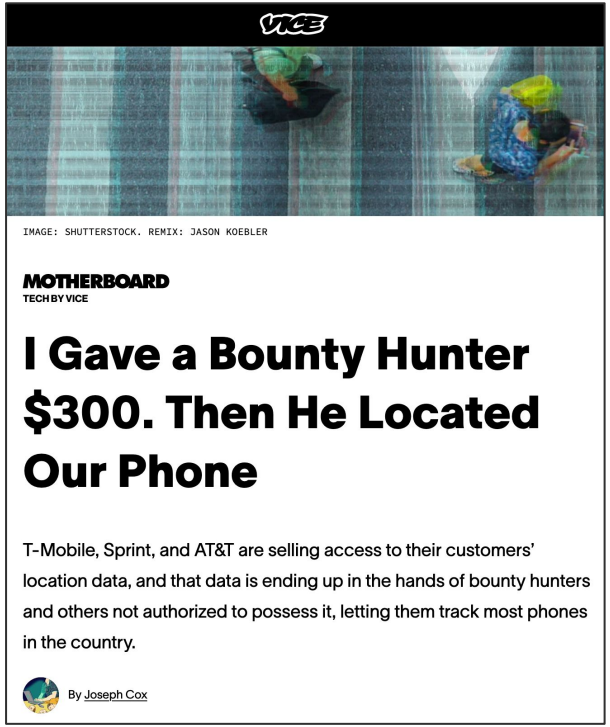
Pretty Good Phone Privacy (PGPP)

Paul Schmitt
Princeton

Barath Raghavan
USC

Cellular Location Privacy

- Phones are location tracking devices in disguise
- Carriers sell customers' data to data brokers
- Data brokers sell user data to anyone
- Towers need to talk to phones; impossible to prevent?



VICE

IMAGE: SHUTTERSTOCK. REMIX: JASON KOEBLER

MOTHERBOARD
TECH BY VICE

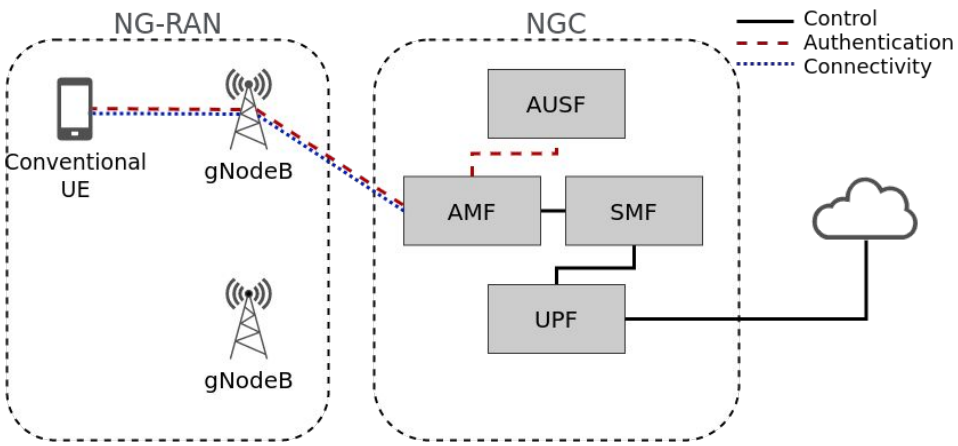
I Gave a Bounty Hunter $300. Then He Located Our Phone

T-Mobile, Sprint, and AT&T are selling access to their customers' location data, and that data is ending up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country.

By Joseph Cox

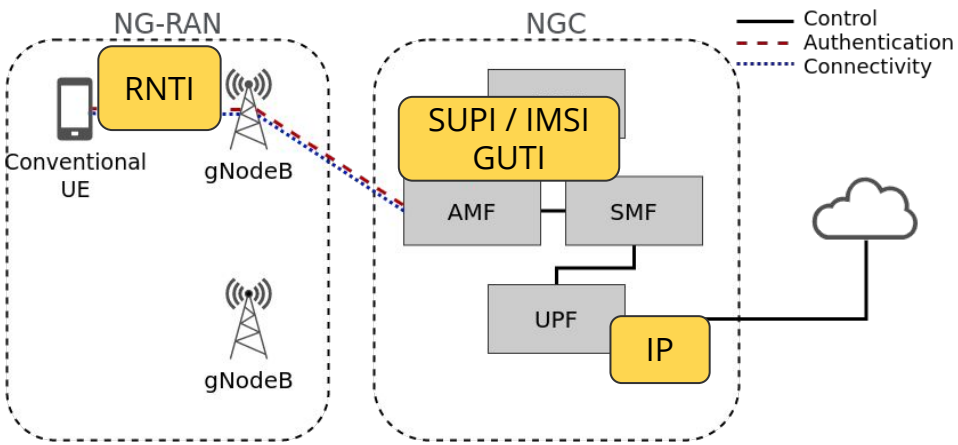
Cellular Identities

- SUPI (Subscription Permanent Identifier) / IMSI (International Mobile Subscriber Identity):
  - Permanent identity held in SIM
  - Globally unique
- GUTI - Globally Unique Temporary Identity
  - Temporary replacement for SUPI / IMSI
- IP Address
  - Dynamically assigned by the core
- RNTI - Radio Network Temporary Identifier
  - Dynamic identifier for over-the-air



