What?

Listening to LTE signals

Why?

For fully passive localization of LTE users

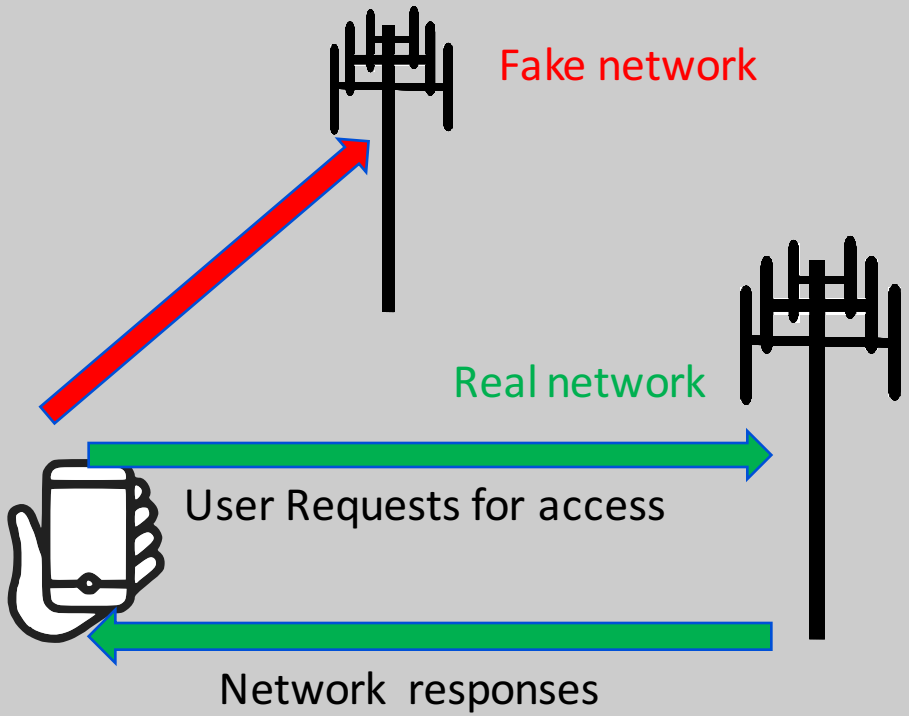
Why LTE(4G)?


GSM
3G
4G/LTE
Weak encryption
Device
authentication
Strong encryption
Mutual
authentication
Stronger
encryption
Mutual
authentication

Why Passive Listening?

Active Attacks:

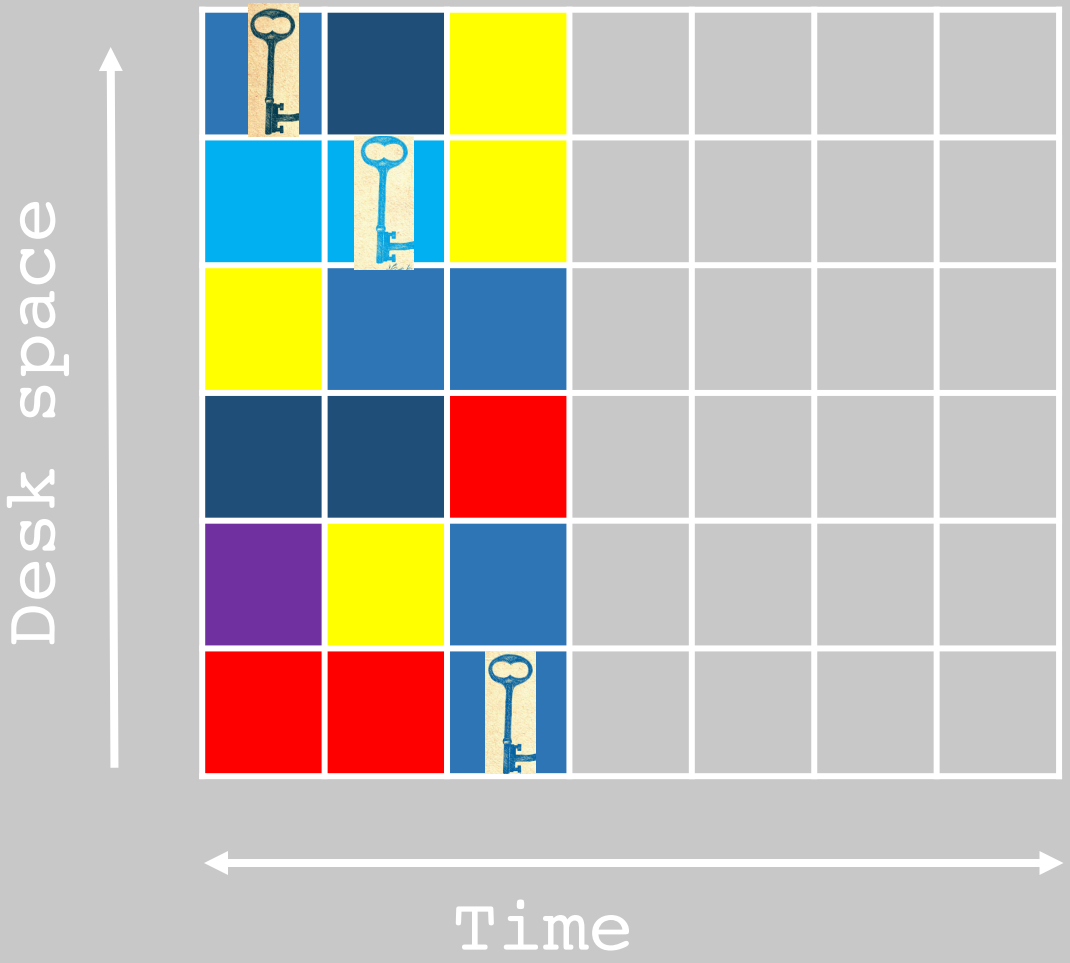
Creating a fake network and attaching mobile user to the fake network
(triggers paging messages, receiving phone's IMSI, and entire data content)



