A Measurement Driven Approach to Detecting Surveillance on Cellular Networks

JARRETT HUDDLESTON, JASMINE FAN, ALEX MARDER

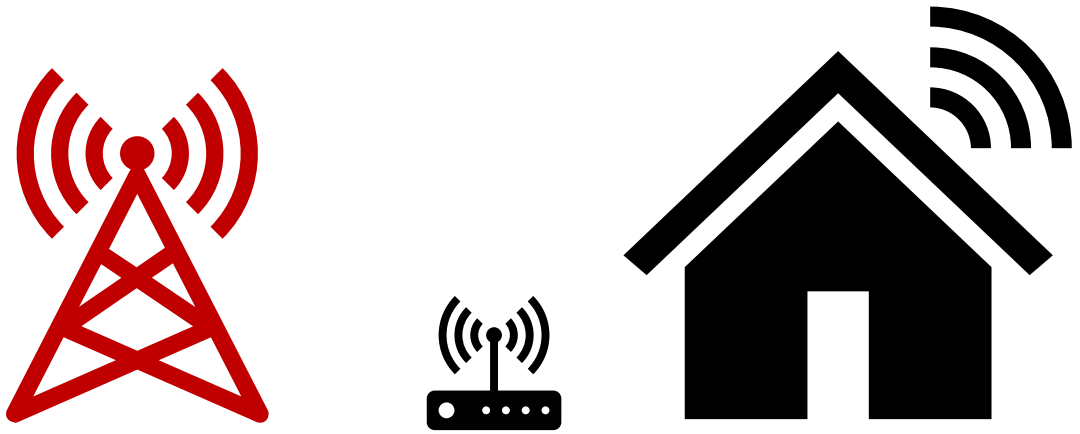
AIMS 19

Introduction

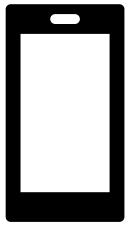
- My lab (JHU NETS) working on a DARPA funded research grant to identify attacks against 5G infrastructure
- Our aim is to make as few assumptions about an attacker as possible
  - We just want to identify when something is abnormal
- I'm leading a project to detect IMSI-Catcher style attacks using Software Defined Radios (SDR)
  - Ultimate goal is to make a system/tool that can be deployed anywhere

Imagine this scenario

- Suppose you have a mostly static, private network overseas
  - Forward operating base
  - NGO operation
- Another party may want to listen in
  - IMSI-Catcher/Stingray
- Our system could catch them



5G Connection Overview



Advertise MIB/SIB

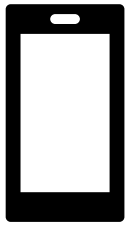
RACH Process

Register with IMSI/SUCI/SUPI

Authenticate

- UE receives broadcast of cell information
- UE Initiates the RACH process
  - Agree on shared channel
- Registration
  - UE shares IMSI/SUPI/SUCI
- Authentication
  - cell sends Auth request
  - UE sends Auth response

What if the Cell is lying?



