IoTSniffer: Detecting Unauthorized Traffic in Industrial IoT

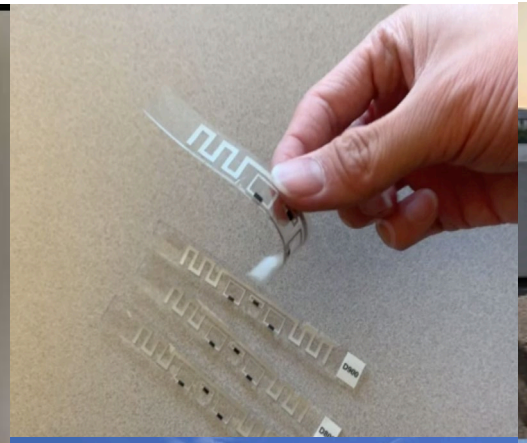
Swarun Kumar

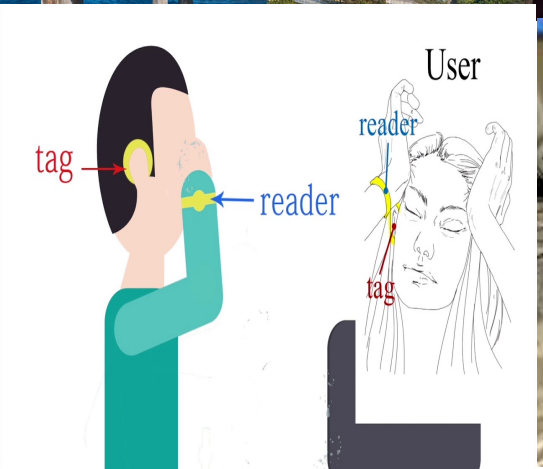
Assistant Professor, ECE, CMU

http://swarunkumar.com

WiTech Lab

”All things Wireless”



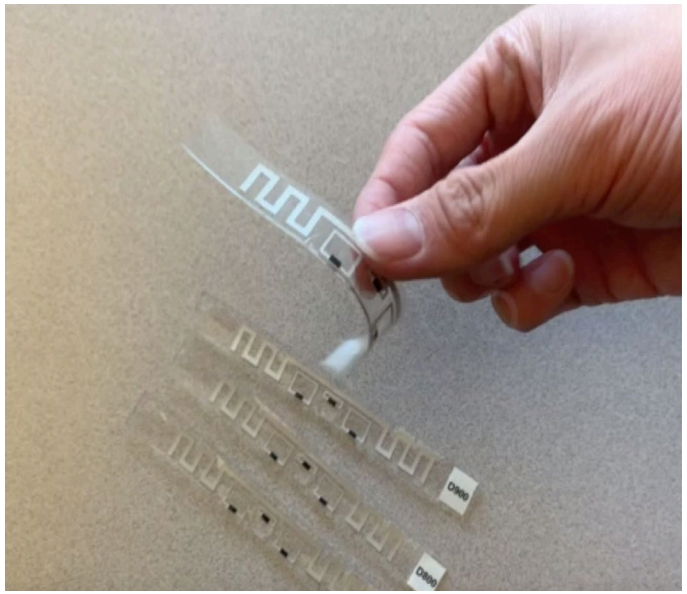


WiTech Lab

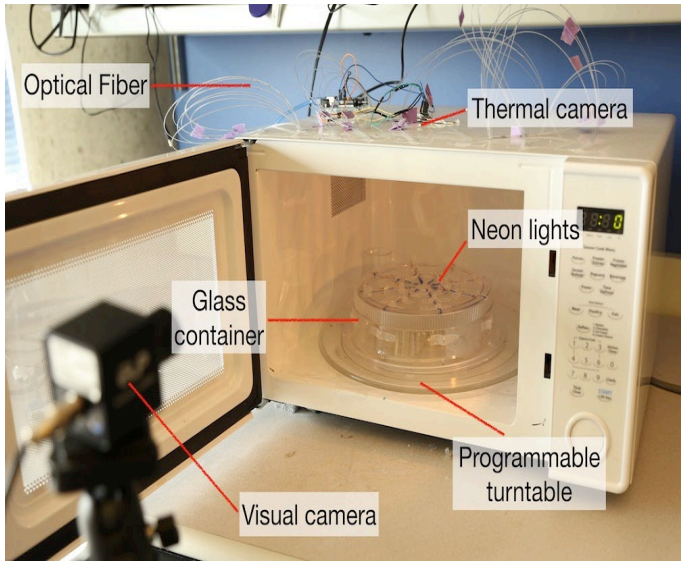
”All things Wireless”

5-G & IoT

Battery-Free Sensing



New Frontiers



Wireless Security & Privacy

Traditional View: Add security & privacy features to wireless

Our View: Use wireless features to improve security & privacy

Thank you Cylab!