Passive Listening:

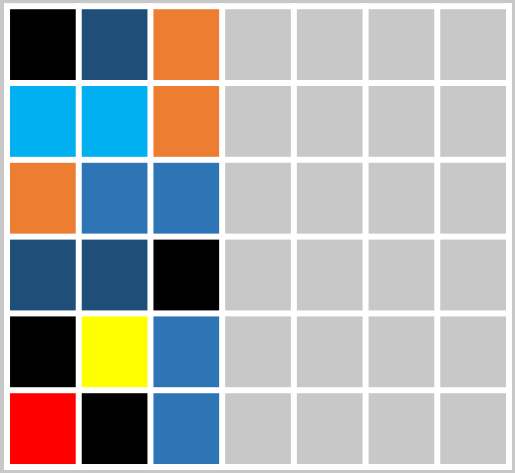
No external transmission and fishing to mobile devices

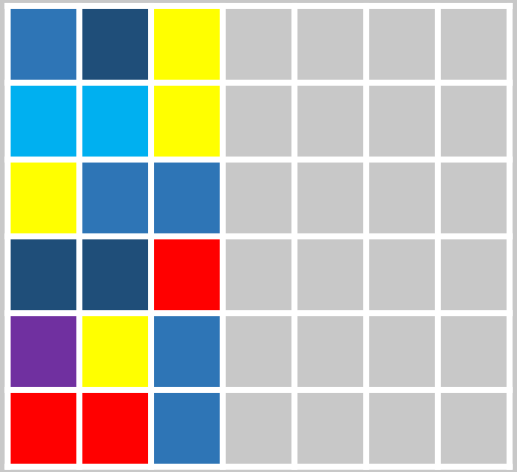
Structure of the Resources

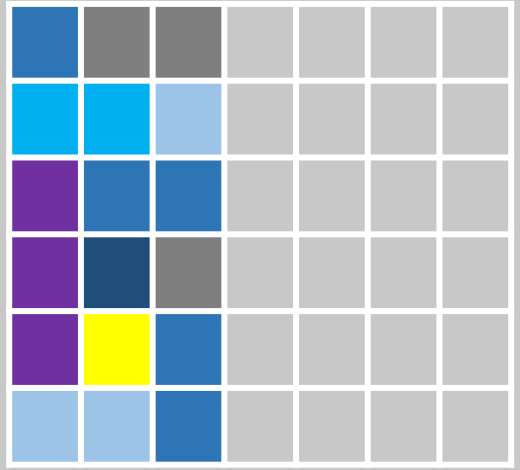


sampled, coded, modulated,