Advertise MIB/SIB

RACH Process

Register with IMSI/SUCI/SUPI

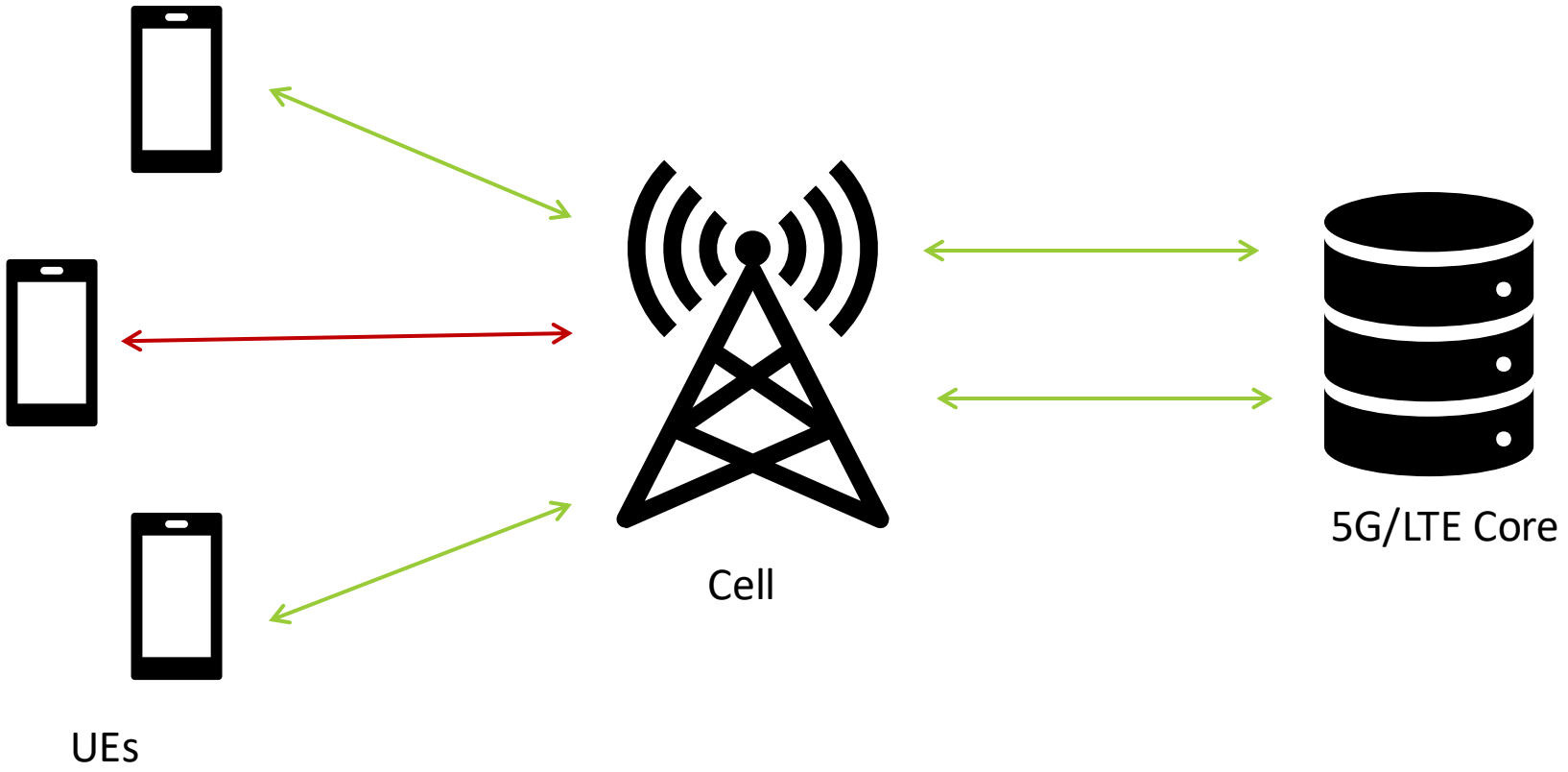
Authenticate (Fail)

- Base stations are fairly transparent
- Authentication fails without access to the core network
- Authentication fails after unique ID is sent

Our Detection Approach

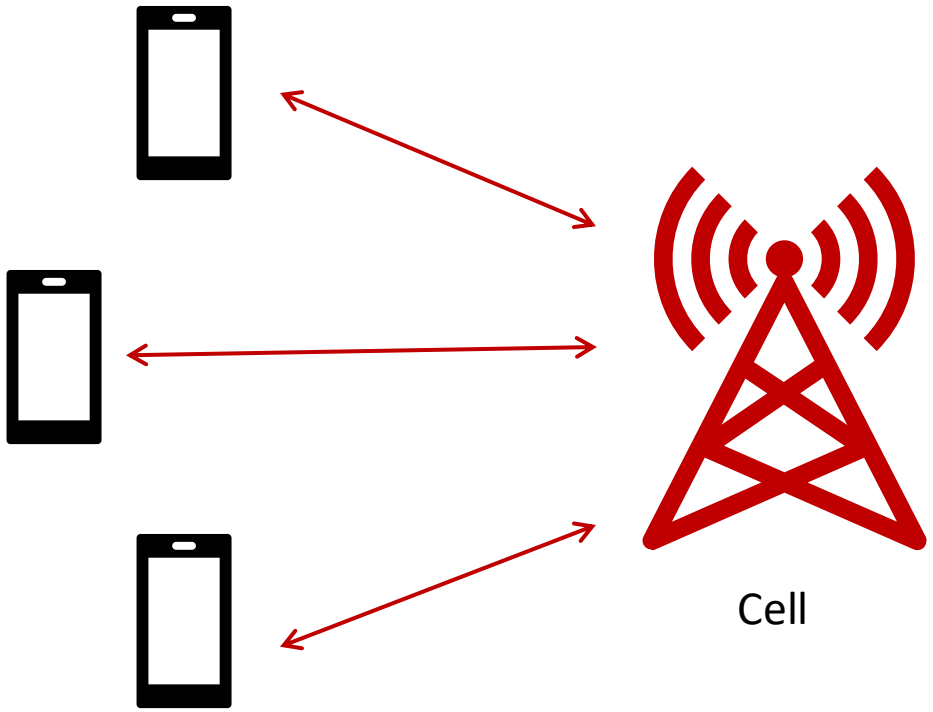
- Create a mobile measurement setup
- In any desired location, measure all visible 5G/LTE cells
  - NR-Scope (5G), NG-Scope (LTE)
- Variations from standard traffic could suggest suspicious behavior, even if not an IMSI Catcher
- We're interested in how much data is being transmitted

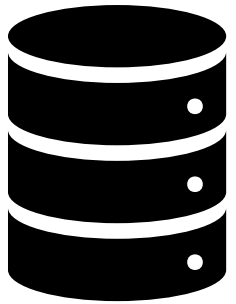
Why is data quantity useful?