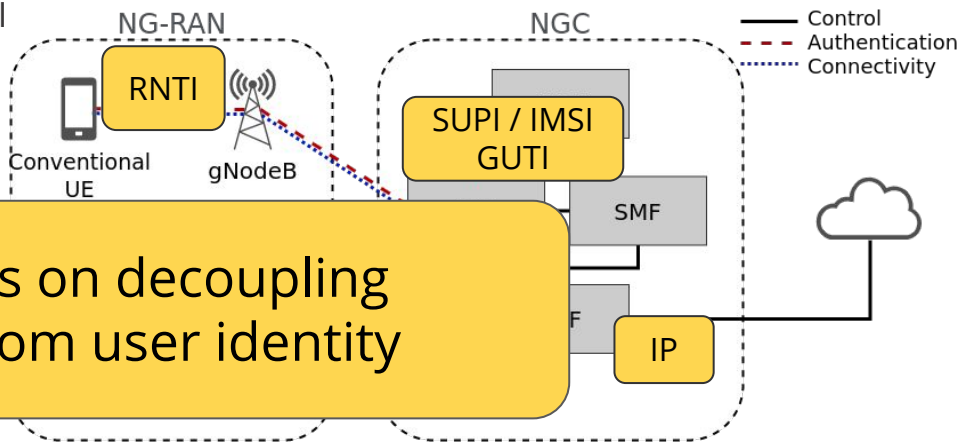
Cellular Identities

- SUPI (Subscription Permanent Identifier) / IMSI (International Mobile Subscriber Identity):
  - Permanent identity held in SIM
  - Globally unique
- GUTI - Globally Unique Temporary Identity
  - Temporary replacement for SUPI / IMSI
- IP Address
  - Dynamically assigned by the core
- RNTI - Radio Network Temporary Identifier
  - Dynamic identifier for over-the-air



Cellular Identities

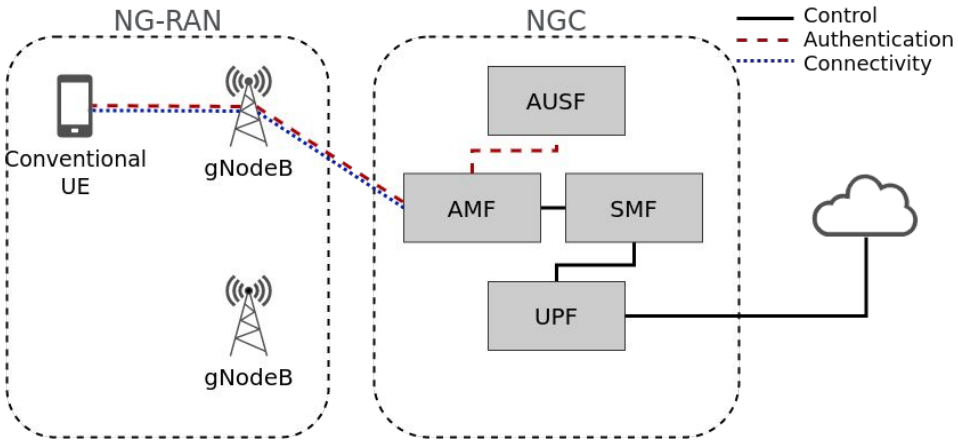
- SUPI (Subscription Permanent Identifier) / IMSI (International Mobile Subscriber Identity):
  - Permanent identity held in SIM
  - Globally unique
- GUTI - Globally
  - Temporar
- IP Address
  - Dynamical
- RNTI - Radio Network Temporary Identifier
  - Dynamic identifier for over-the-air



PGPP focuses on decoupling SUPI / IMSI from user identity

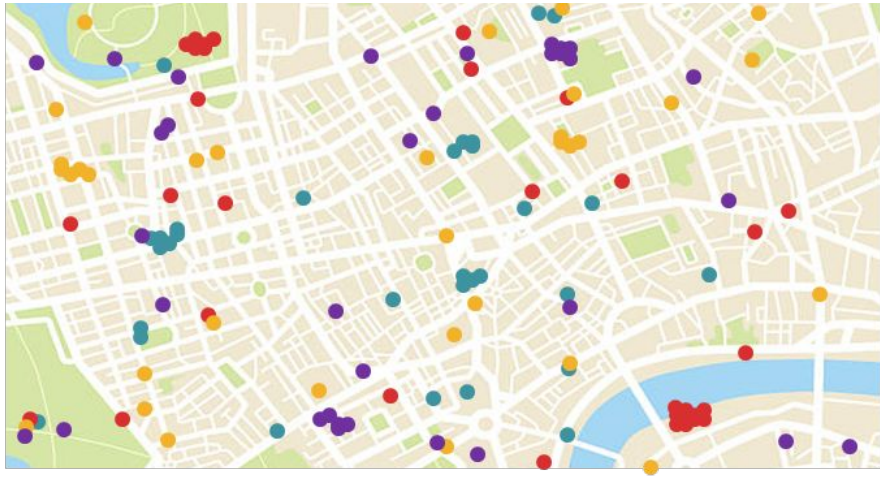
Conventional Cellular

- Connectivity, billing, and authentication use same credentials (SUPI / IMSI)
- Design was based on trust of all parties
- 5G makes things worse!



