Location Leaks on the GSM Air Interface

Denis Foo Kune,

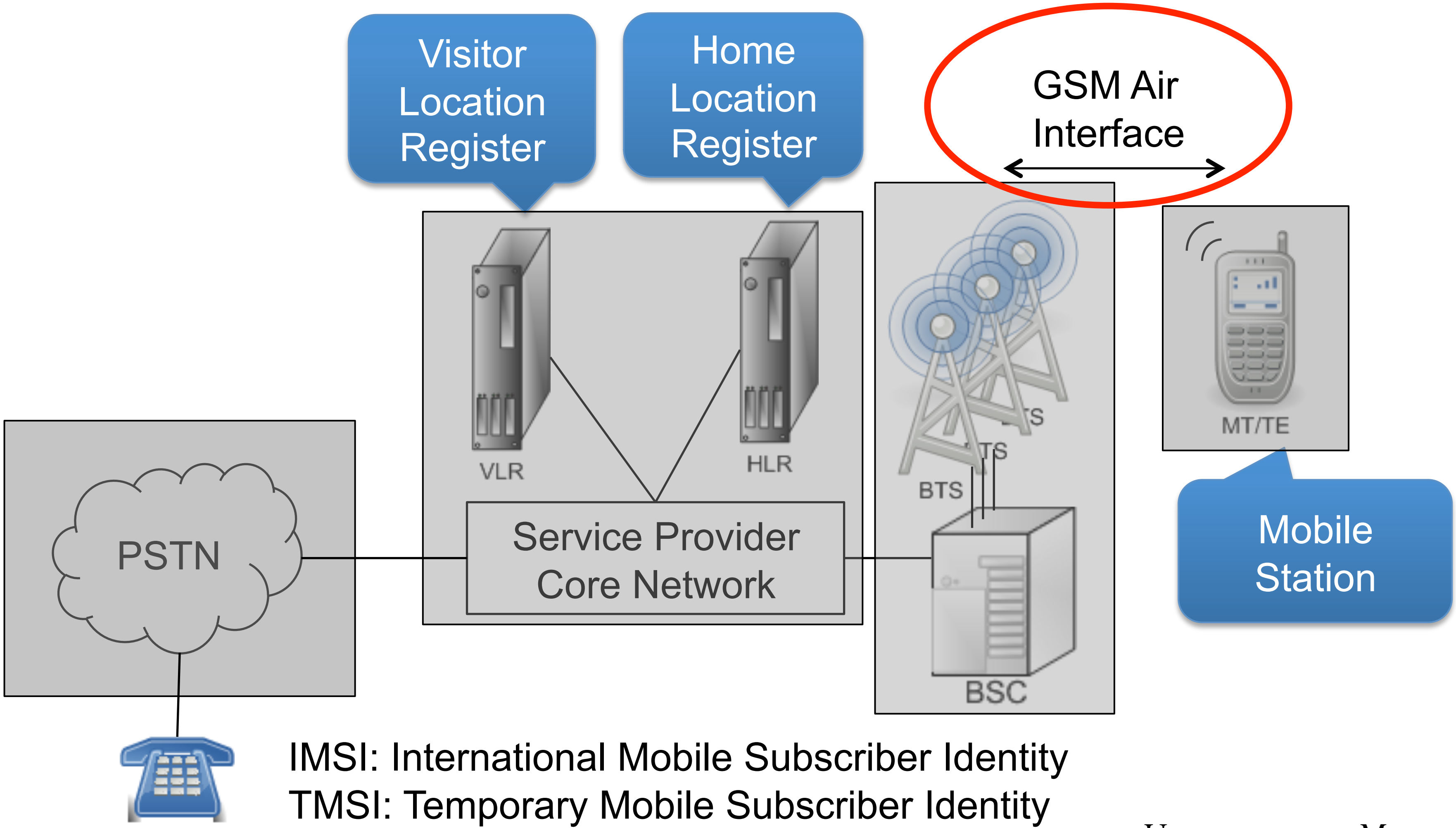
John Koelndorfer, Nick Hopper,
Yongdae Kim

University of Minnesota

Problem definition

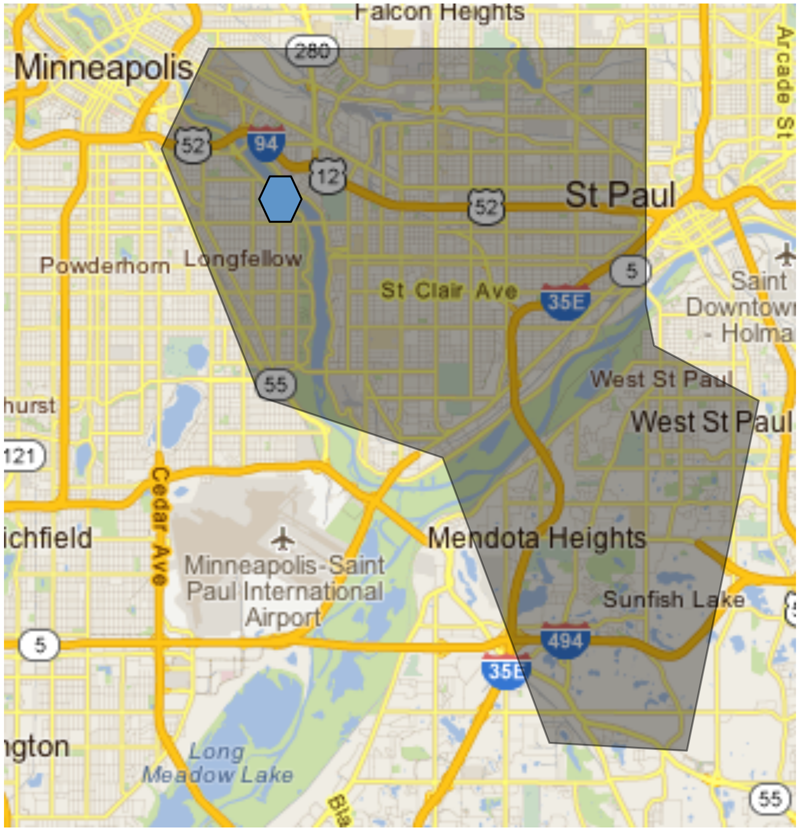
- Large array of towers broadcasting messages
  - Can those messages reveal a phone’s location?
- Given a person’s phone number
  - can we locate the tower they are attached to in a GSM network?
- GSM: dominant protocol worldwide
  - Analysis of layer 2/3 messages only.
- No collaboration from the service provider.
- No support from apps.