- In a normal network, we expect at least some phones to connect
- Will see standard connection steps
- Plus data flowing to and from the core

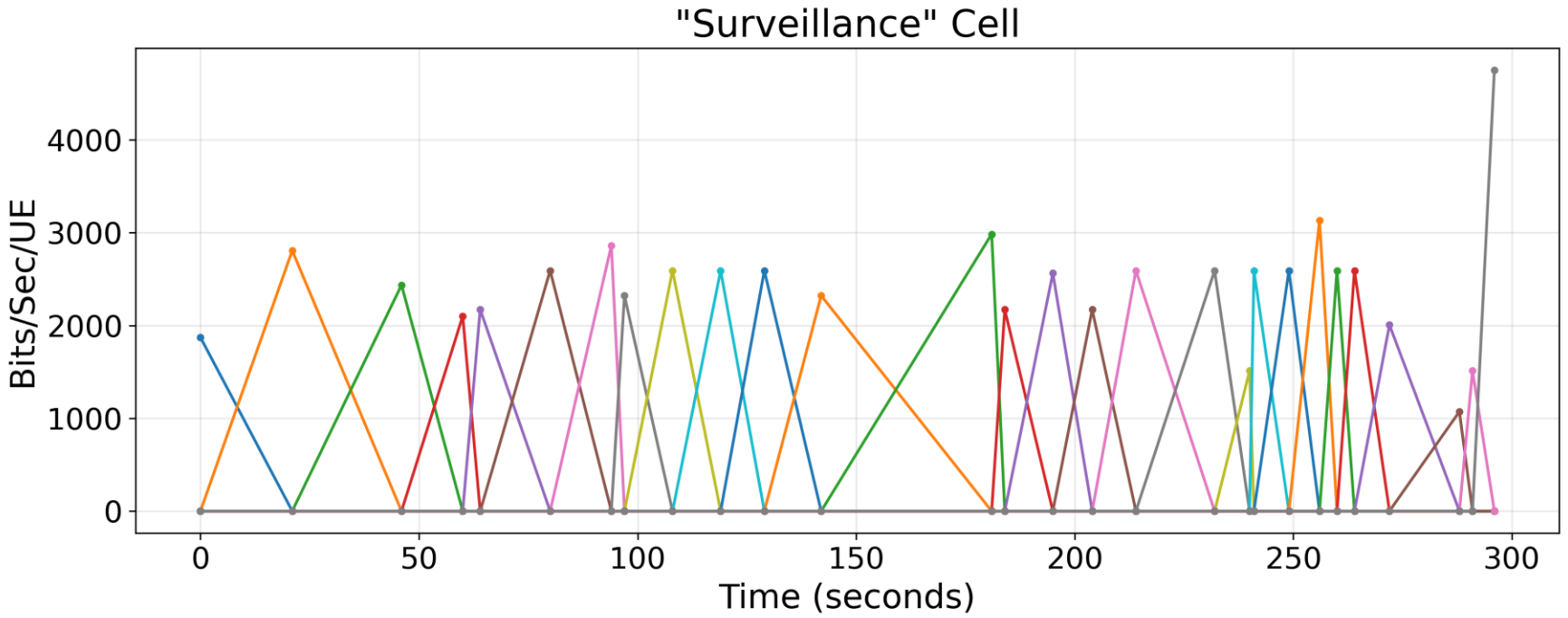
Why is data quantity useful?