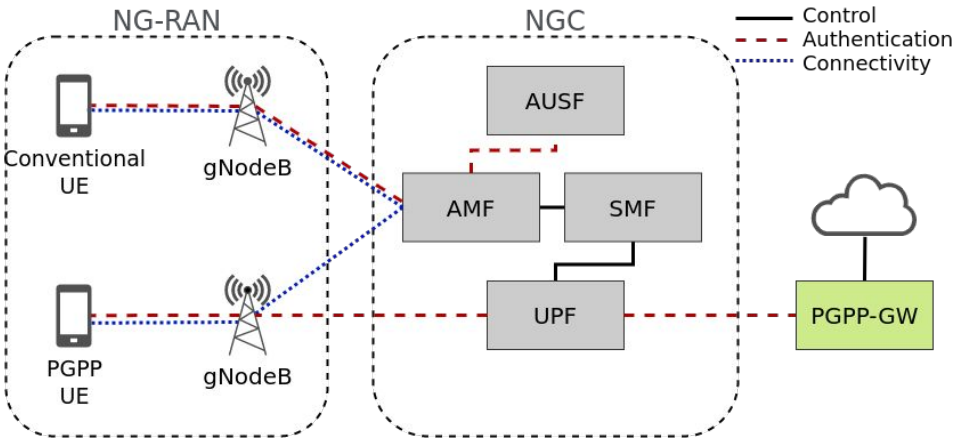
Bulk Attacks

- SUPI / IMSI can be used to identify individuals throughout network
- IMSI catchers (e.g., Stingray)
- SDRs
- Carrier logs
- Government surveillance

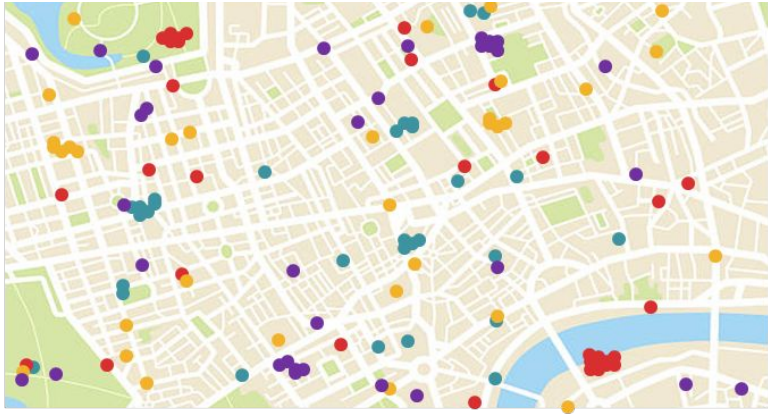


Pretty Good Phone Privacy (PGPP)

- Goal: remove trust from carrier *itself*
- Decouples connectivity from authentication and billing
- Bulk (passive) attacks:
  - Nullify IMSI - identical values
  - Oblivious authentication