- Detection and Mitigation of Fake News
  (with PI Osman Yagan), 2018
- Wireless Security for Low-Power IoT (2019)
- Lightweight Security for IoT Fog Networks
  (with PI Osman Yagan), 2020
- Detecting Unauthorized I-IoT Traffic (2020)

Akshay Gadre
2020 Cylab PhD Fellow
(PS: Check out his poster!)

Thank you Cylab!

- Detection and Mitigation of Fake News
  (with PI Osman Yagan), 2018

- Wireless Security for Low-Power IoT (2019)

- Lightweight Security for IoT Fog Networks
  (with PI Osman Yagan), 2020

- Detecting Unauthorized I-IoT Traffic (2020)

Thank you Cylab!

- Detection and Mitigation of Fake News
  (with PI Osman Yagan), 2018

- Wireless Security for Low-Power IoT (2019)

- Lightweight Security for IoT Fog Networks
  (with PI Osman Yagan), 2020

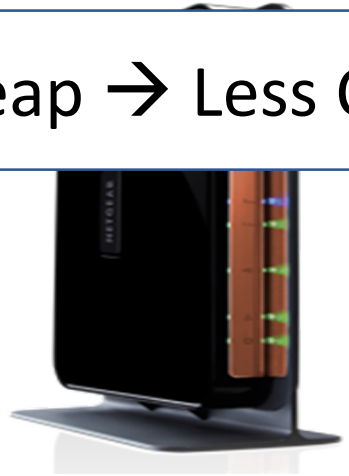
- Detecting Unauthorized I-IoT Traffic (2020)

Can we detect radio adversaries?

Legitimate Device

Low Power, Cheap → Less Capable

Malicious Adversary

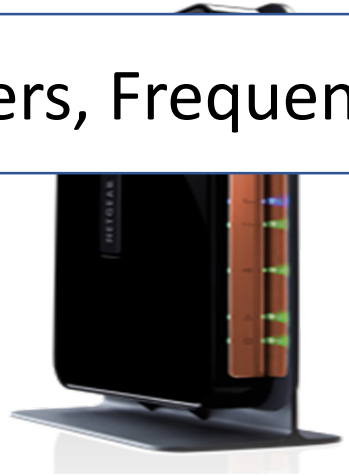


Base station

Idea: Use Hardware Imperfections!

Legitimate Device

Cheap ➔ Unique filters, Frequency shifts, etc.



Malicious Adversary

Can’t predict / emulate!

Use Wireless “Physically Unclonable Functions” to Achieve Security Goals

Impact

- IPSN 2020 Best Paper, Paper at ICC
- Seeded new awards: NSF CPS (~ $1.5 million), ARL
- Exploring new industry collaborations

Thank you Cylab!

- Detection and Mitigation of Fake News
  (with PI Osman Yagan), 2018

- Wireless Security for Low-Power IoT (2019)

- Lightweight Security for IoT Fog Networks
  (with PI Osman Yagan), 2020

- Detecting Unauthorized I-IoT Traffic (2020)

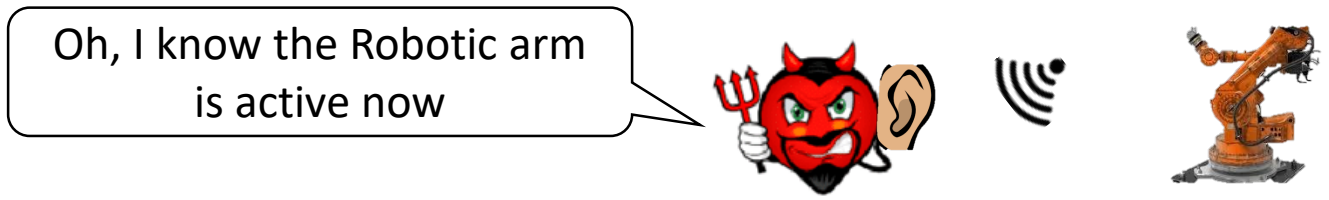
Industrial IoT is increasingly wireless

I-IoT Wireless is Fragmented

.. Partly because they provide different range, data rates and infrastructure needs.

Implication: Many Security Holes

- **Passive Attacks**: Monitoring Traffic Flows



- **Active Attacks**: Mimicking/taking over operations

Our Focus

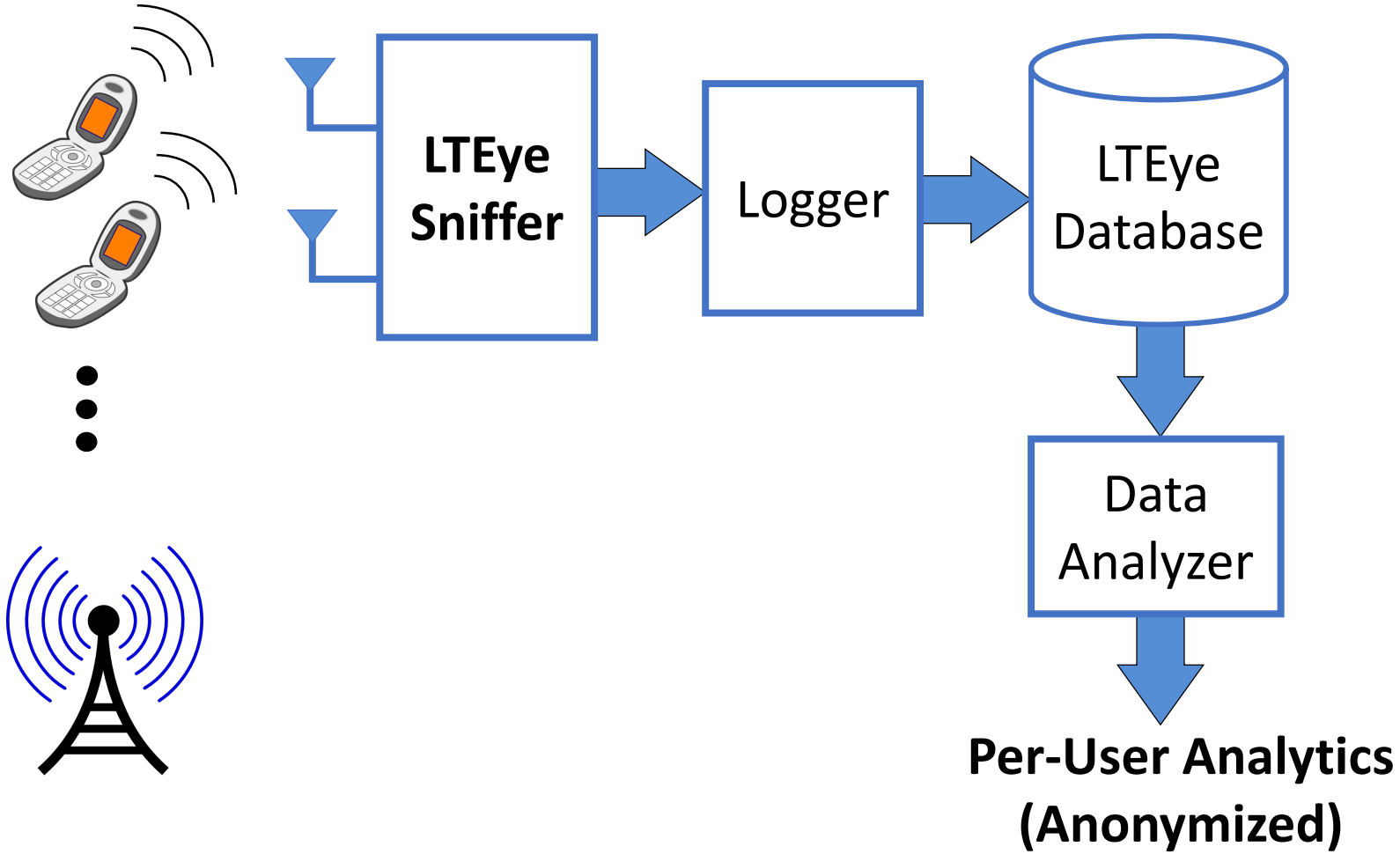
Solution: IoTSniffer

Instrument the environment with software radios that both detect and locate unauthorized traffic.

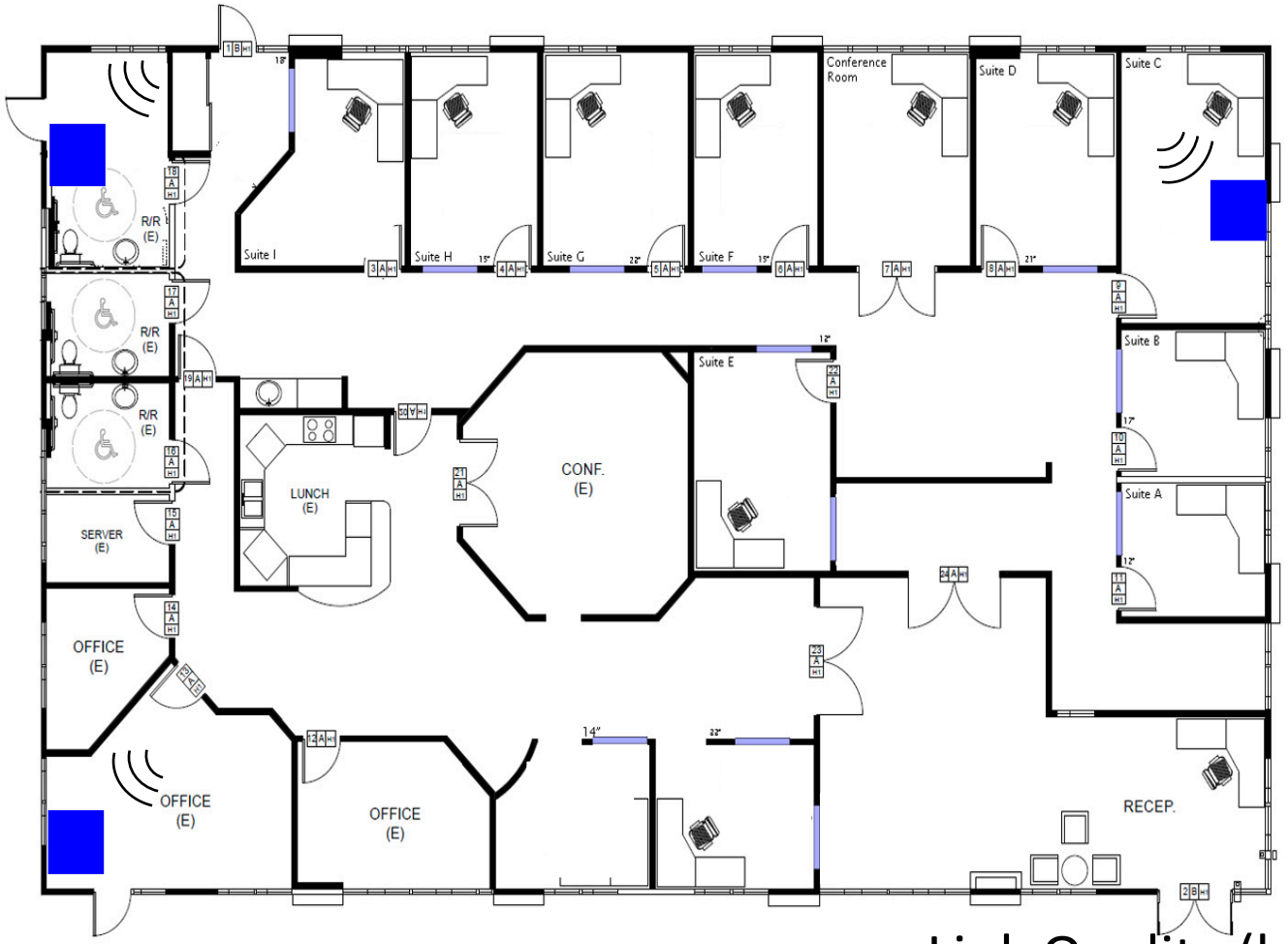
Our Secret Sauce

- *An Efficient Decoding Pipeline*: Handle diverse I-IoT technologies
- *Learning & Tracking Sender Behavior*: Using wireless channels
- *Device Tracking*: Even for non-cooperating sender devices!

Prior Work: LTE Sniffing (LTEye)



Overview of LTEye

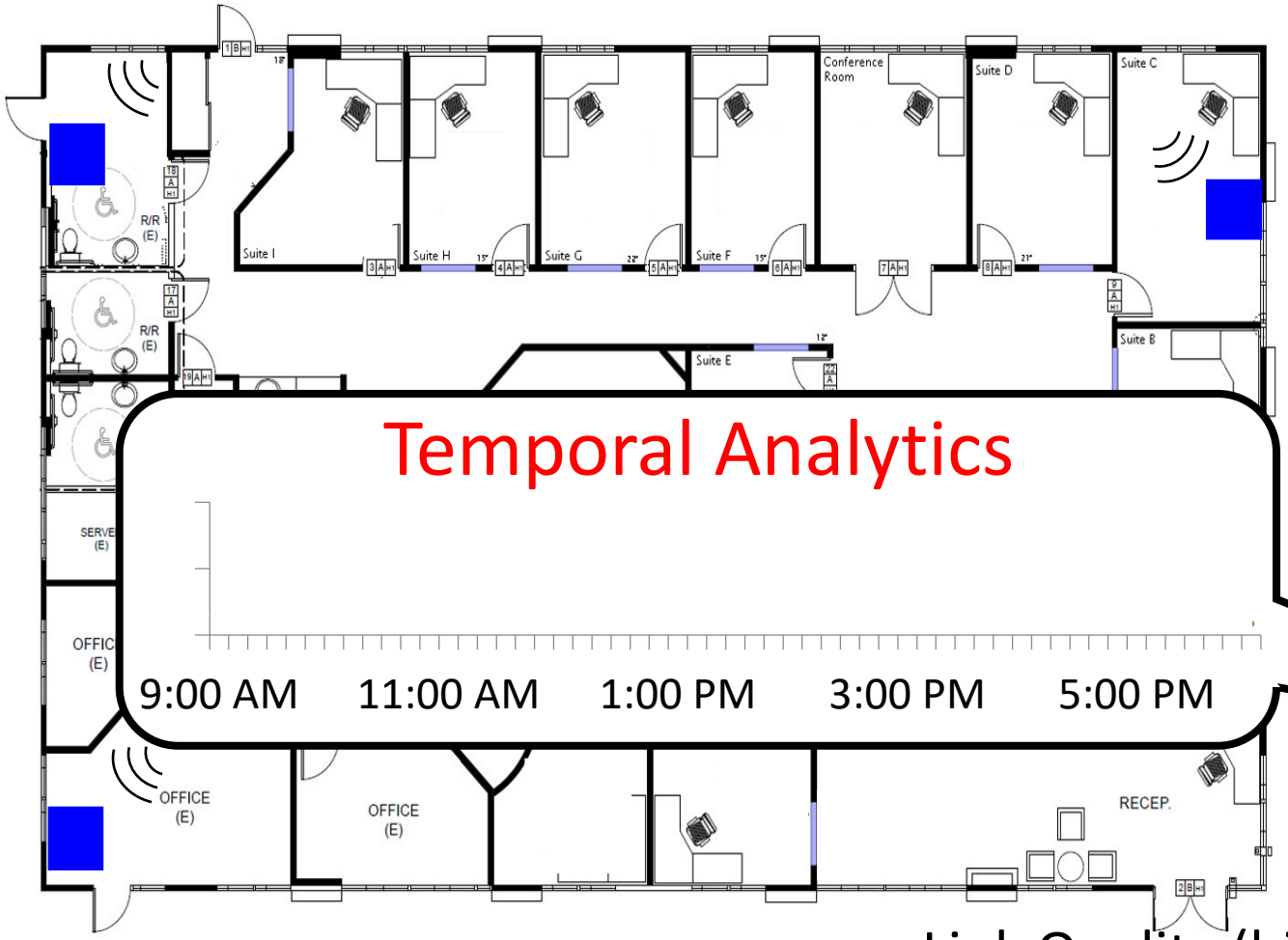


User ID	Qlty

Link Quality (bits/RE)