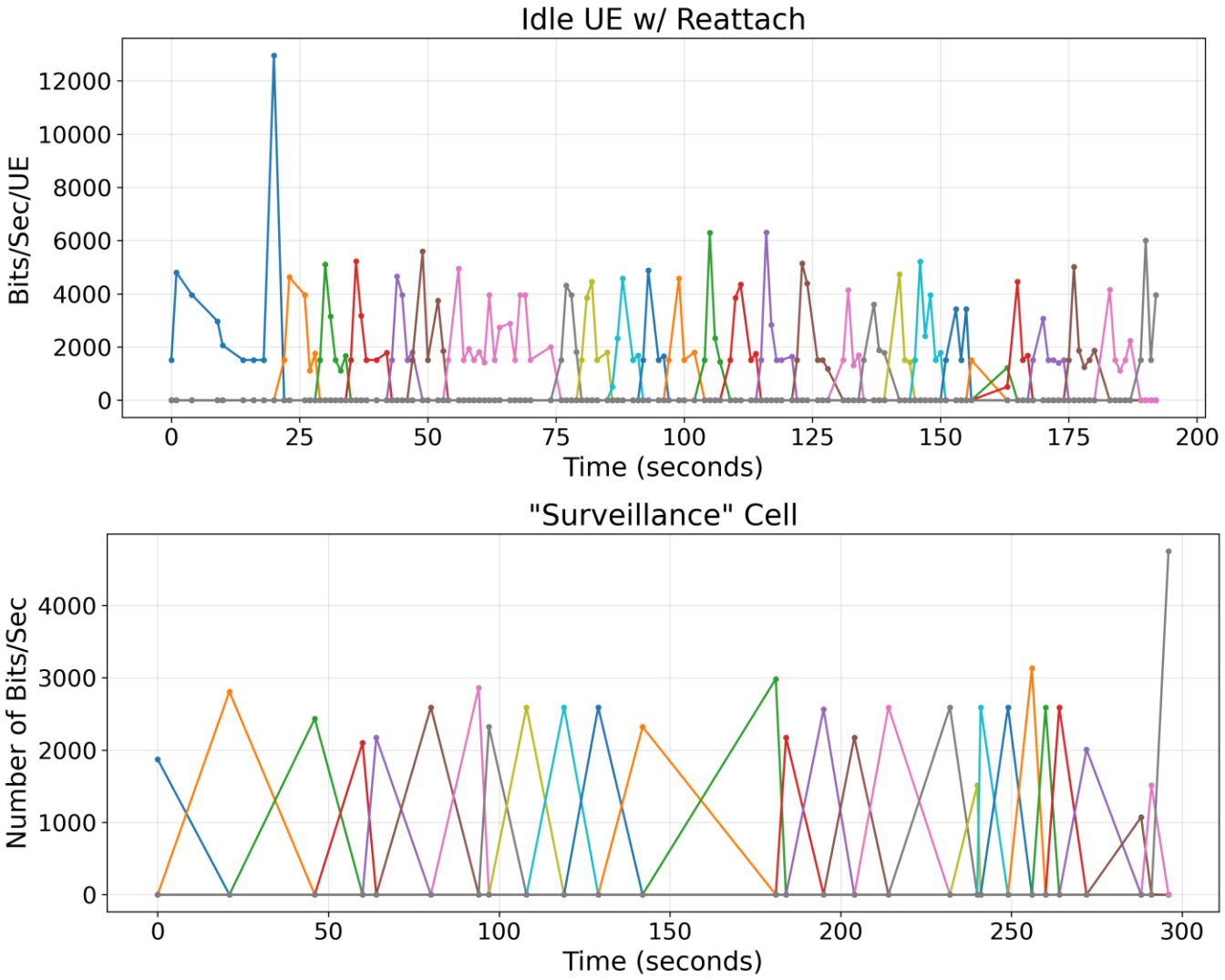
- When no phones can authenticate, no data to/from core
- Cells will schedule the connection process and nothing else