Bulk Attacks

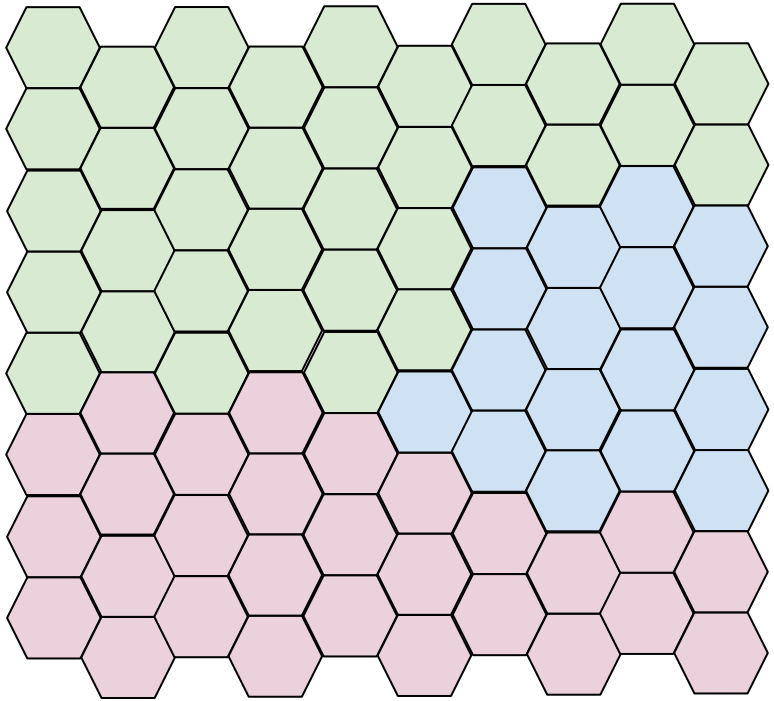


Users as seen today
are <u>identifiable</u>

Users with PGPP
are <u>indistinguishable</u>

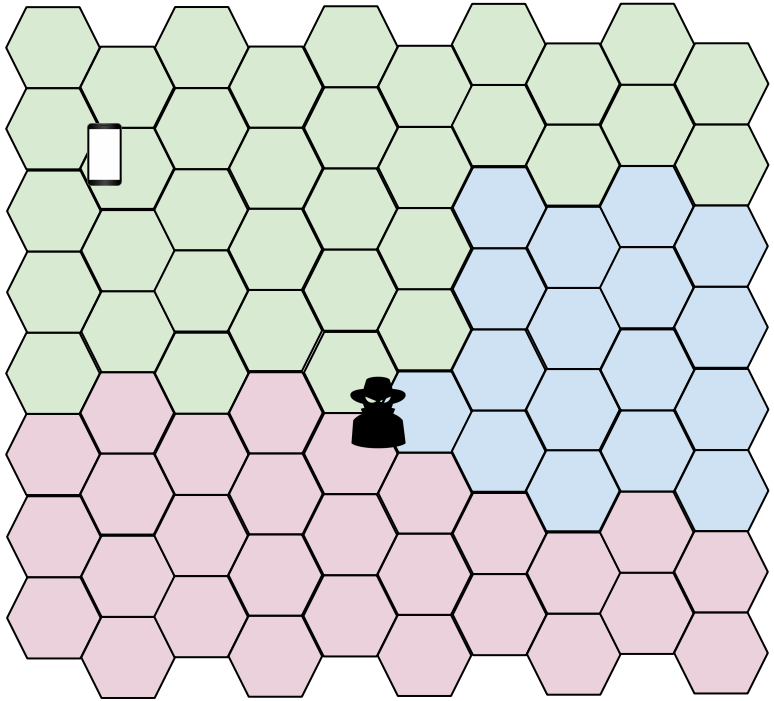
Active Attacks - Paging

- Tracking areas - carrier's perspective
  - Minimize mobility control overhead
- In idle mode, network doesn't know where UE is actually located
  - Page entire tracking area for incoming call or data
- Attack:
  - Call / FB / Whatsapp



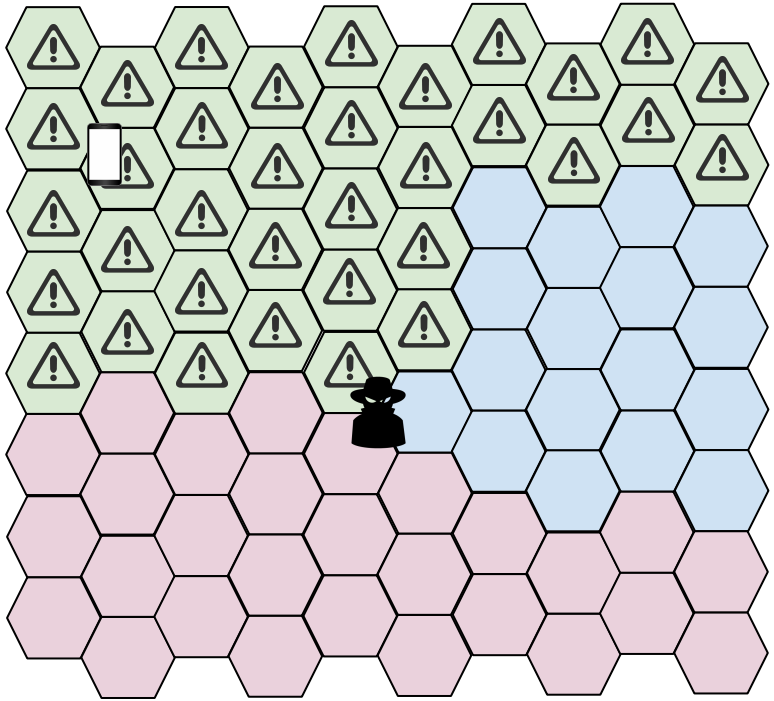
Active Attacks - Paging

- Tracking areas - carrier's perspective
  - Minimize mobility control overhead
- In idle mode, network doesn't know where UE is actually located
  - Page entire tracking area for incoming call or data
- Attack:
  - Call / FB / Whatsapp