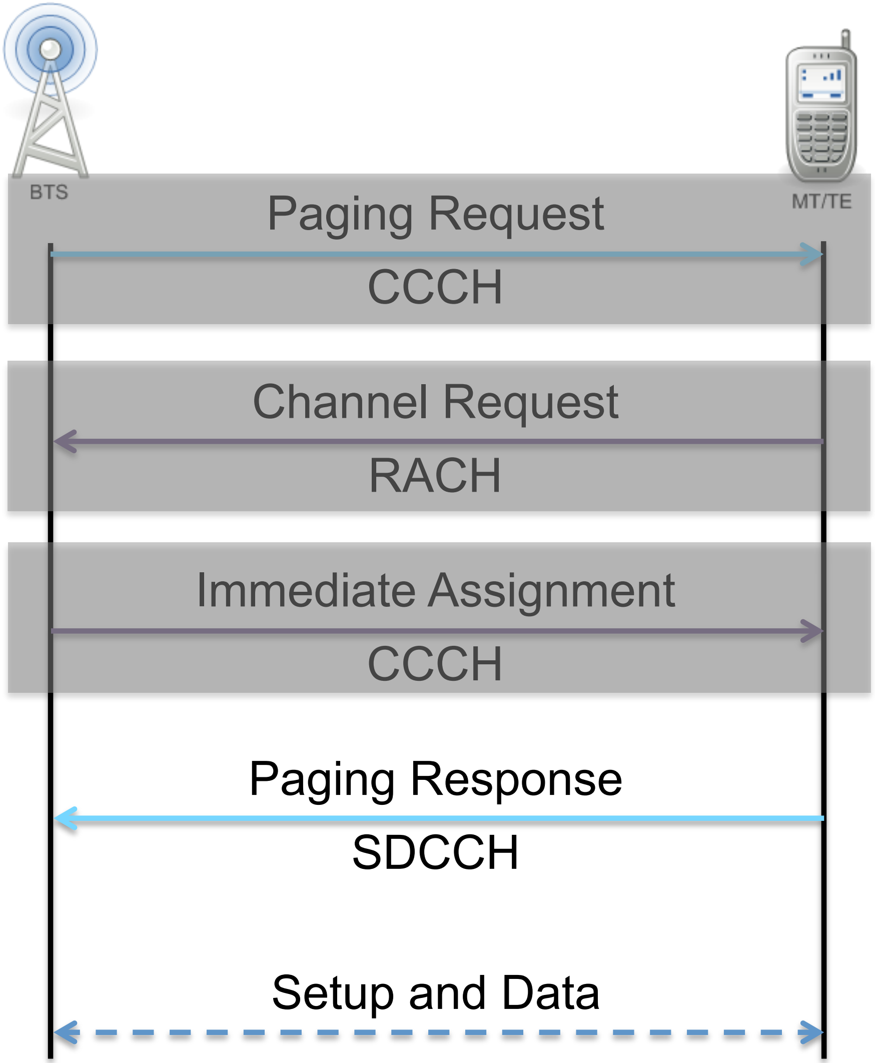
Cellular network architecture



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

The GSM paging procedure





Paging Request

CCCH

Channel Request

RACH

Immediate Assignment

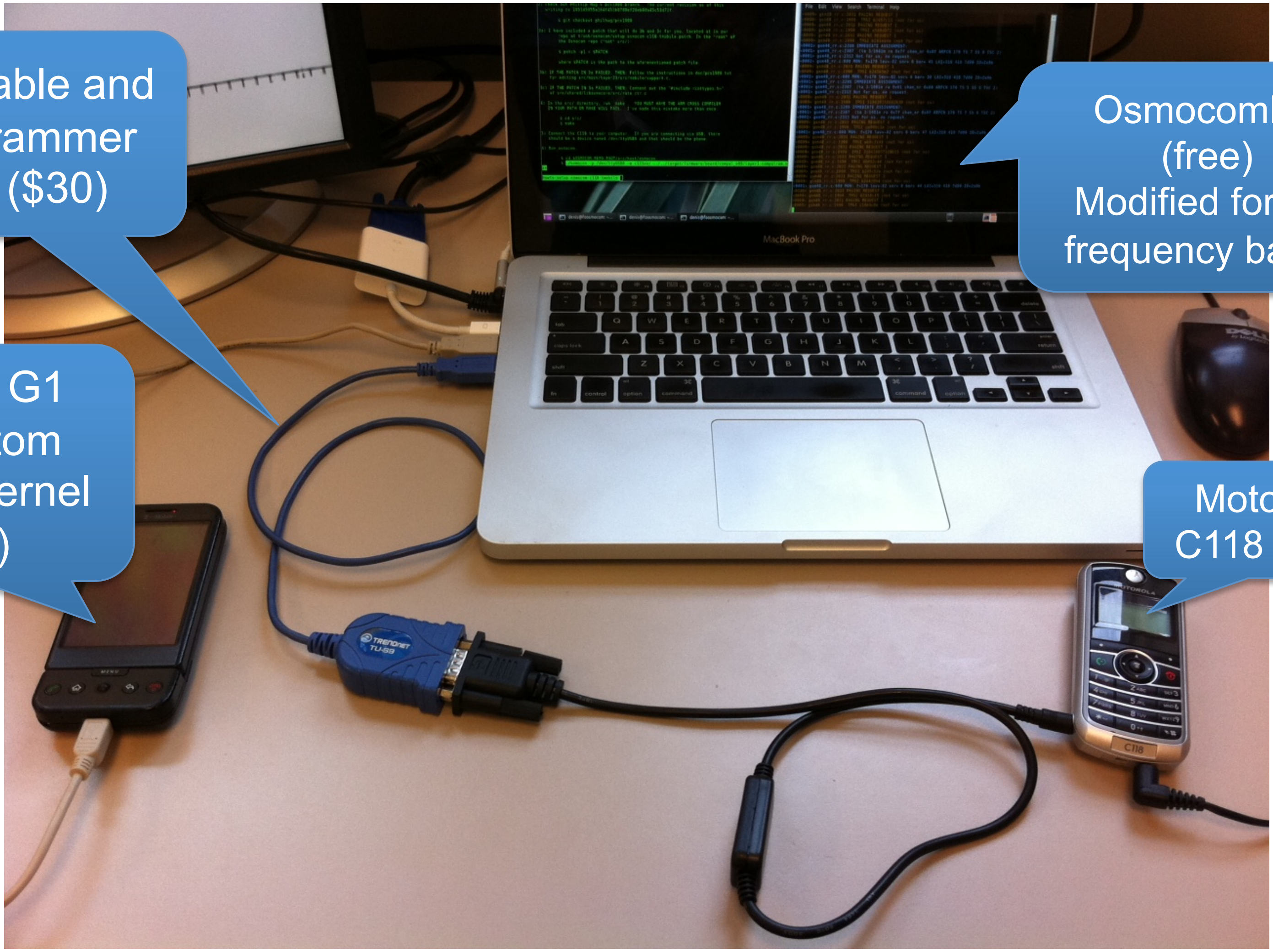