We can already see this in the lab

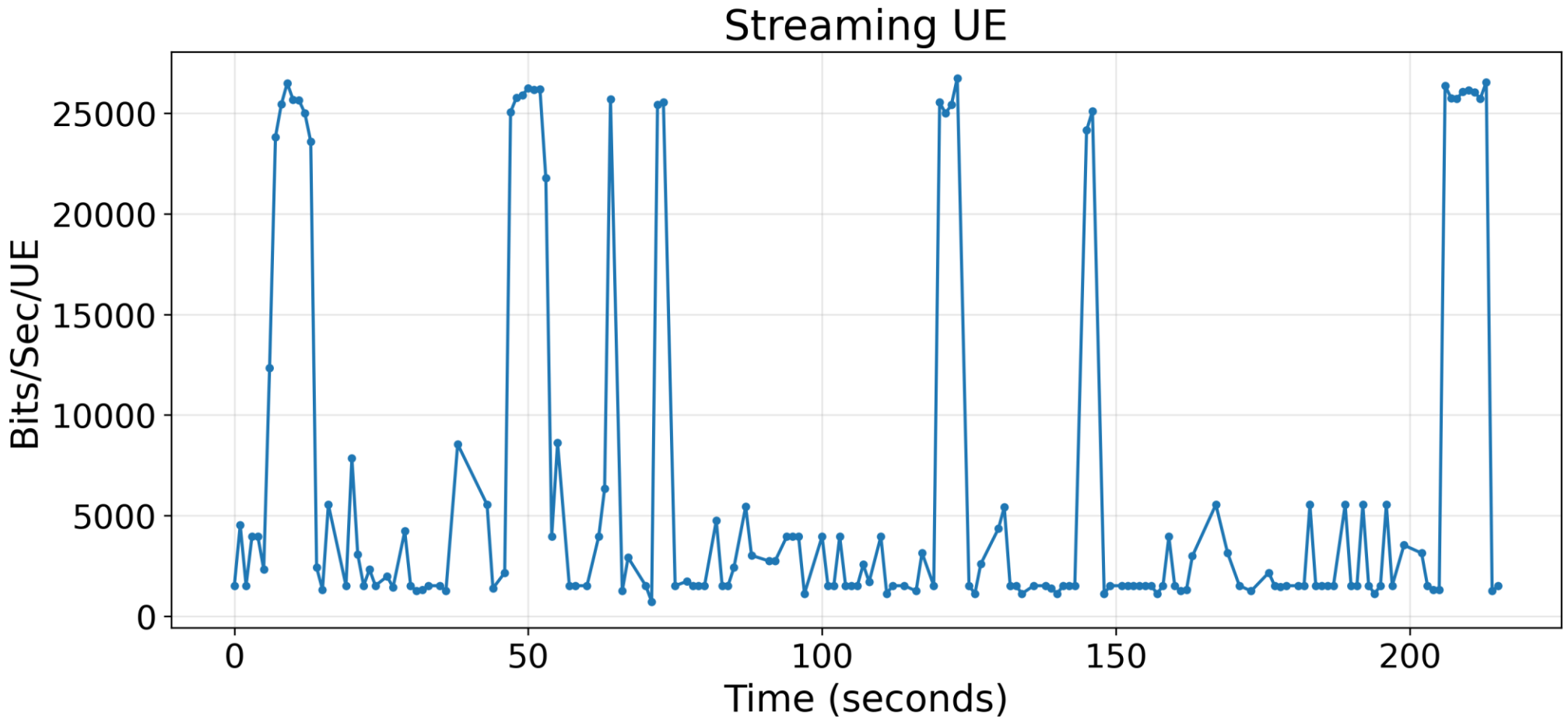


- Phones try to connect to cell but aren't allowed to
- Each color is a new UE connecting to the cell
- We use the number of bits allocated in each scheduling message

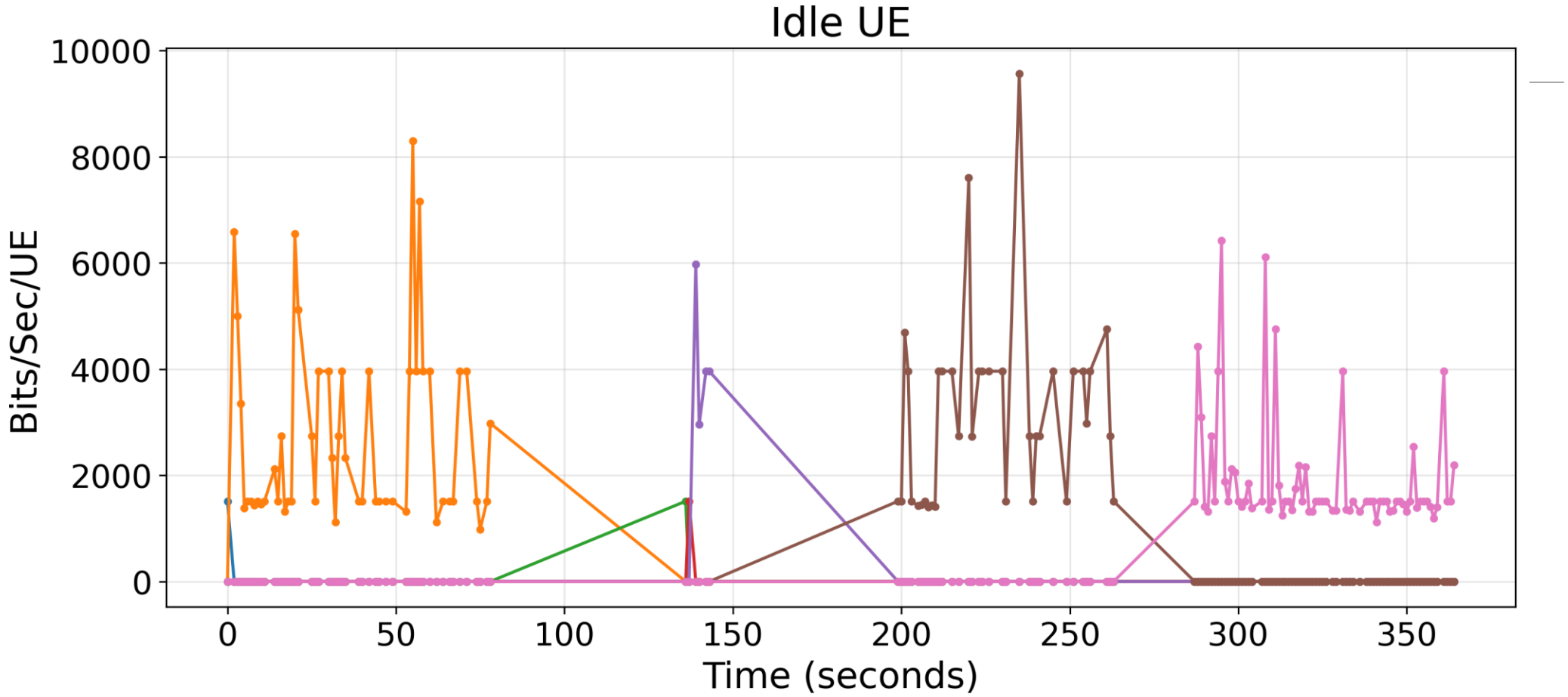
Why is amount of data useful?