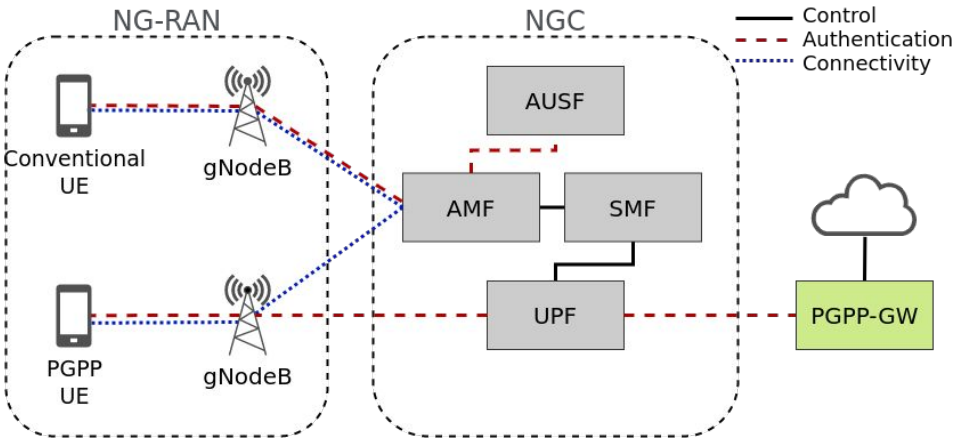
Active Attacks - Paging

- Tracking areas - carrier's perspective
  - Minimize mobility control overhead
- In idle mode, network doesn't know where UE is actually located
  - Page entire tracking area for incoming call or data
- Attack:
  - Call / FB / Whatsapp



Pretty Good Phone Privacy (PGPP)

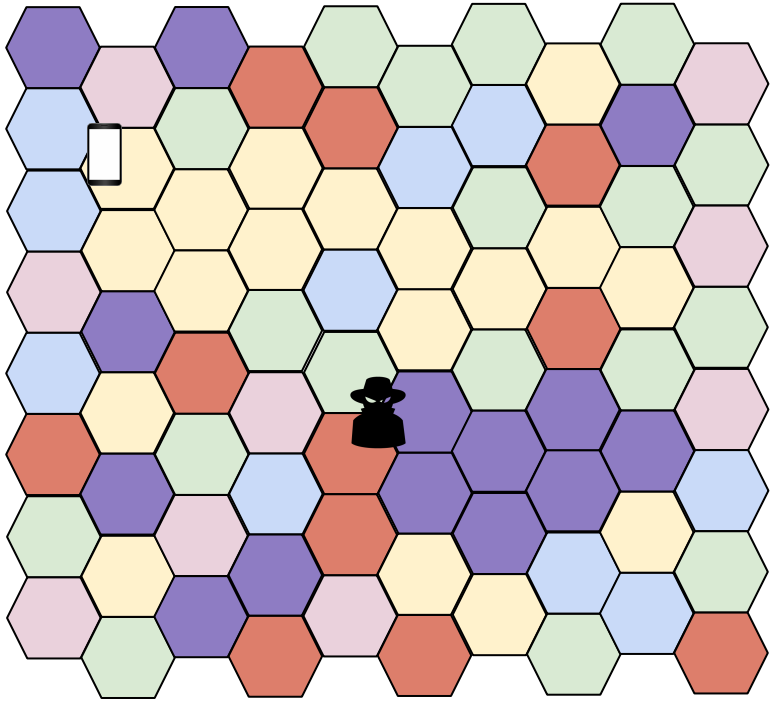
- Goal: remove trust from carrier *itself*
- Decouples connectivity from authentication and billing
- Bulk (passive) attacks:
  - Nullify IMSI - identical values
  - Oblivious authentication
- Active attacks:
  - Randomize and increase broadcast domain



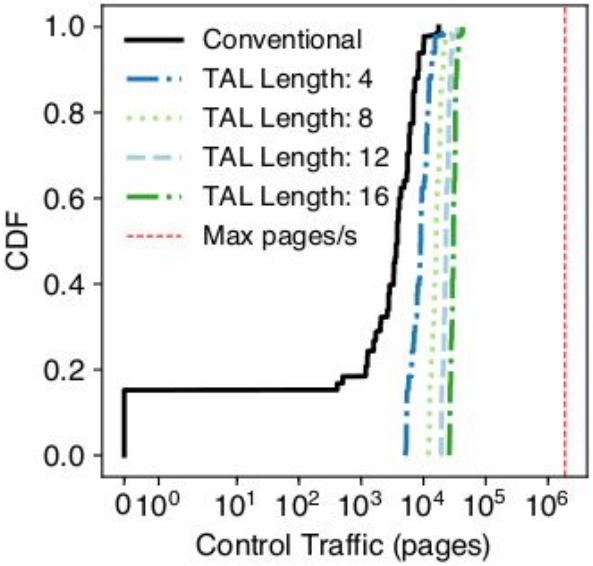
Paging Attacks - Custom Tracking Area Lists

- Tracking area lists
  - Bottom-up (UE perspective) view of the network
  - Randomized for each UE