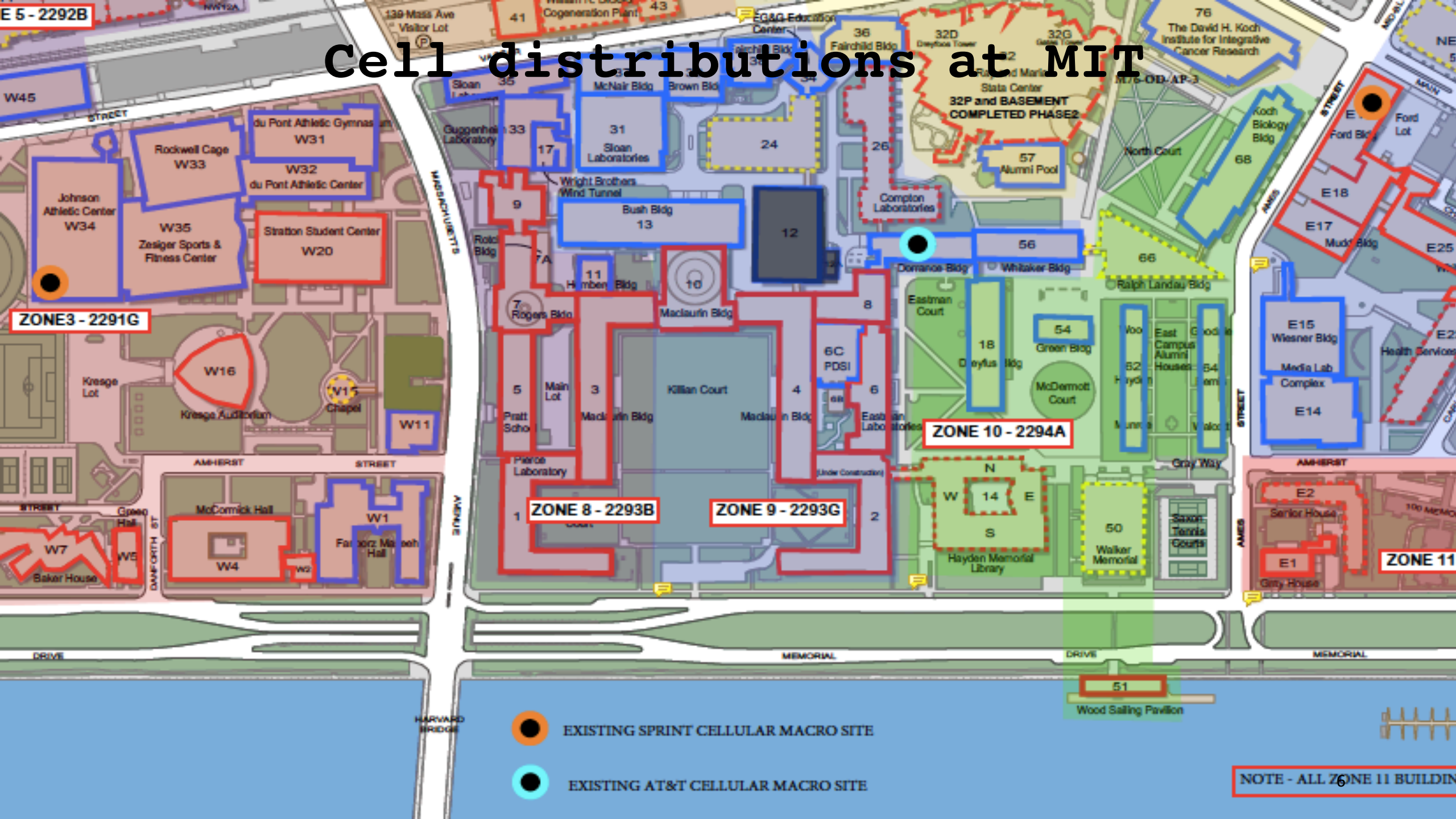
More Cell Towers



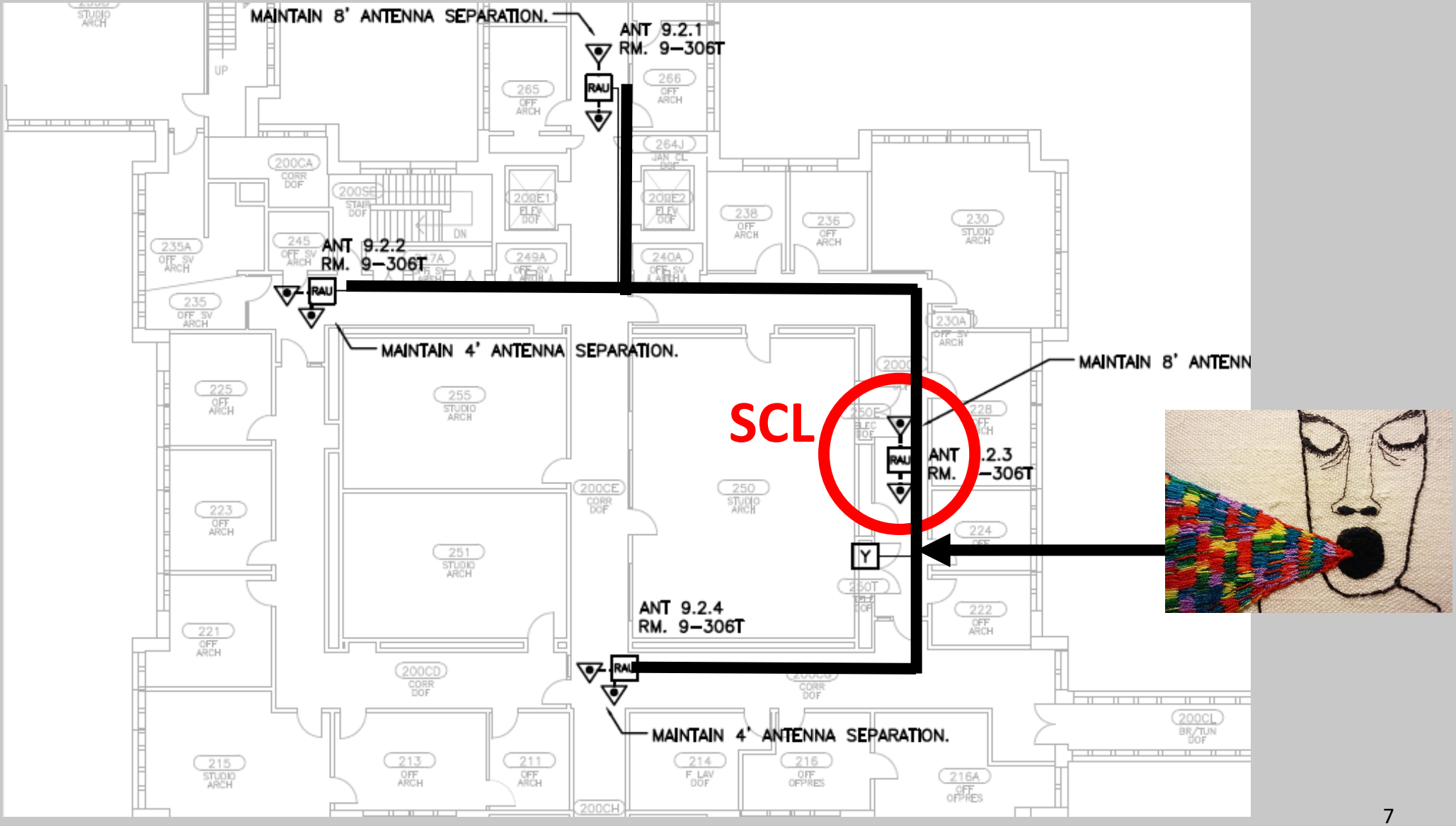




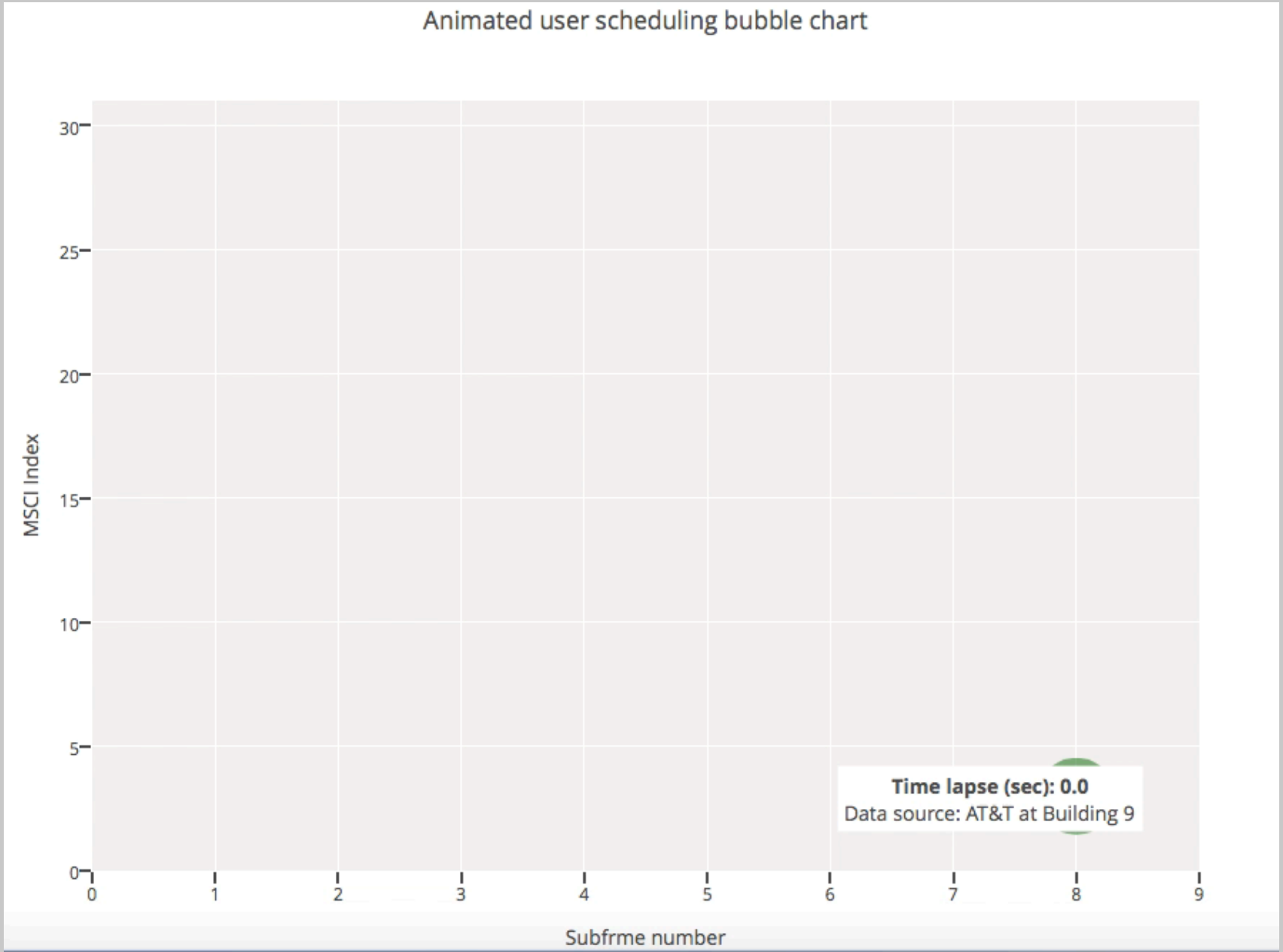
Cell distributions at MIT



Building 9/ Second Floor– AT&T



AT&T Allocations in Building 9/ Saturday Dec 3rd