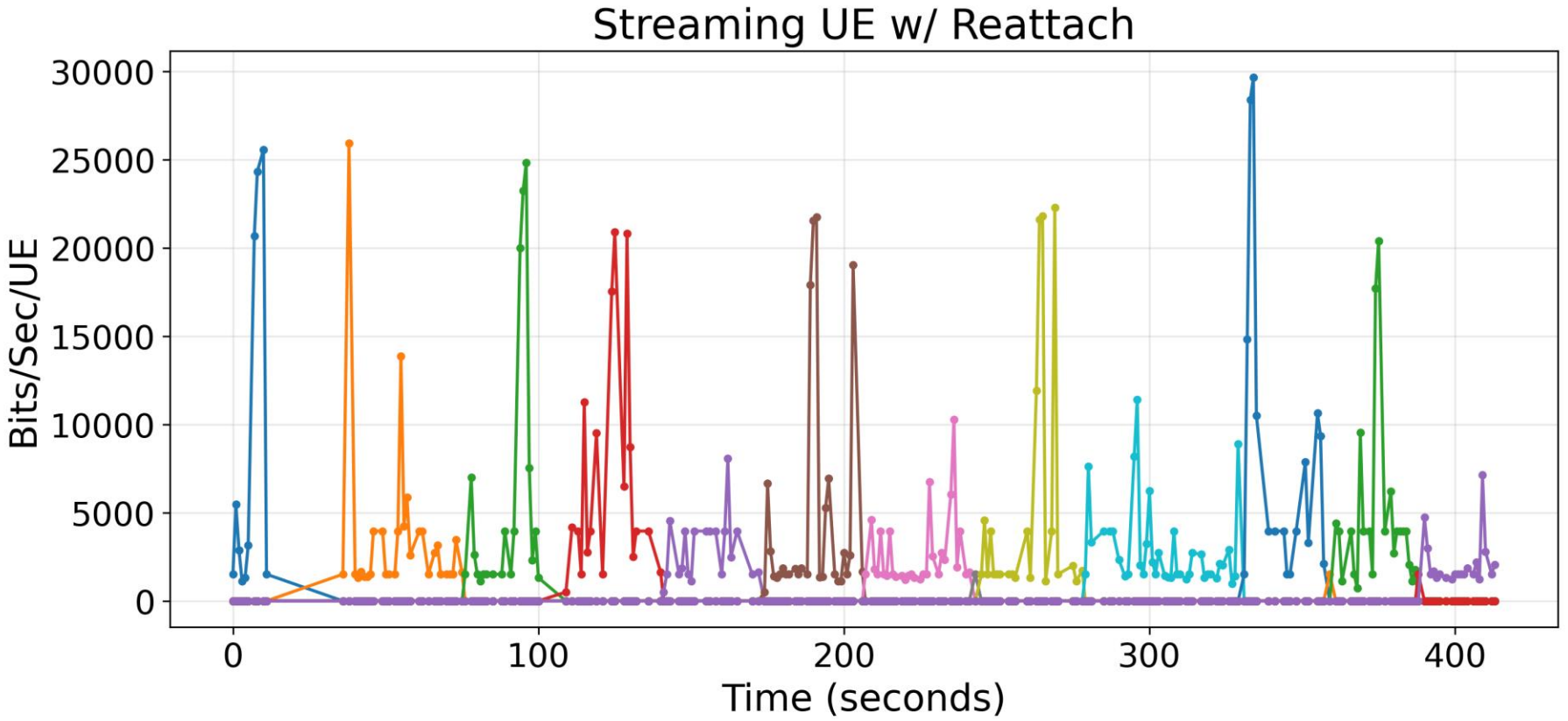
Phone Activity - Streaming



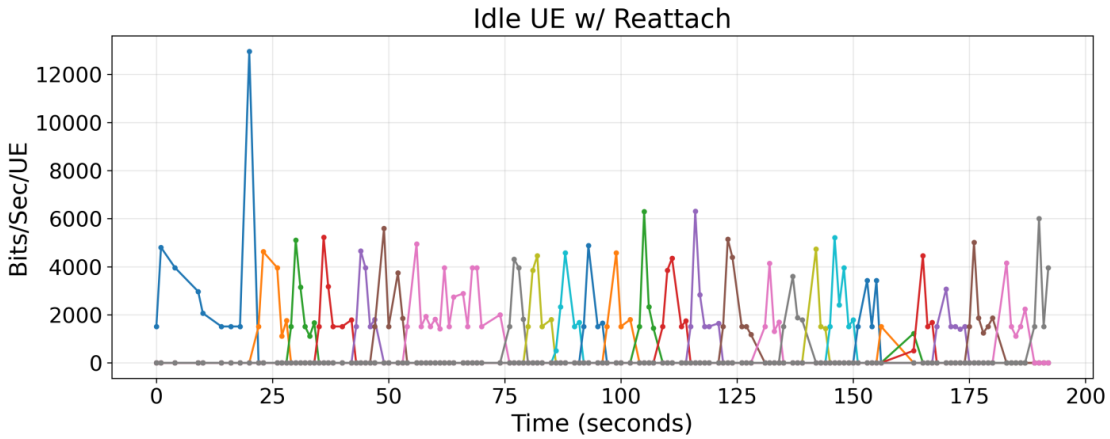
Phone Activity - Idle