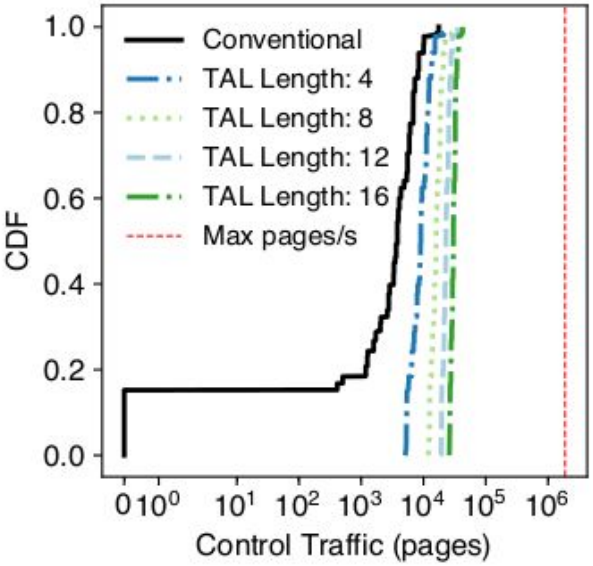
- Exchange mobility update overhead for location anonymity
  - More tracking area boundaries

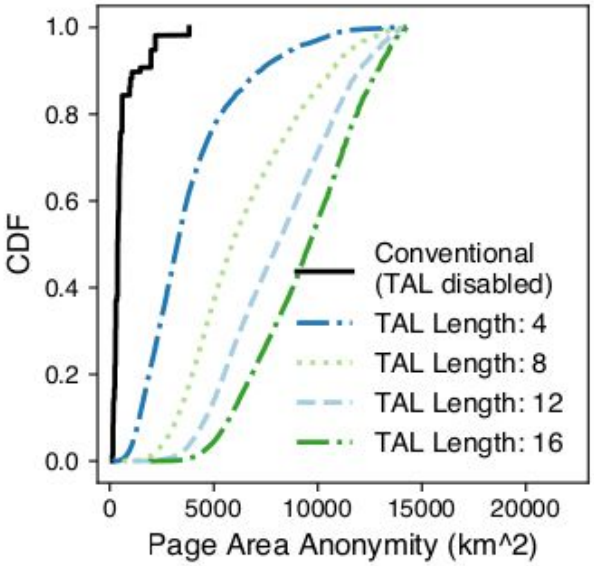


PGPP Trades Control Traffic for Anonymity

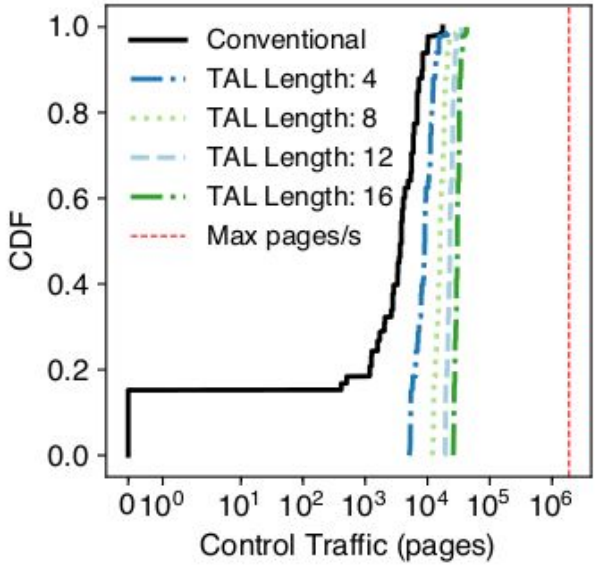


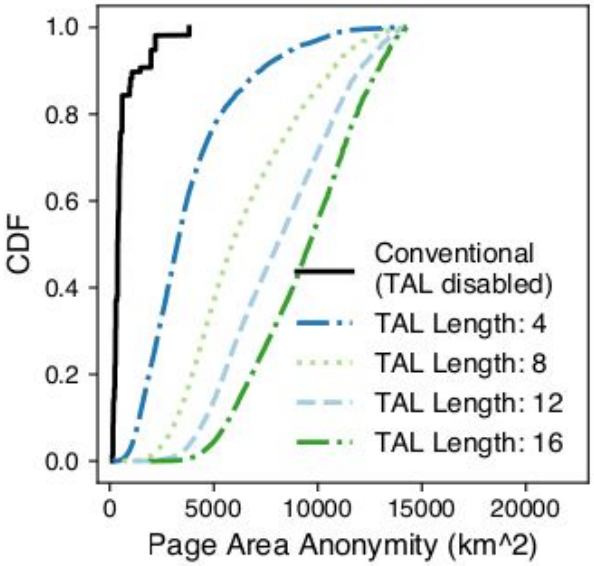
PGPP Trades Control Traffic for Anonymity