CCCH

Paging Response

SDCCH

Setup and Data

Measurement platform



Serial cable and reprogrammer cable ($30)

OsmocomBB (free) Modified for US frequency bands

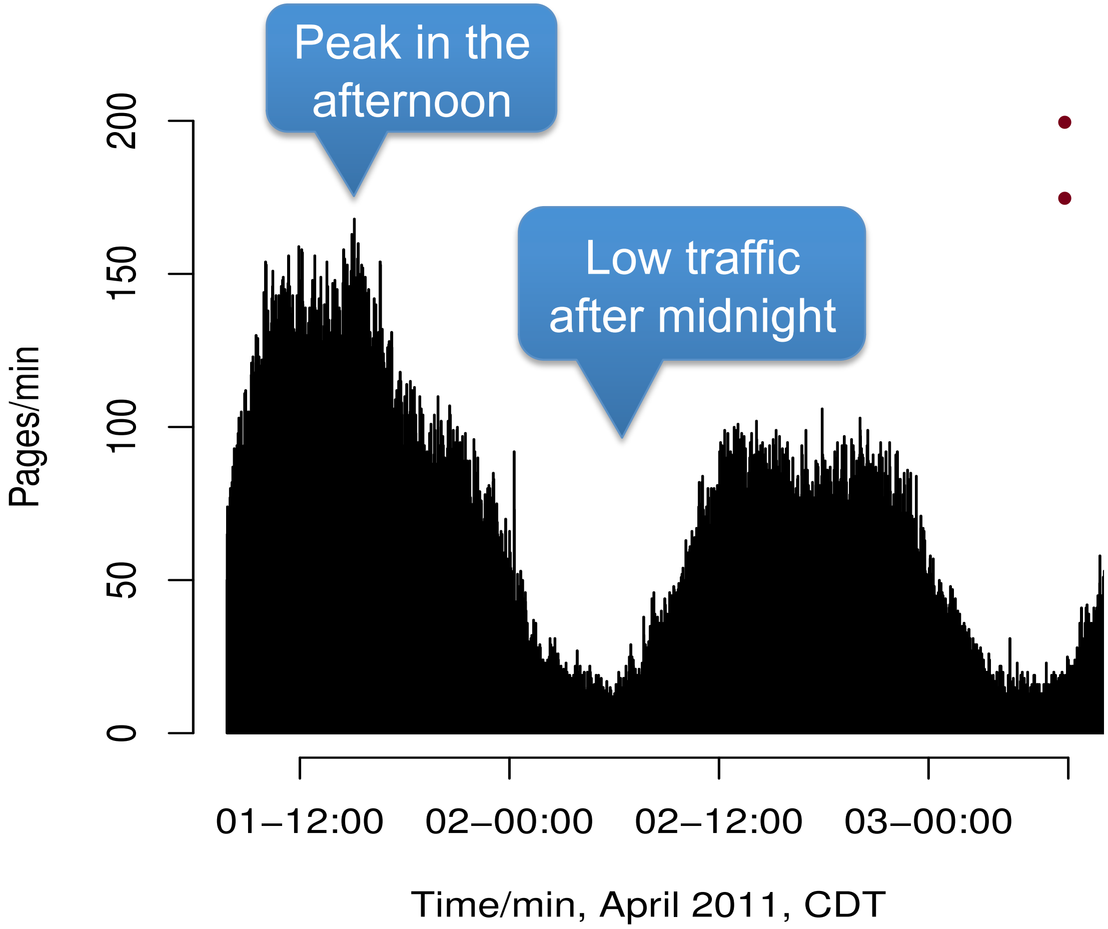
T-Mobile G1 with custom Android Kernel ($100)

Motorola C118 ($30)