MIT Underground Tunnels

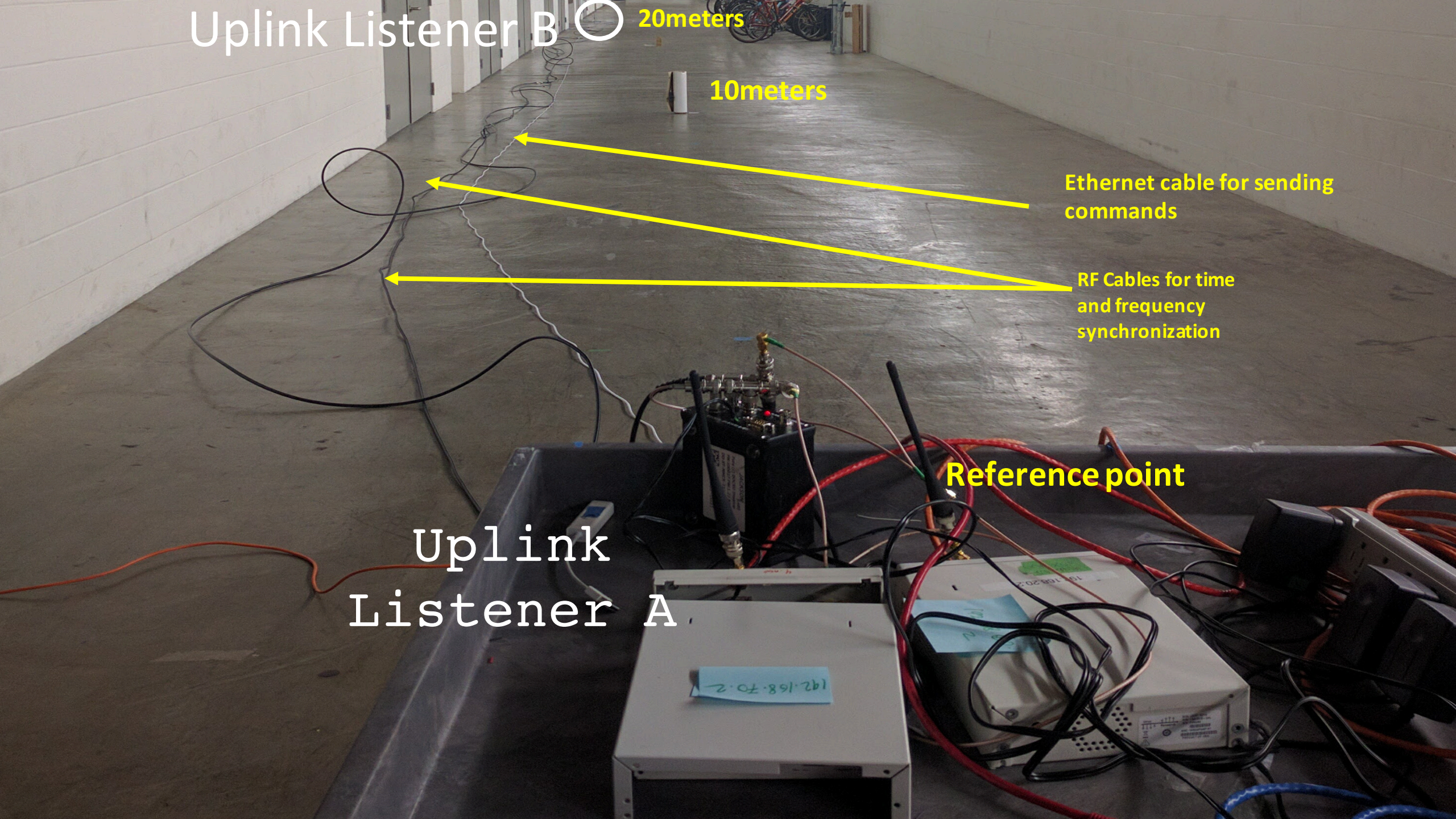
Antennas

Code to synchronize all the listeners

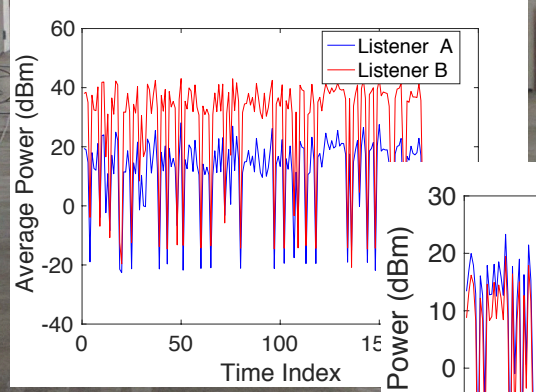
Listening to the shouter (downlink)

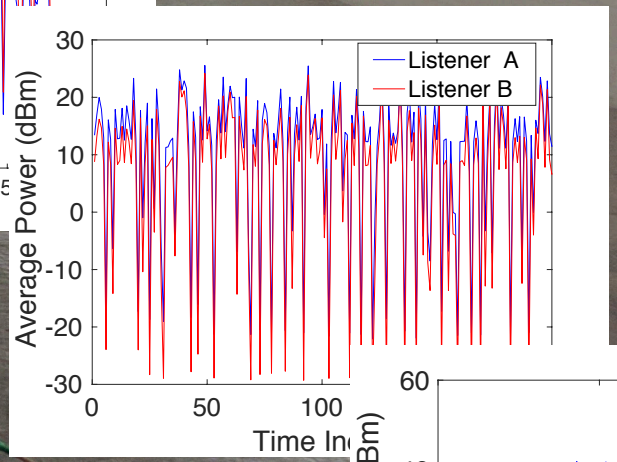
