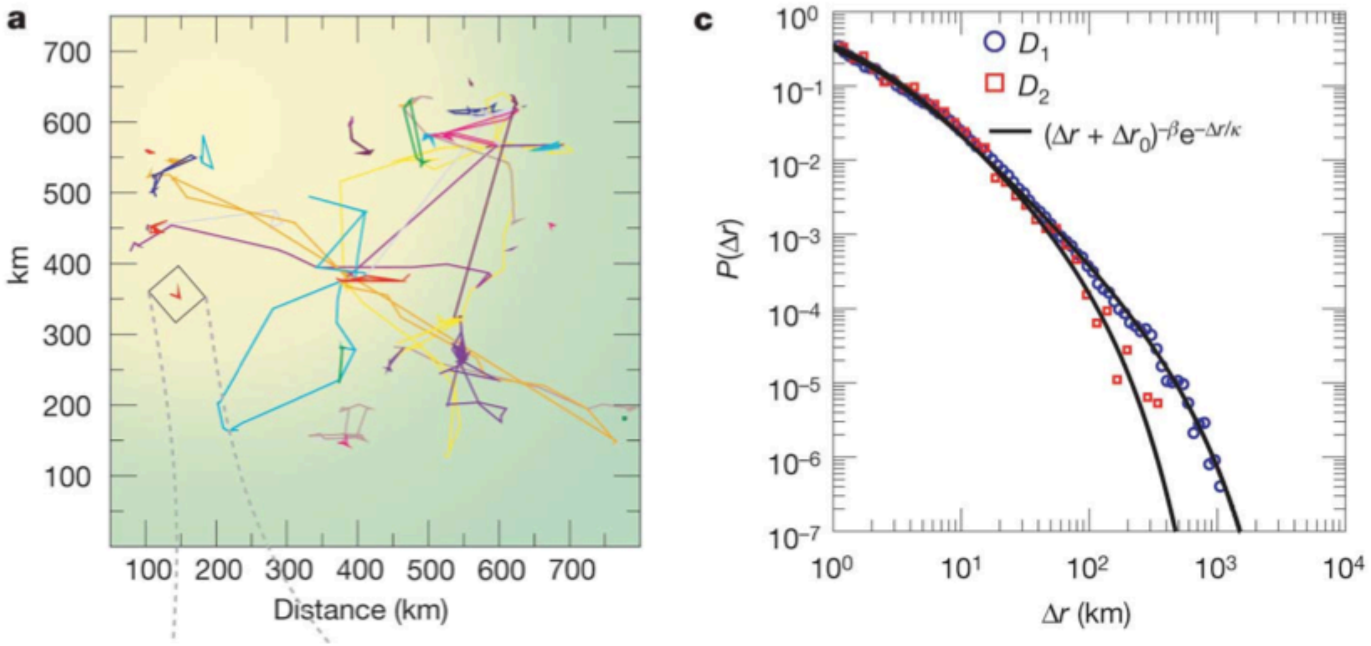
- Page multiple areas.
  - Less than 0.6% of paging requests are not type 1.
  - Available bandwidth for additional pages.
  - Human trajectories are predictable.
- Continuous time mixes.
  - Switch TMSI at least once per page.
    - phone/TMSI bitwise unlinkable.
  - Prevent traffic analysis.
    - Cover traffic.
    - Add exponential delay to paging requests.

How do we prevent those attacks?

- Page multiple areas
- Make phone/TMSI bitwise unlinkable
- Prevent traffic analysis
  - Cover traffic
  - Change distribution of egress traffic

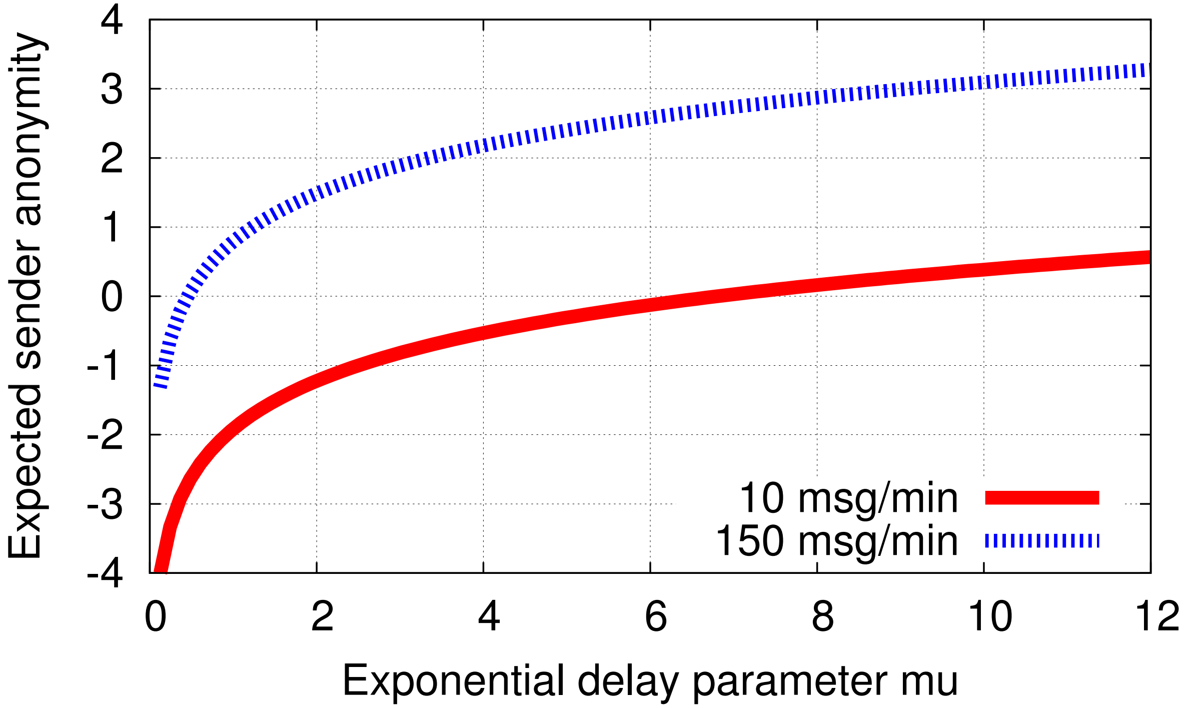
Paging multiple LACs

- Less than 0.6% of paging requests are not type 1
  - Available bandwidth for additional pages
- Human trajectories are very predictable
  - Gonzales, Hidalgo, Barabasi ‘05



Applying known anonymity schemes

- Continuous time mixes applied to the paging channel
  - Arrival rate follows a Poisson distribution
  - Change departure rate to an exponential distribution



Conclusion

- Systems with broadcast paging protocols could leak location information.
- Leaks observable with
  - readily available equipment equipment,
  - no (direct) help from the service provider.
- Proposed low cost fixes.
- Responsible disclosures.
  - 3GPP, Nokia, AT&T research

Questions

- foo@cs.umn.edu
- http://www.cs.umn.edu/~foo