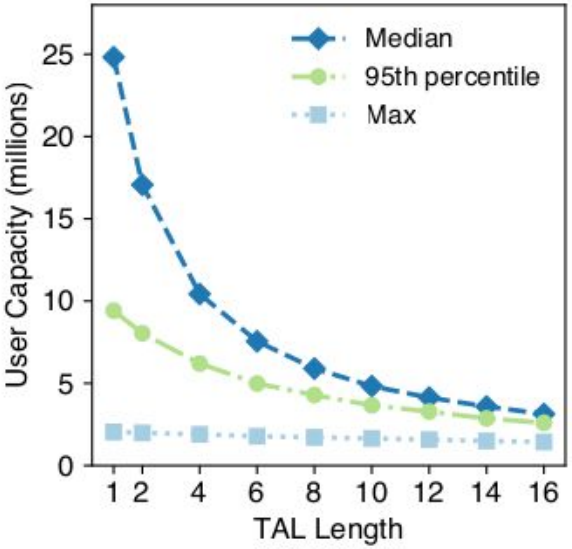




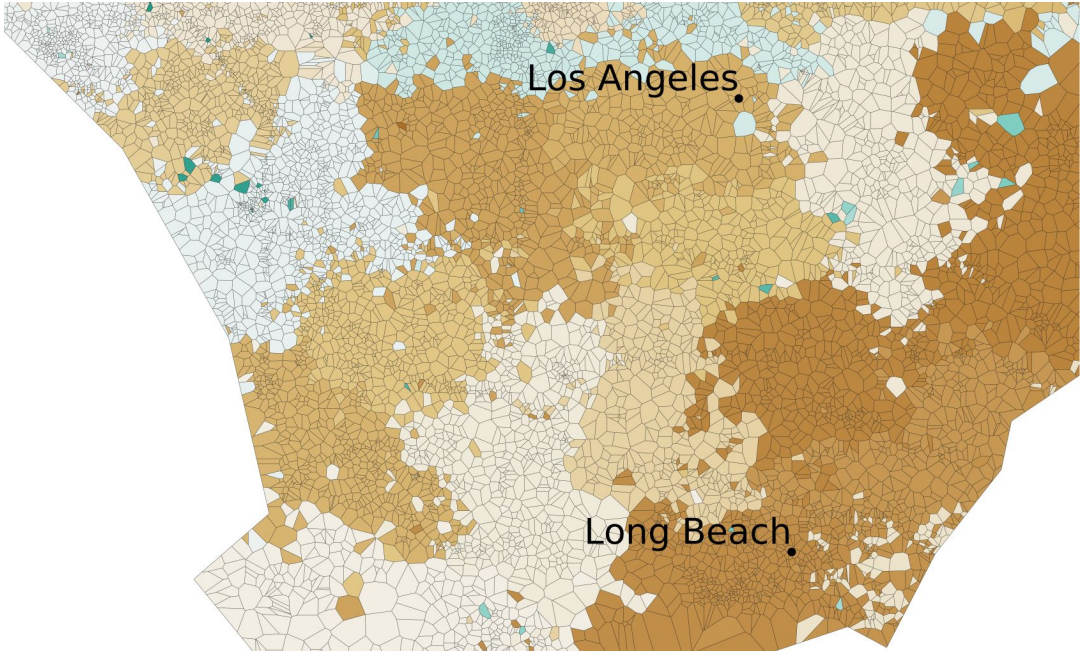
PGPP Trades Control Traffic for Anonymity



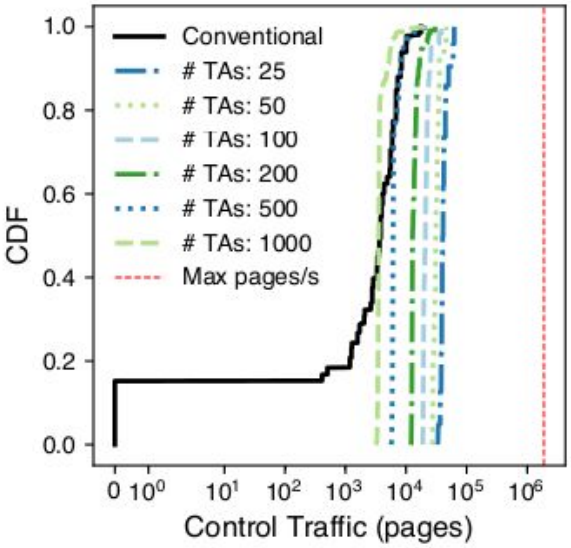




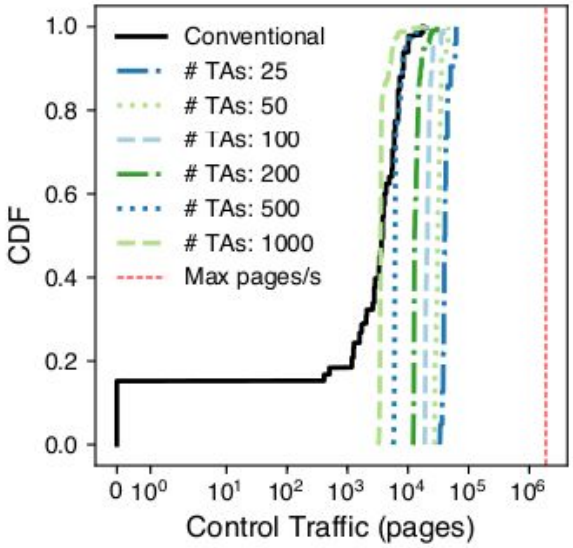
Control Traffic Managed by Changing the Map