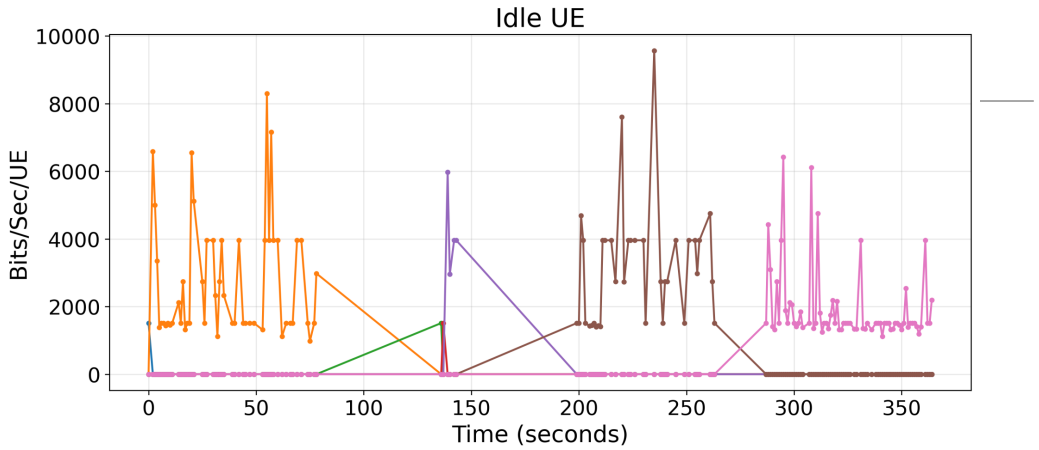


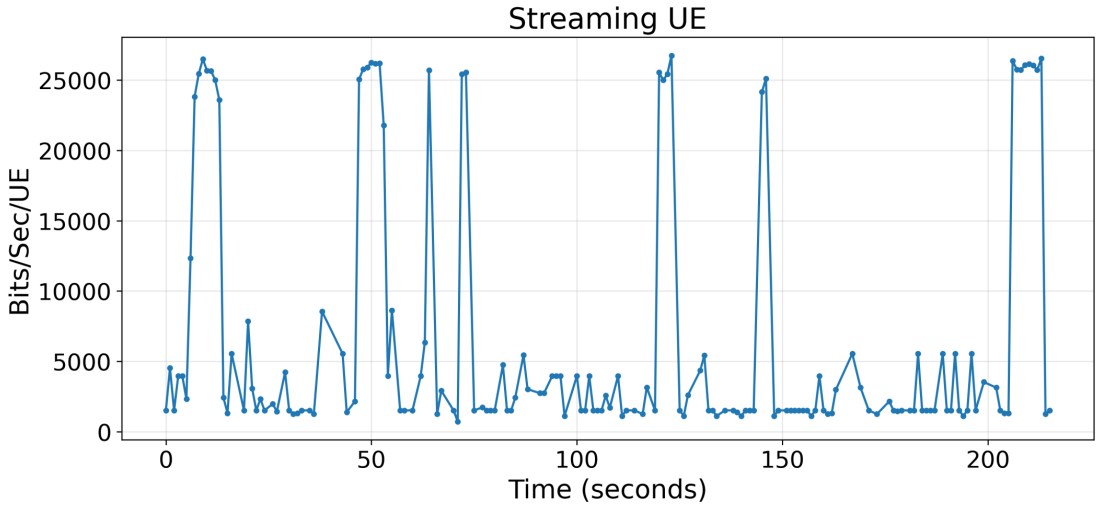
Phone Activity – Streaming & Reattaching