Listening to the mobile phones (uplink)

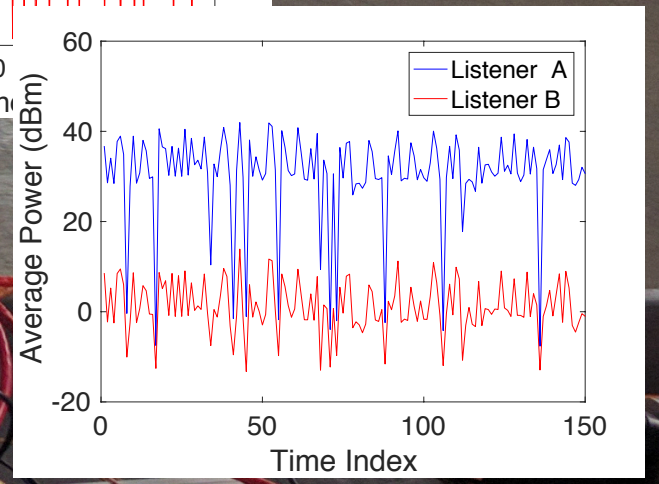
Timing and Frequency source


Uplink Listener B
20meters
10meters
Ethernet cable for sending commands
RF Cables for time and frequency synchronization
Reference point
Uplink Listener A

Calibration: Power ratio



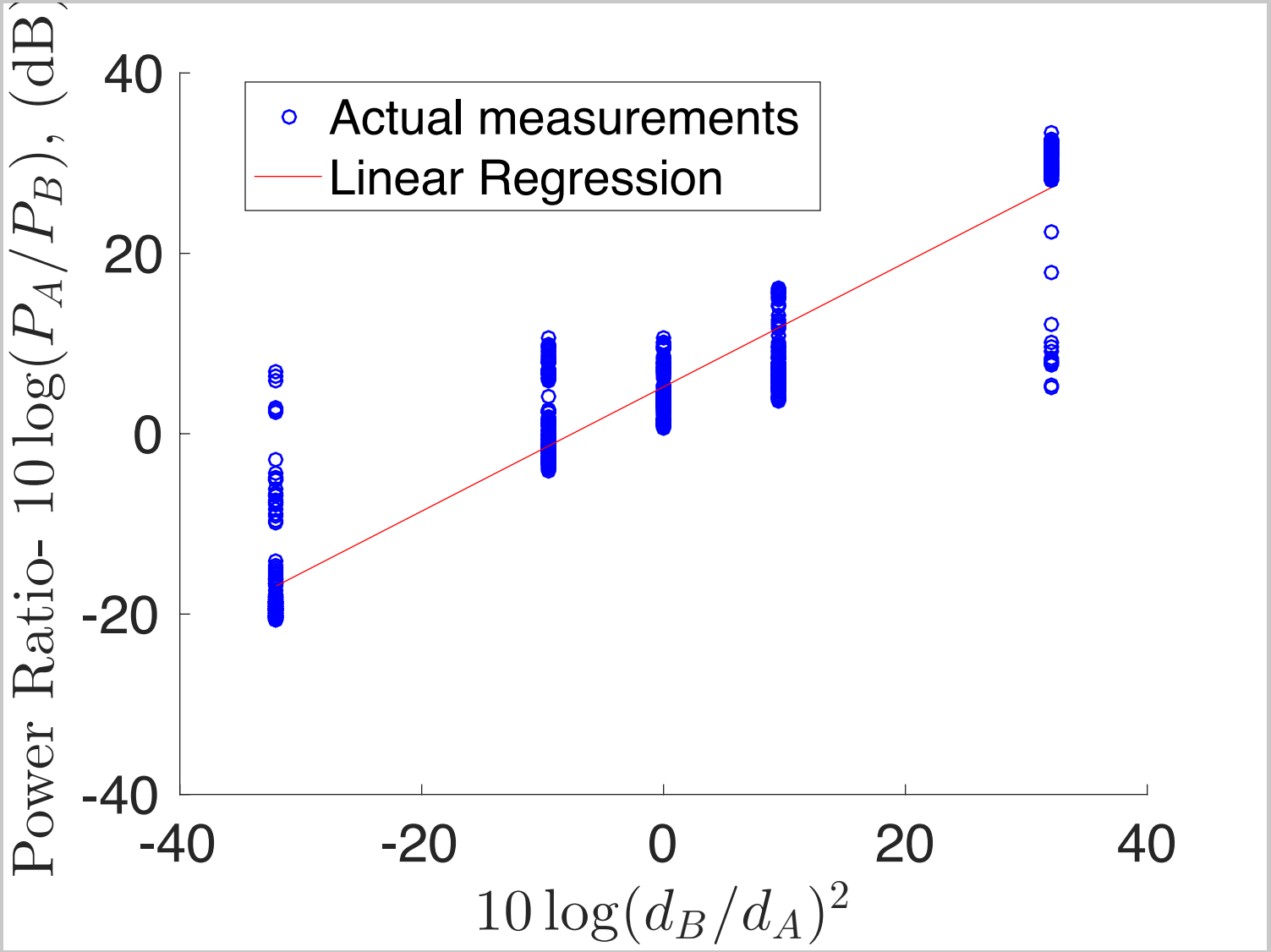




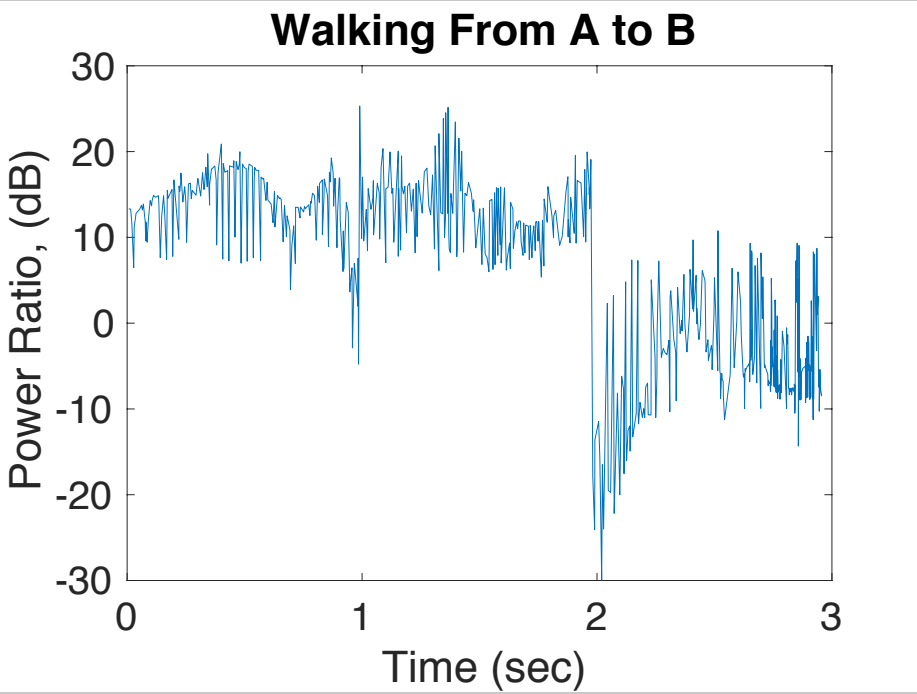
Linear Regression:

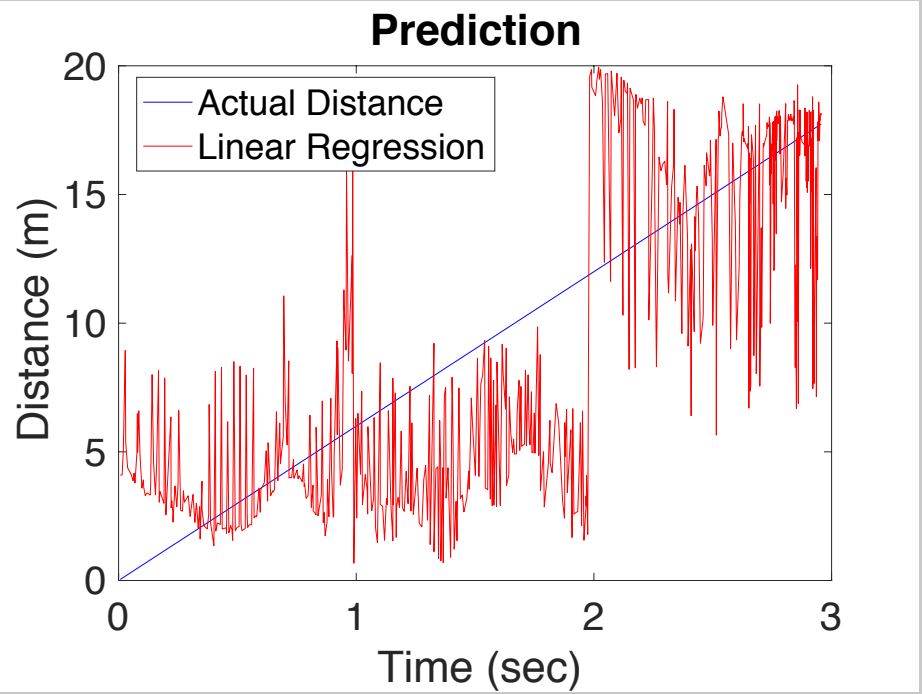
Listeners A and B are spaced 20m apart

$$\frac{P_A}{P_B} \propto \frac{d_B}{d_A}$$



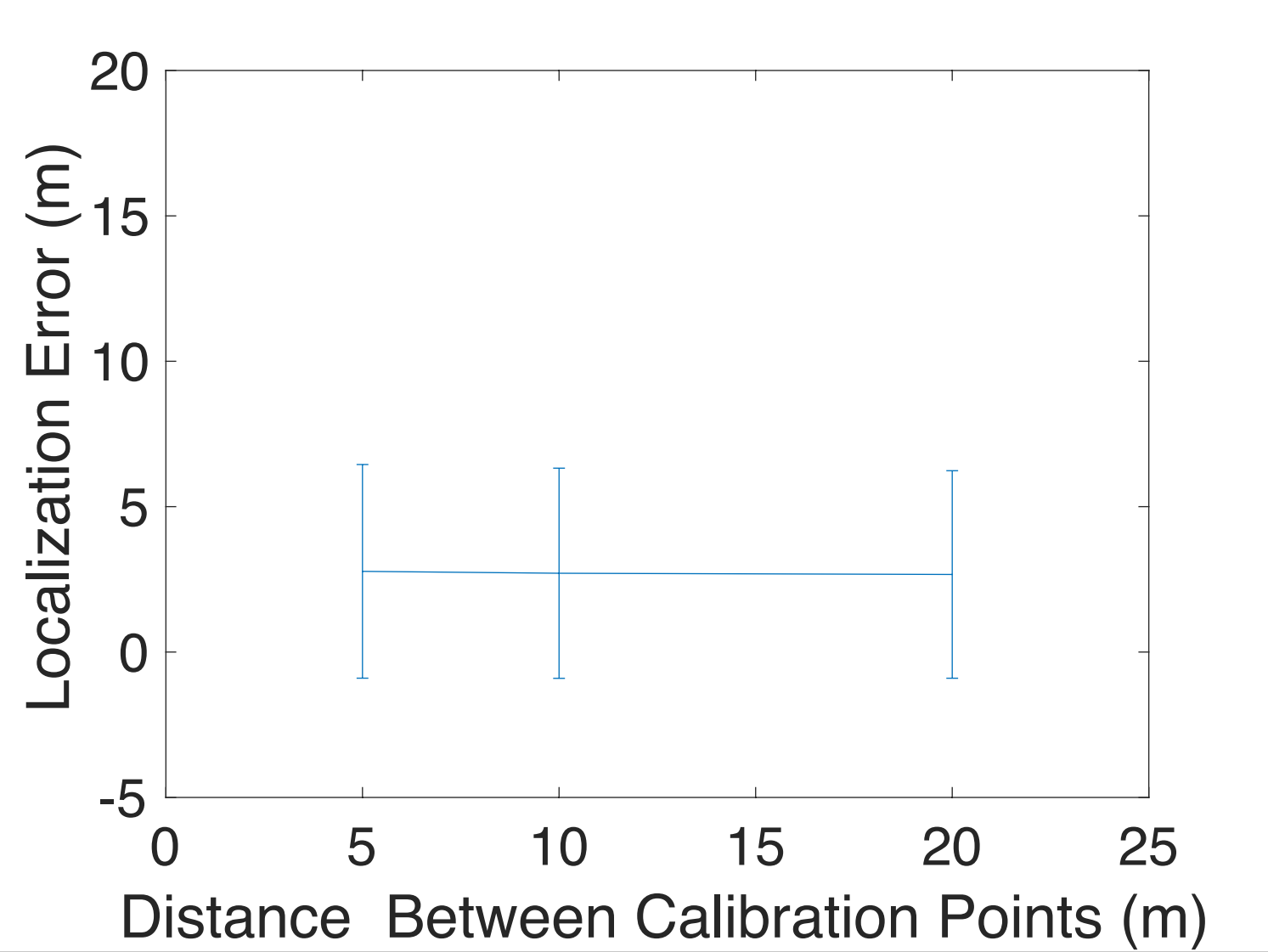
Distance Prediction





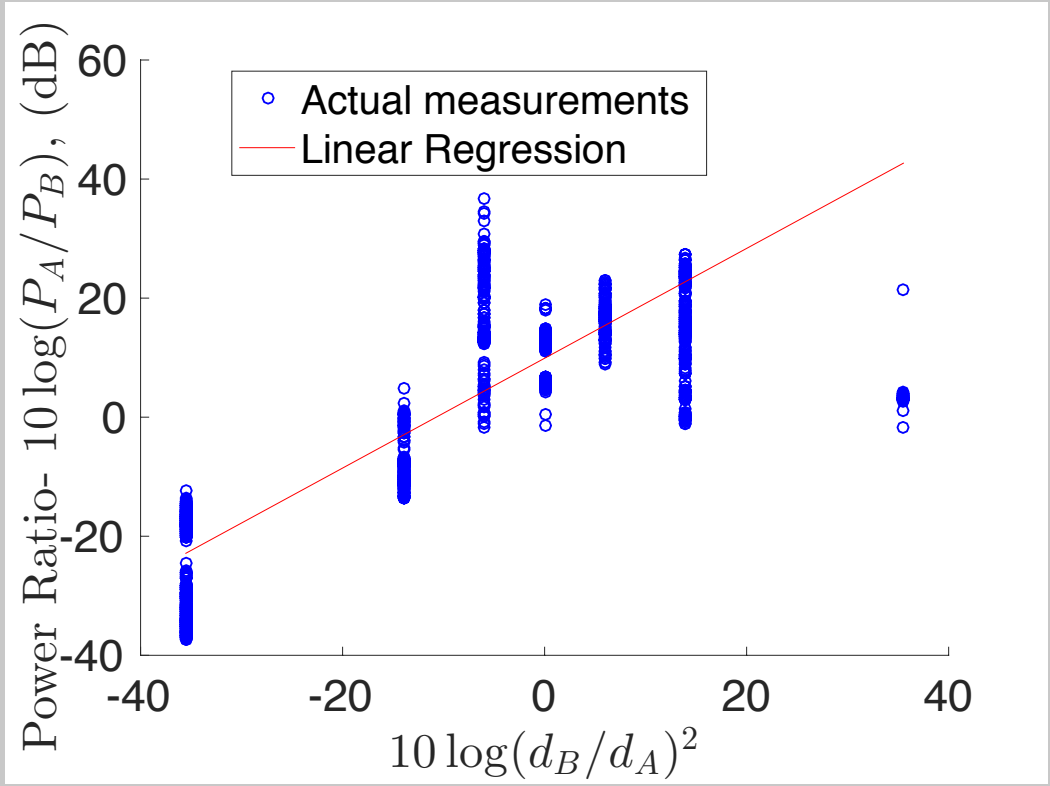
Median Error: 1.72m
Mean Error: 2.66m
Standard deviation of Error: 3.5m

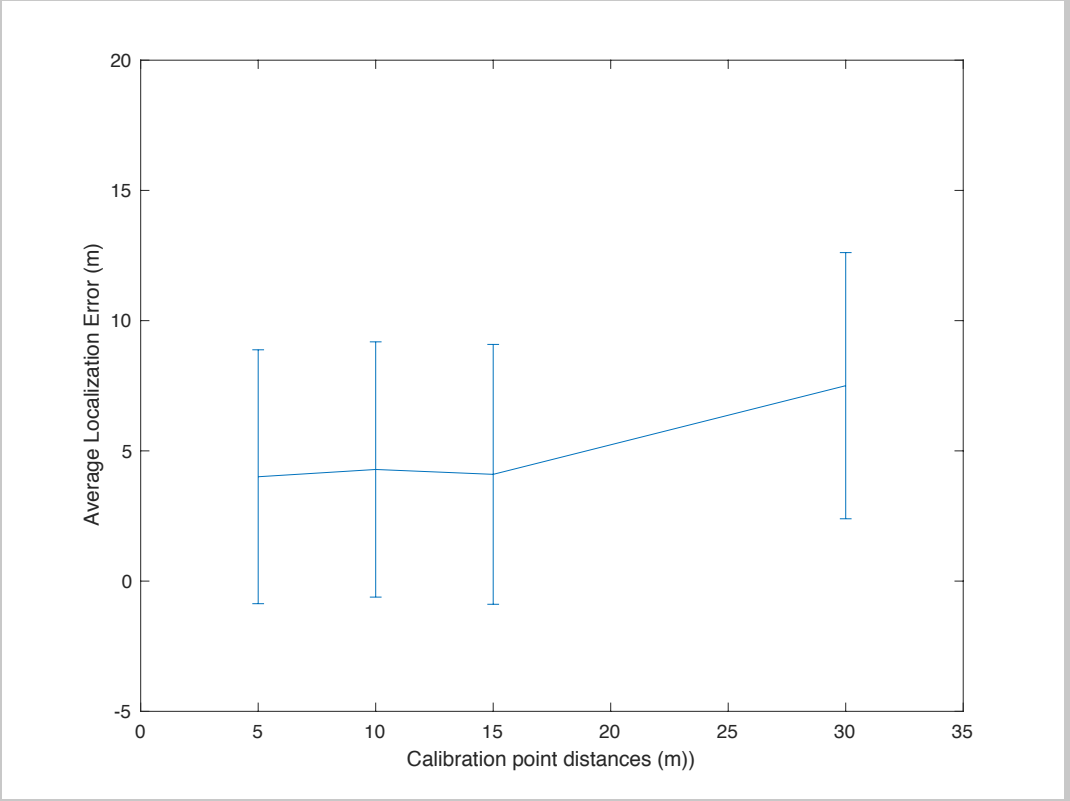
Localization Error vs. Calibration Accuracy



Why 20m distancing?

Low receiver sensitivity at 30m





To be answered

Increasing localization accuracy?

In above experiment I used basic available devices and antennas

Multipath (obstacles) effect?

More experiments in Lobby 7, Localization using phase differences

Tracking?

Using trajectories

Removing the wires and cost?

Requires more development and research/ Cheaper devices our in production

Is the data representative?

Wi-Fi Monitoring

Thank you