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

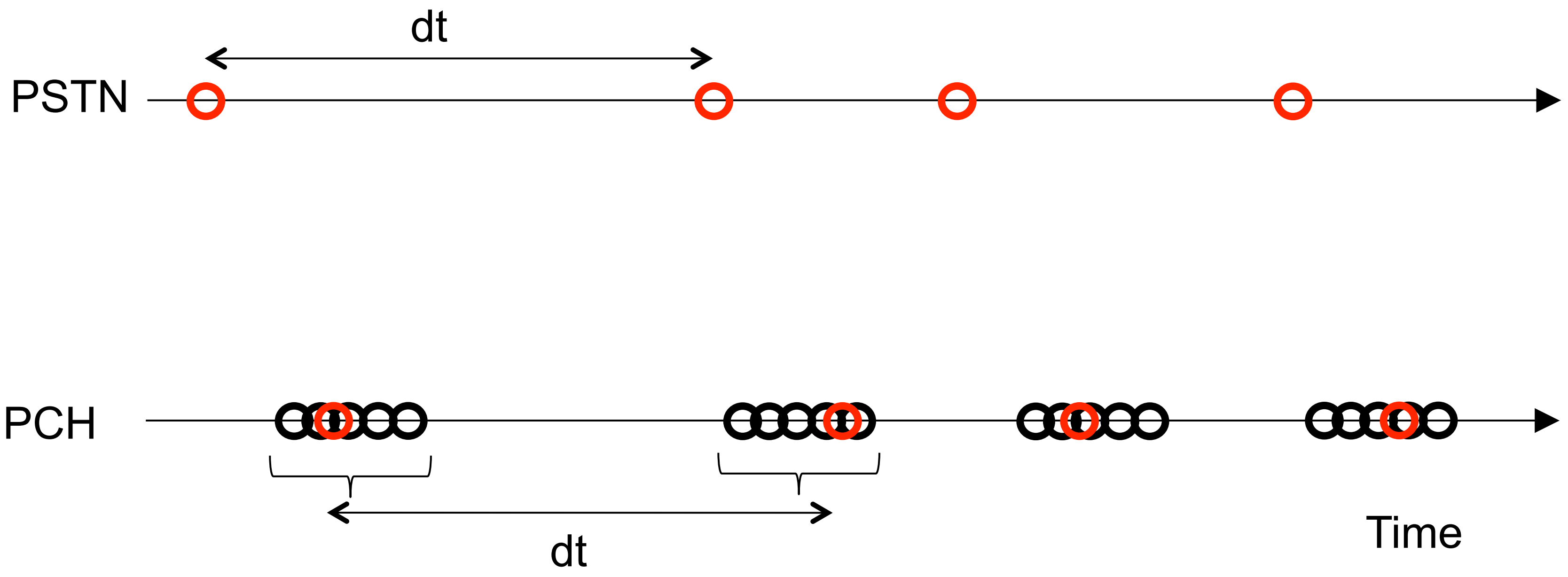


Peak in the afternoon

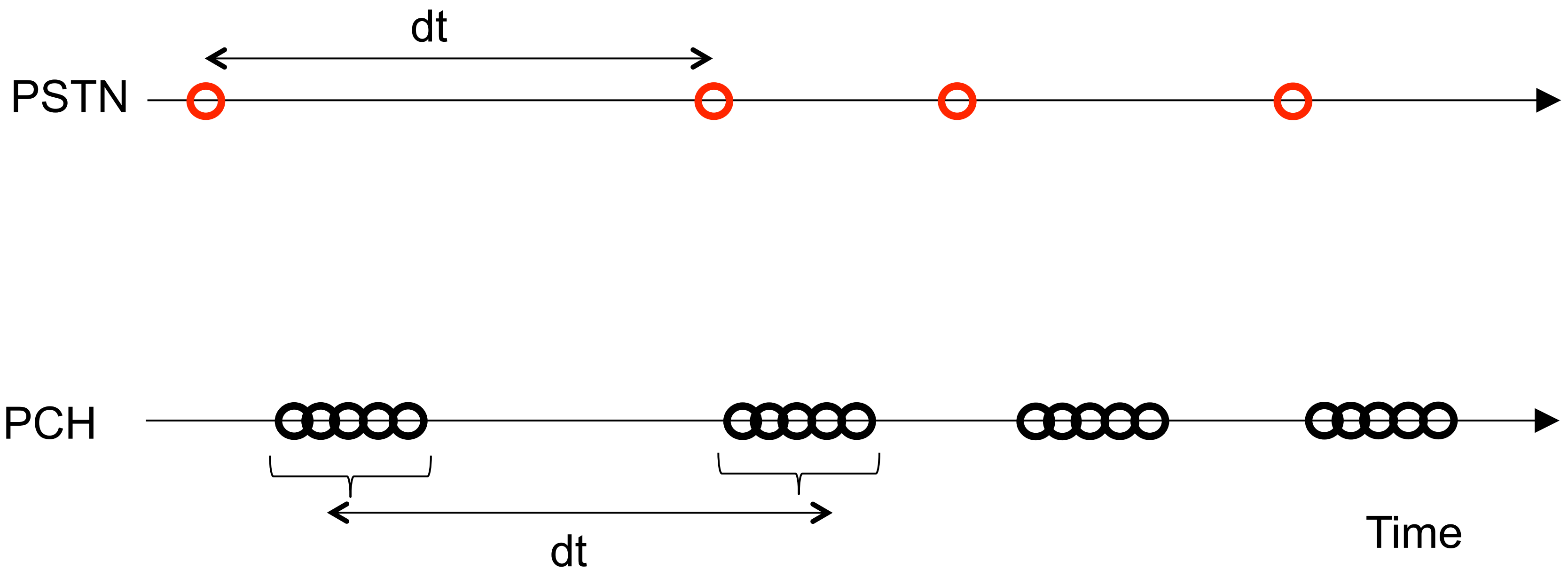
Low traffic after midnight

- University campus
- Day of the week during the semester

Phone number-TMSI mapping

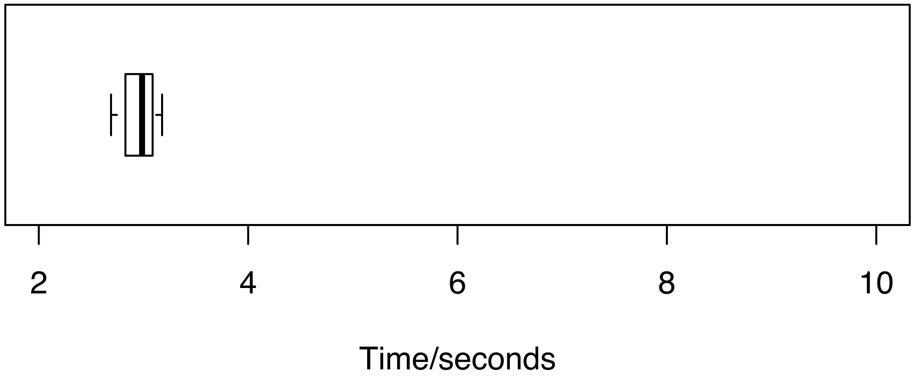


No recovered TMSI

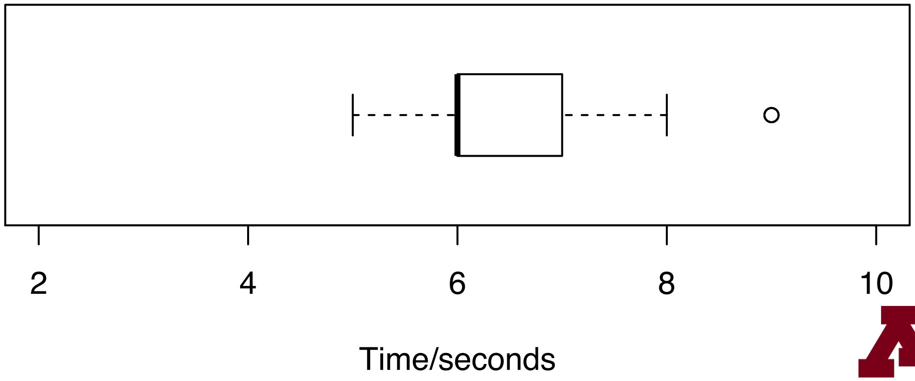


Silent paging

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



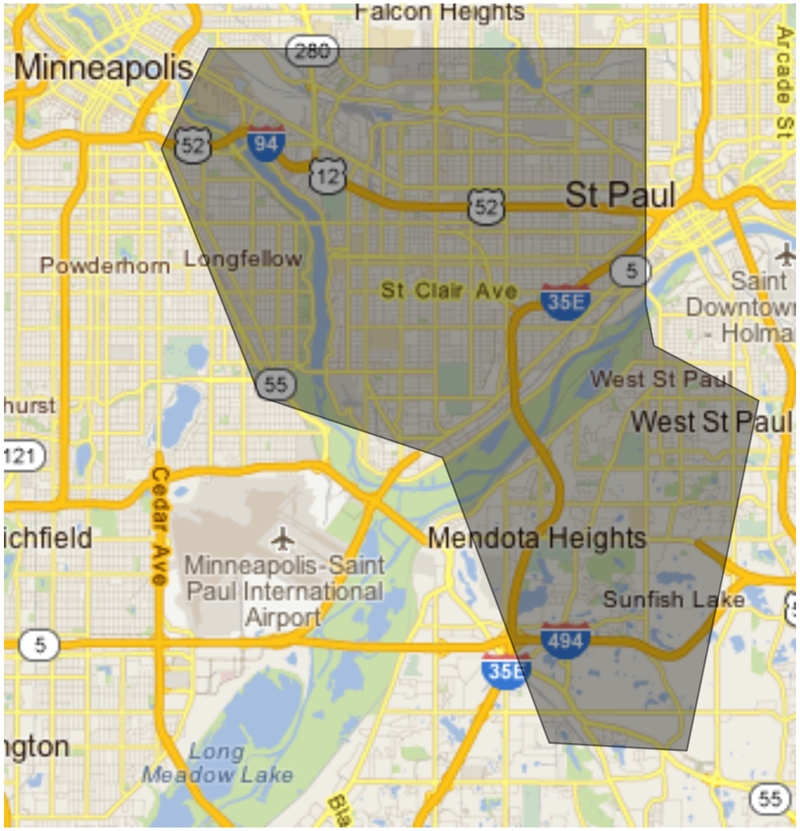
- Median delay between call initiation and ring
  - 6 seconds



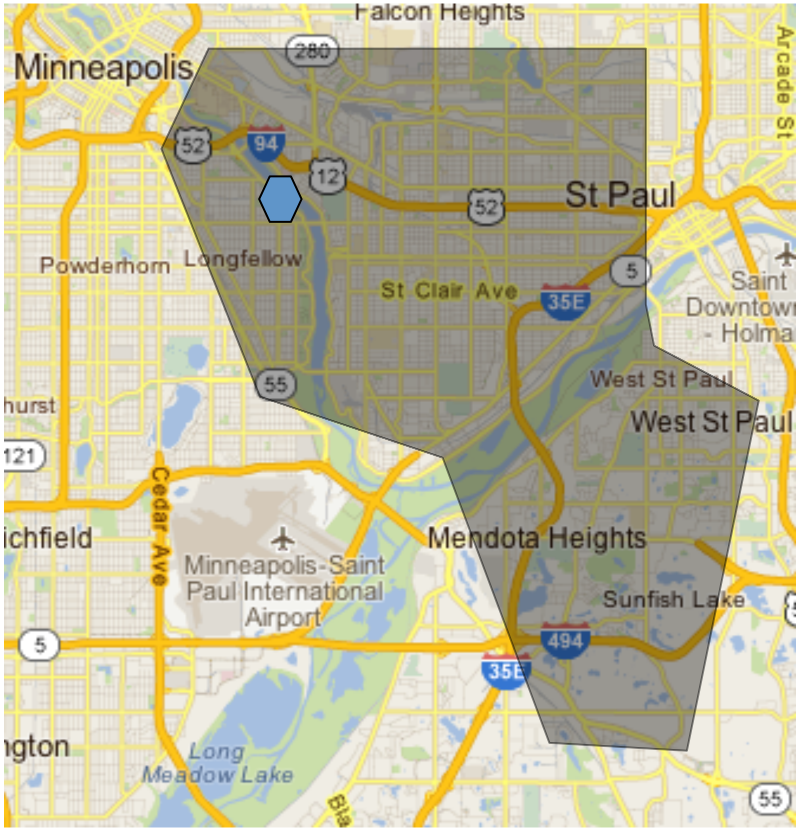
Bounding the LAC

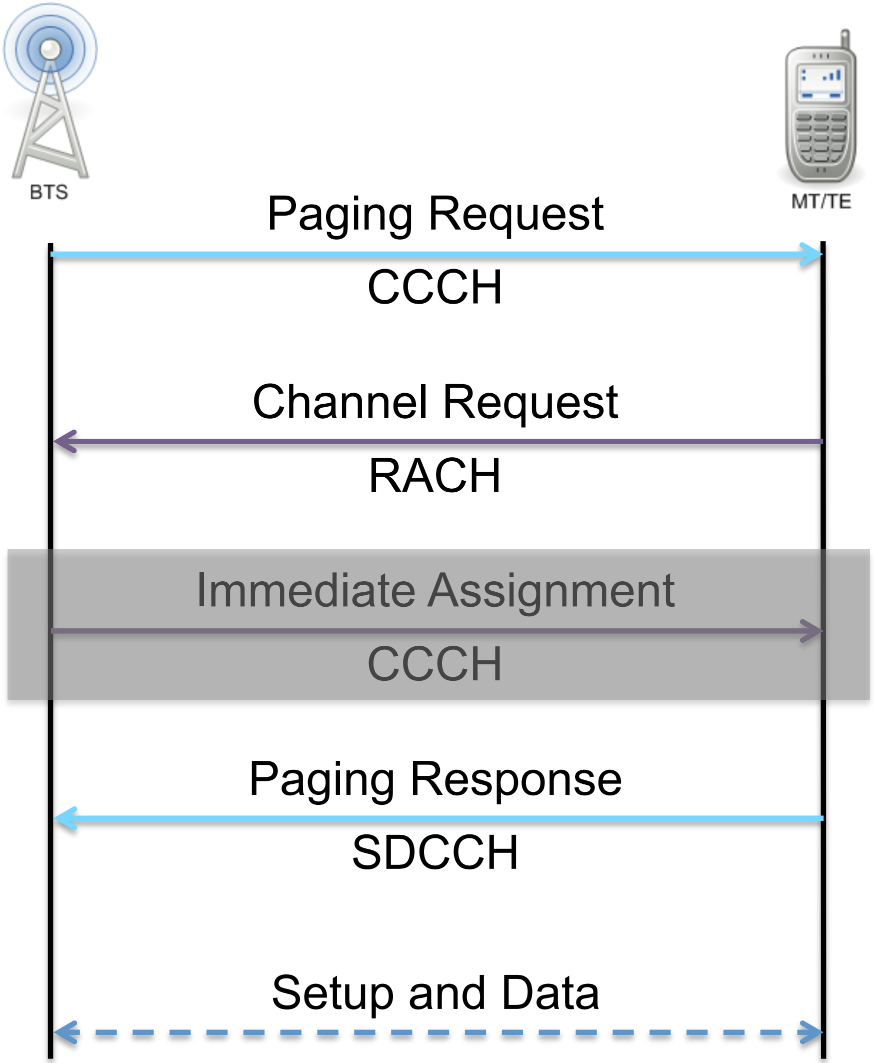
- LACs can be very large.
  - T-Mobile LAC 747d: 100km^2
- Used a wall-following algorithm, road permitting.

- 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

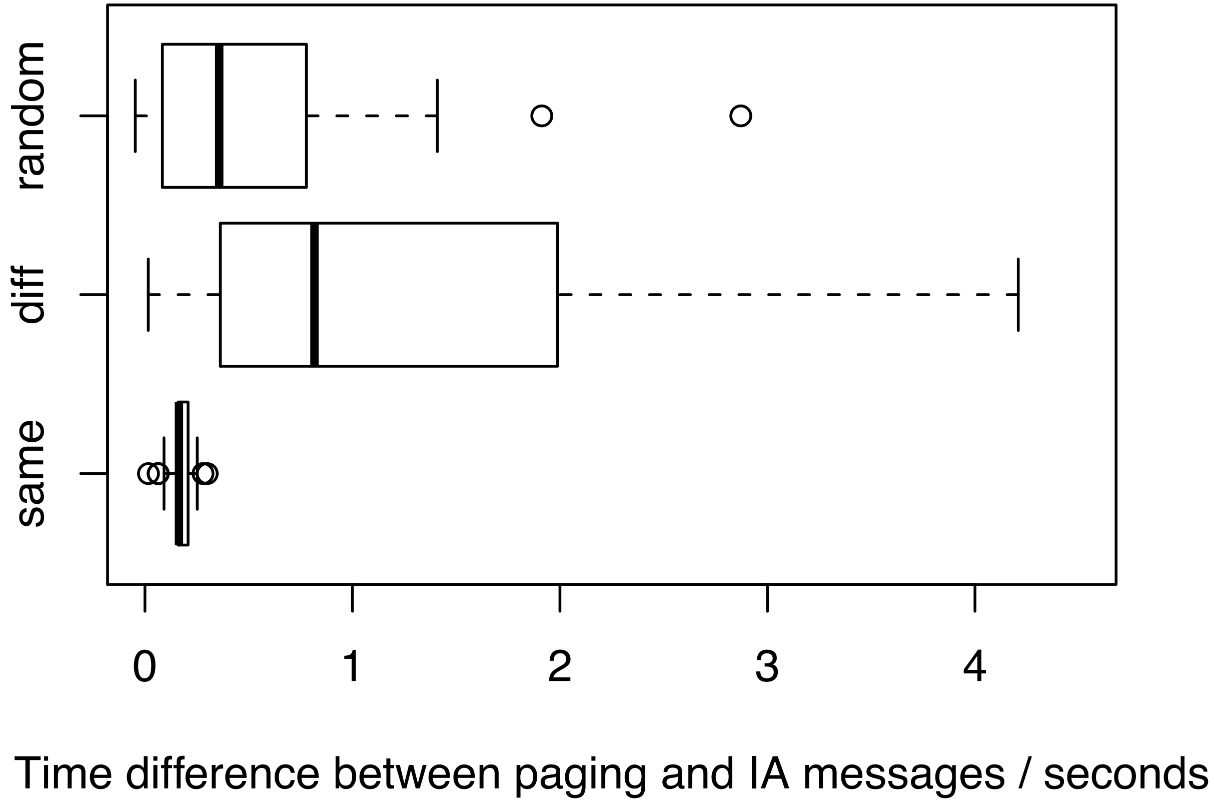
Paging Response

SDCCH

Setup and Data

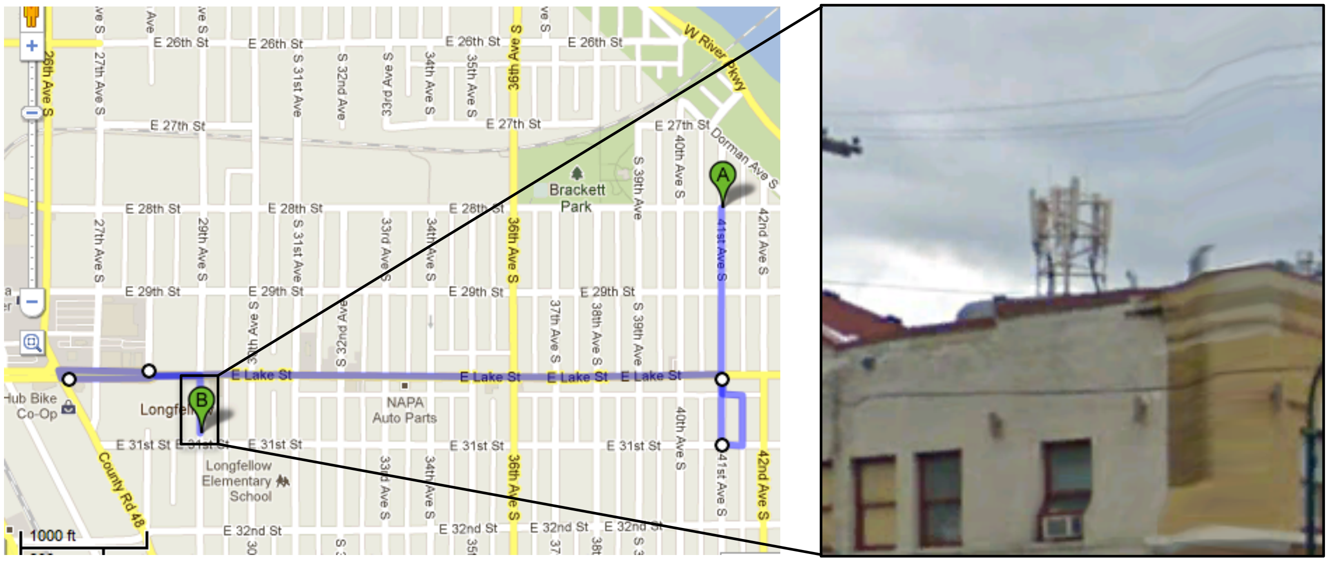
Same tower test

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

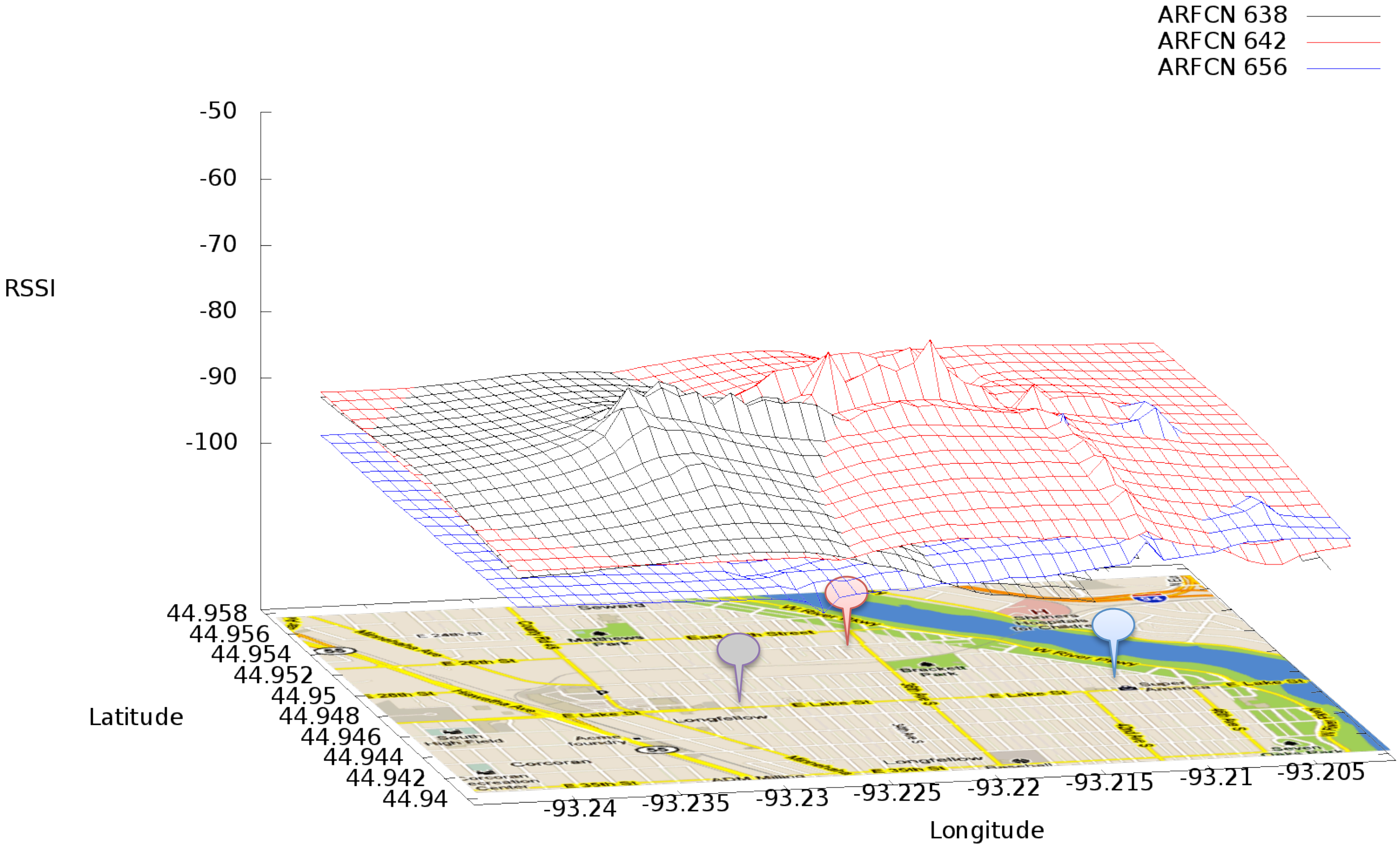


Finding individual towers

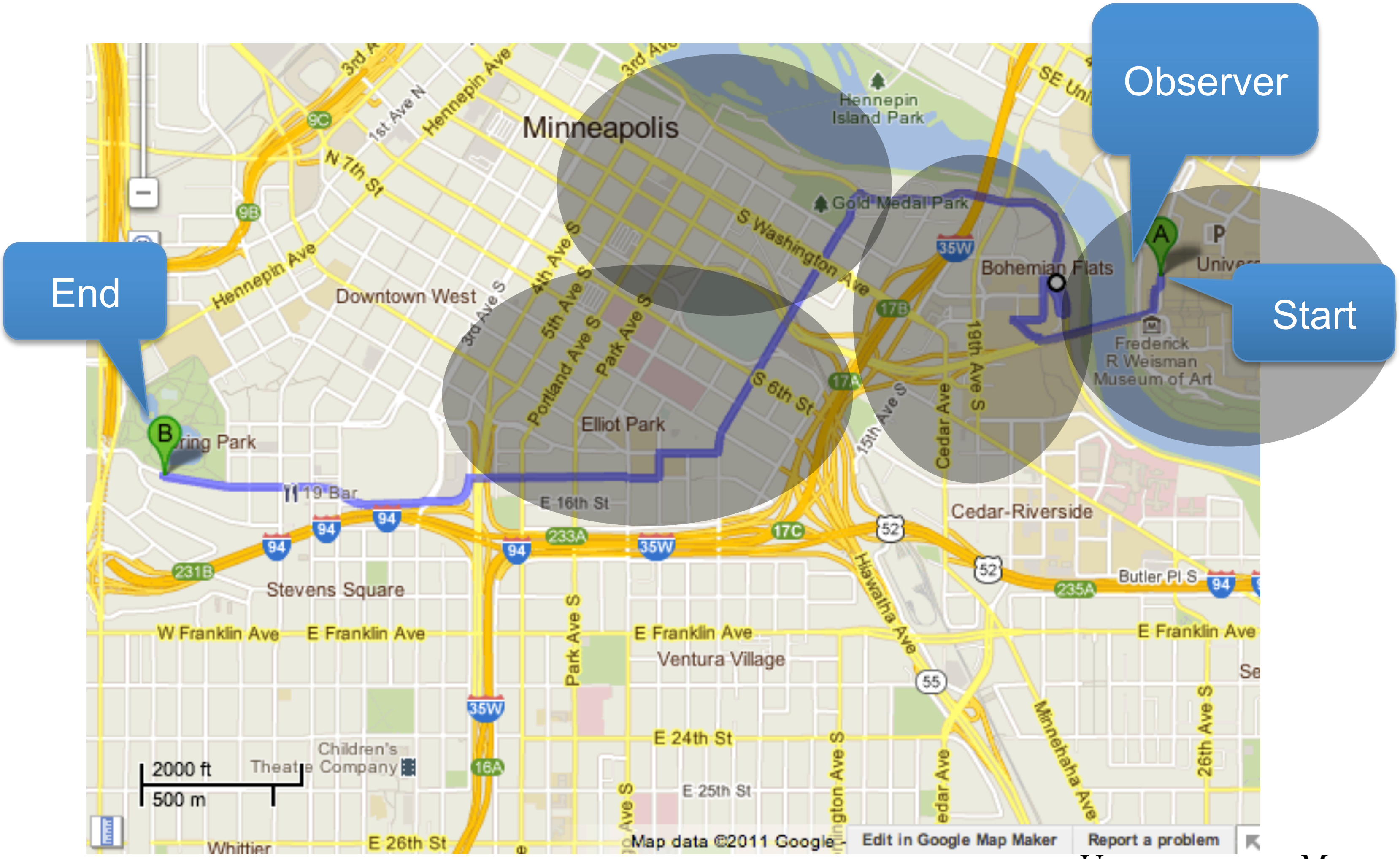
- Find individual towers with a hill-climbing algorithm.
  - Non-uniform RF attenuation.
  - Overshoot by 50m to avoid local maximum.



ARFCN a phone is likely to camp on



Tracking users in motion



Observer

Start

End

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.

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

Thank you

- Questions