2 3 4 5

Overview of LTEye



Temporal Analytics

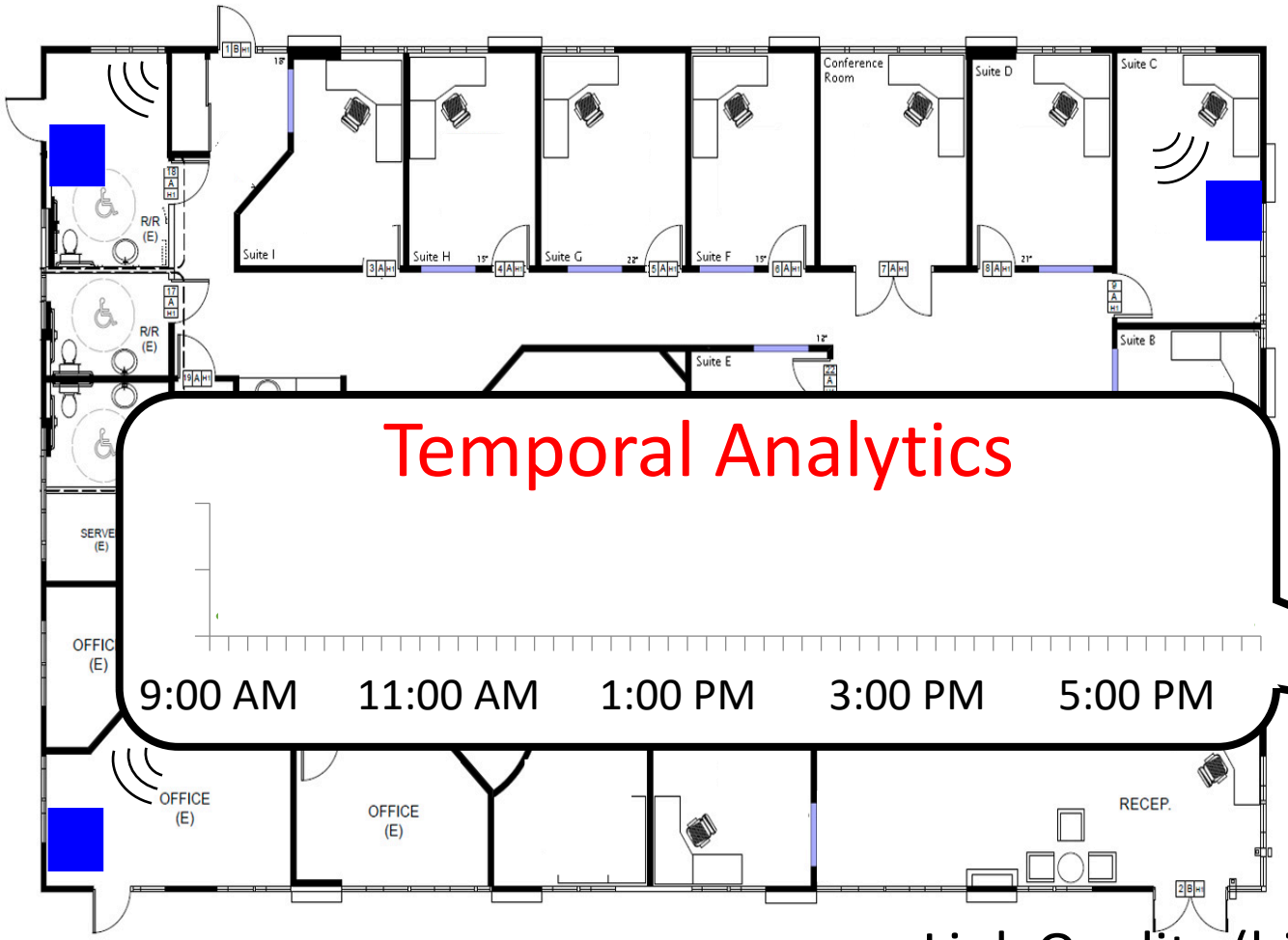
9:00 AM 11:00 AM 1:00 PM 3:00 PM 5:00 PM

User ID	Qlty
1	
2	
3	
4	
5	
6	
7	
8	

Link Quality (bits/RE)

2 3 4 5

Overview of LTEye



Temporal Analytics

9:00 AM 11:00 AM 1:00 PM 3:00 PM 5:00 PM

User ID	Qlty
1	
2	
3	
4	
5	
6	
7	
8	

Link Quality (bits/RE)

2 3 4 5

Overview of LTEye

User ID	Qlty
1	
2	
3	
5	
6	
7	
8	

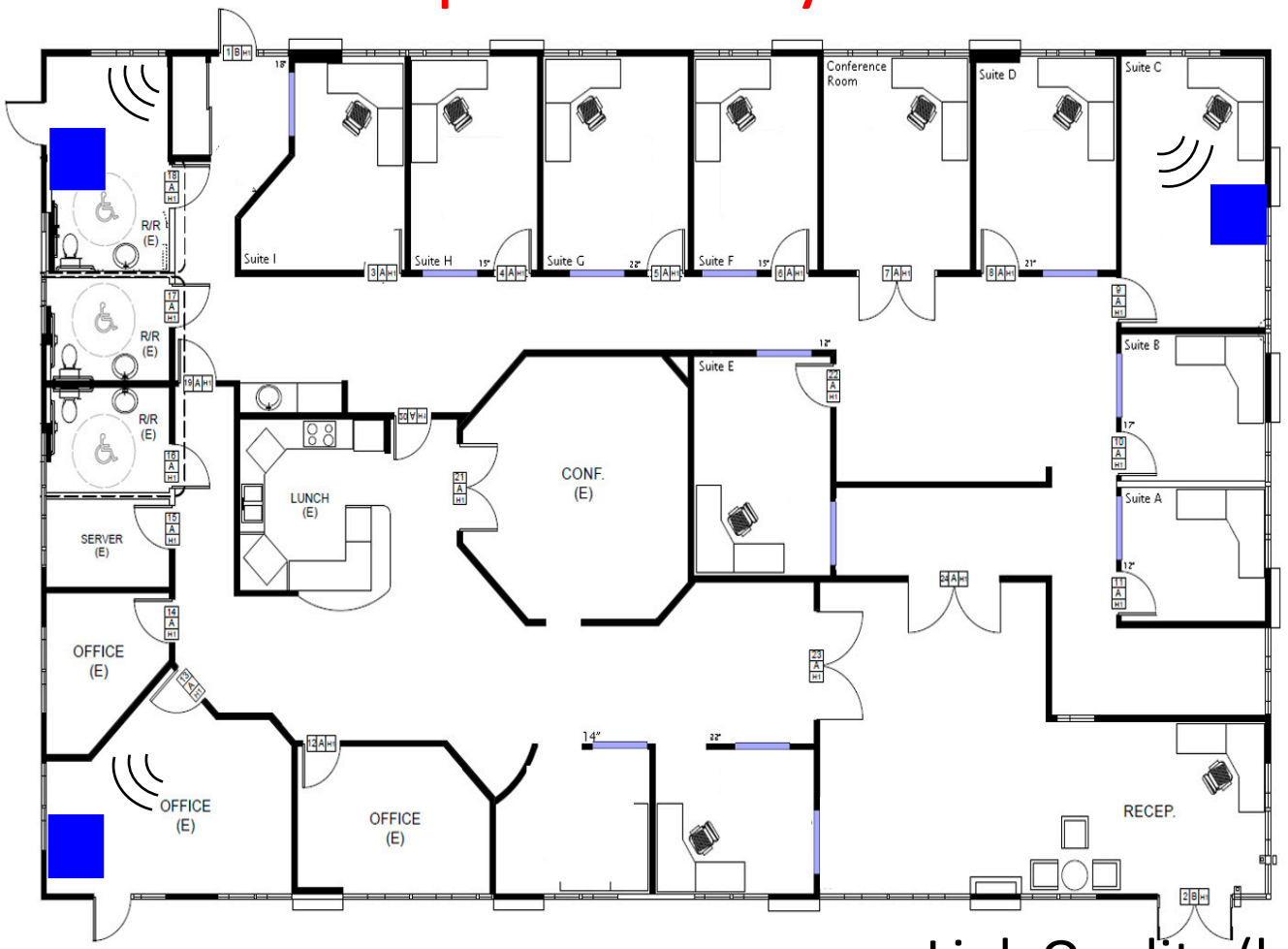
Where are these users in the floorspace?

Link Quality (bits/RE)

2 3 4 5

Overview of LTEye

Spatial Analytics



User ID	Qlty
1	
2	
3	
4	
5	
6	
7	
8	

Link Quality (bits/RE)

2 3 4 5

Open Challenges in I-IoT context

- Heterogeneous Technologies
- Frequency hopping, active evasion from the sniffers
- Efficient Spectrum sensing

A few updates so far

- Complete: Inexpensive Multi-Technology SDR Sniffer (~ $20)
- Support for LoRa, Xbee, Zwave and SIGFOX

A few updates so far

- In Progress: Location-Tracking Experiments

Next Steps: Mill-19 Testbed

Summary: We do wireless!

New solutions that *leverage* wireless to address security and privacy problems

Learn more about my lab's work at:

www.witechlab.com