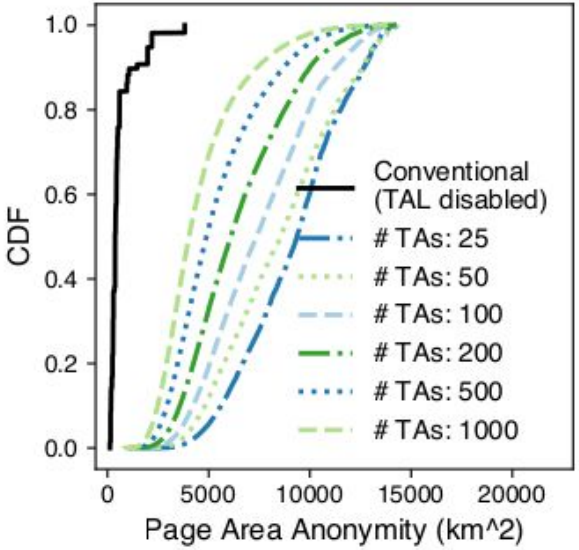


Control Traffic Managed by Changing the Map

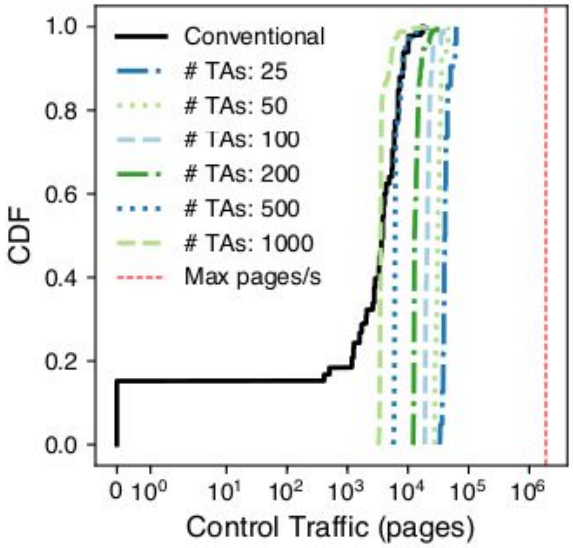


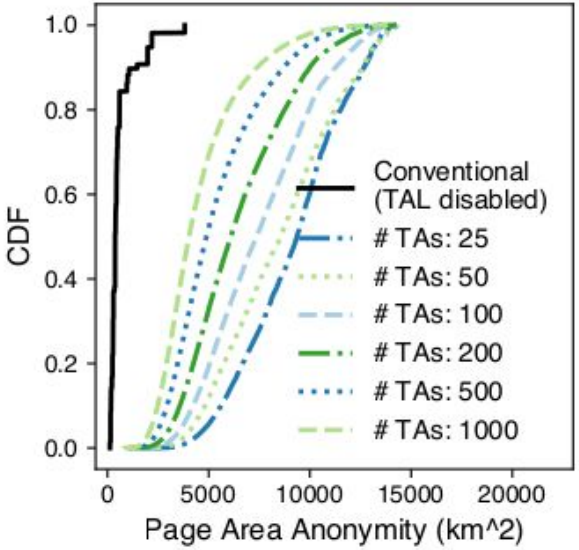
Control Traffic Managed by Changing the Map

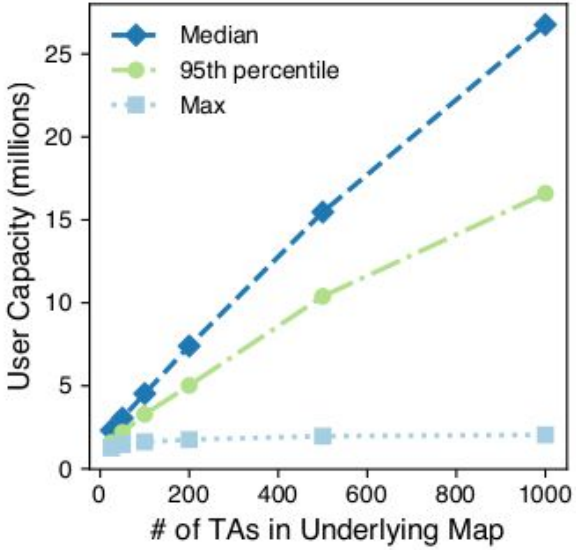




Control Traffic Managed by Changing the Map







Thank you!

Paul Schmitt
pschmitt@cs.princeton.edu