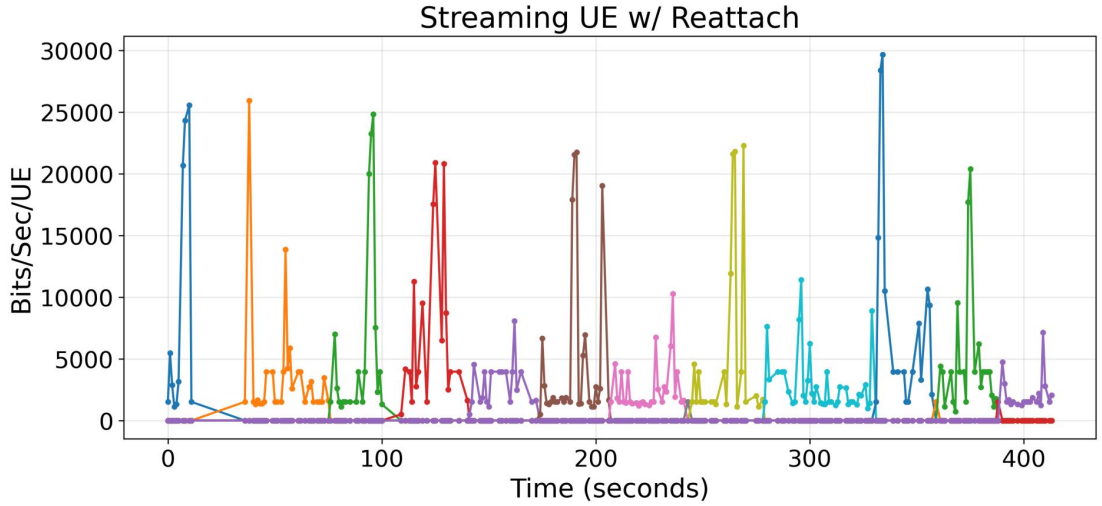


Phone Activity - Comparison



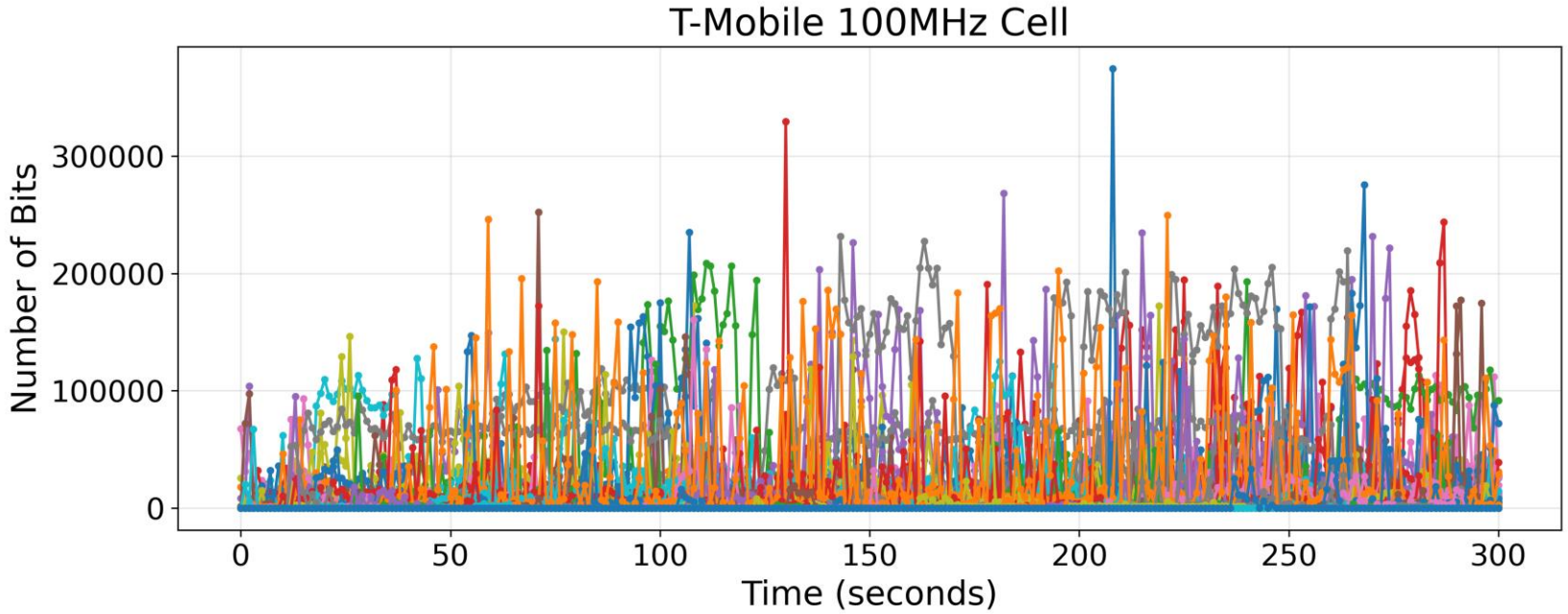






Challenges moving out of the lab

- Commercial cells handle orders of magnitude more UEs, data
- Traffic patterns will vary by setting
  - i.e. highways vs downtown city vs rural areas



Conclusion & Future work

- Initial testing in a lab setting suggests there is a notable difference in data transfer
- Ramp up data collection
  - Measure in different conditions
  - Test different lab configurations
  - Test against more complex surveillance techniques
- This project is ongoing—any feedback is appreciated!

JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING