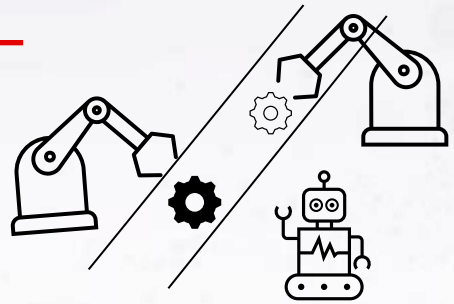
Institute for the Wireless Internet of Things
at Northeastern University

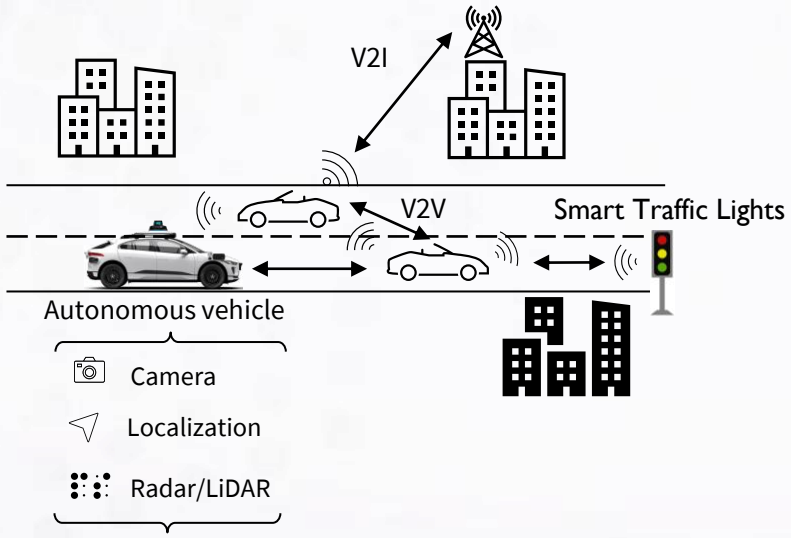
Cybersecurity Risks and Mitigation Strategies in Next Generation Communication Networks

Kaushik Chowdhury
Professor and Associate Dean for Research, College of Engineering
Associate Director of the Institute for the Wireless Internet of Things
Website: https://genesys-lab.org
Email: krc@ece.neu.edu

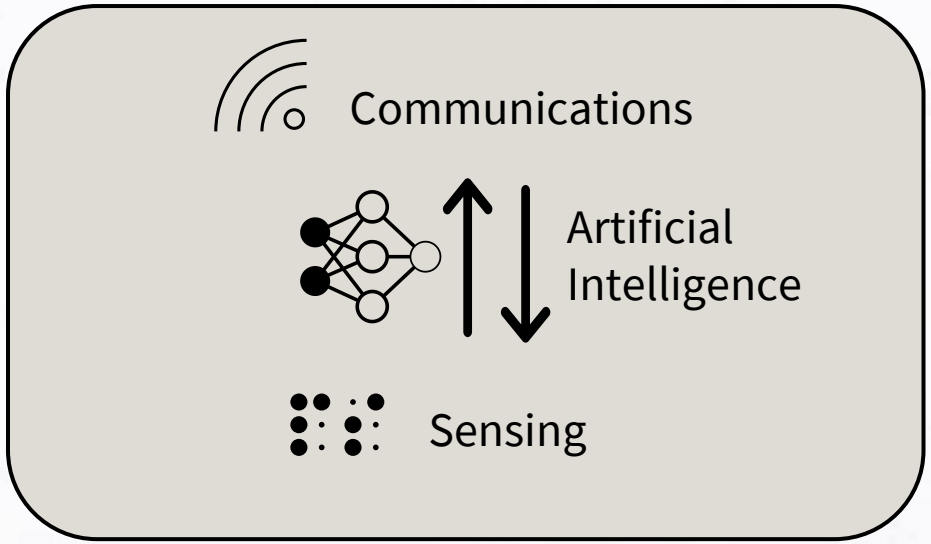
Introduction

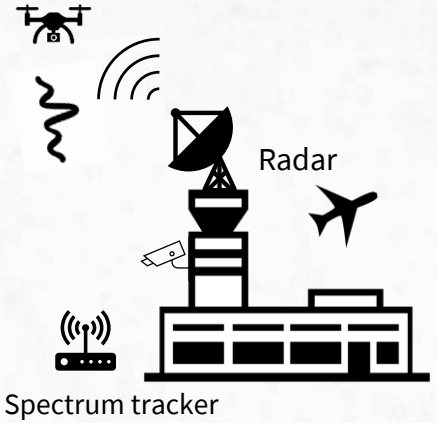


Industrial IoT

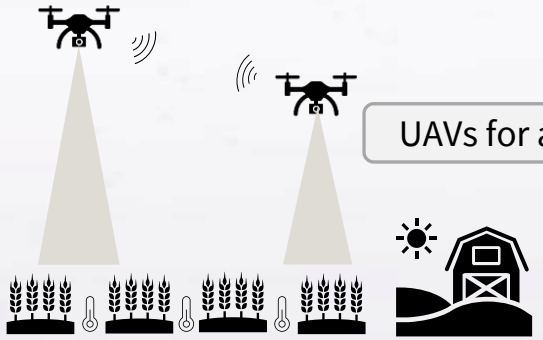


Smart city



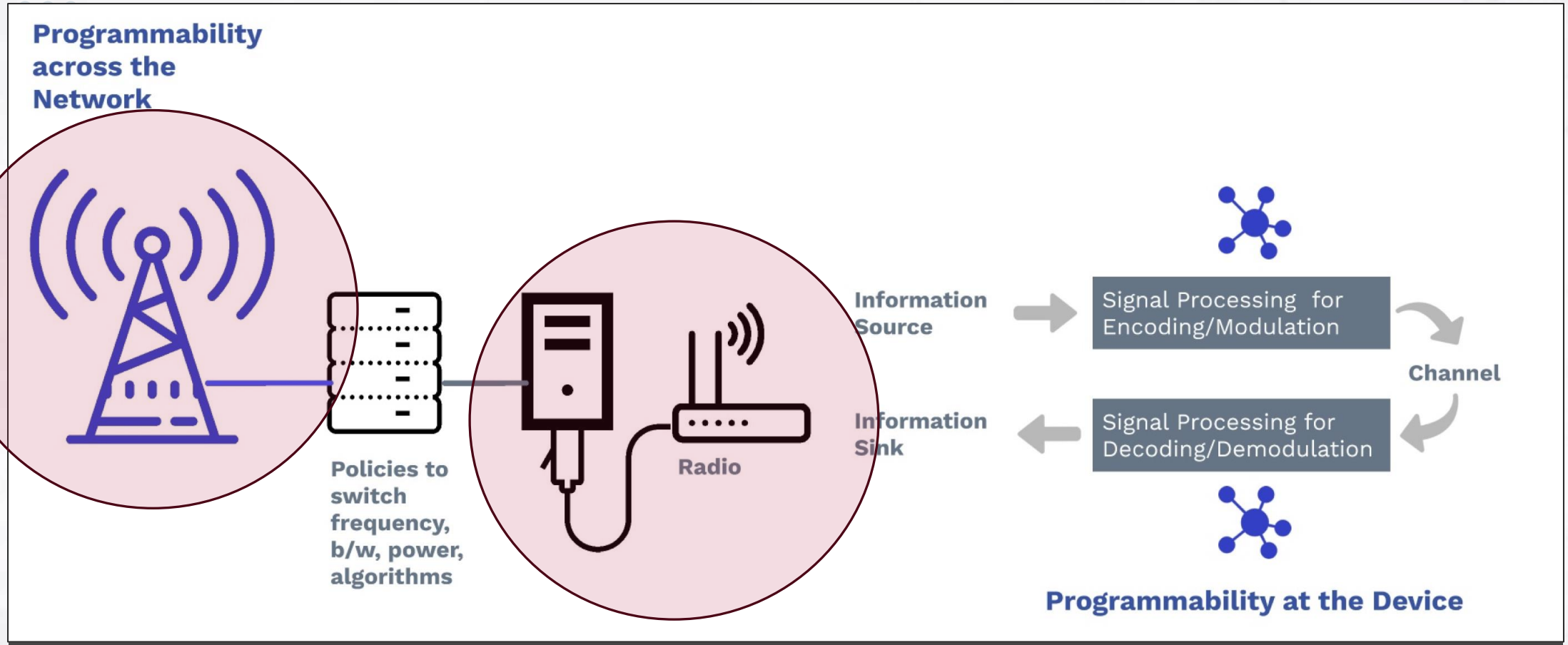


Spectrum Sensing



UAVs for automation

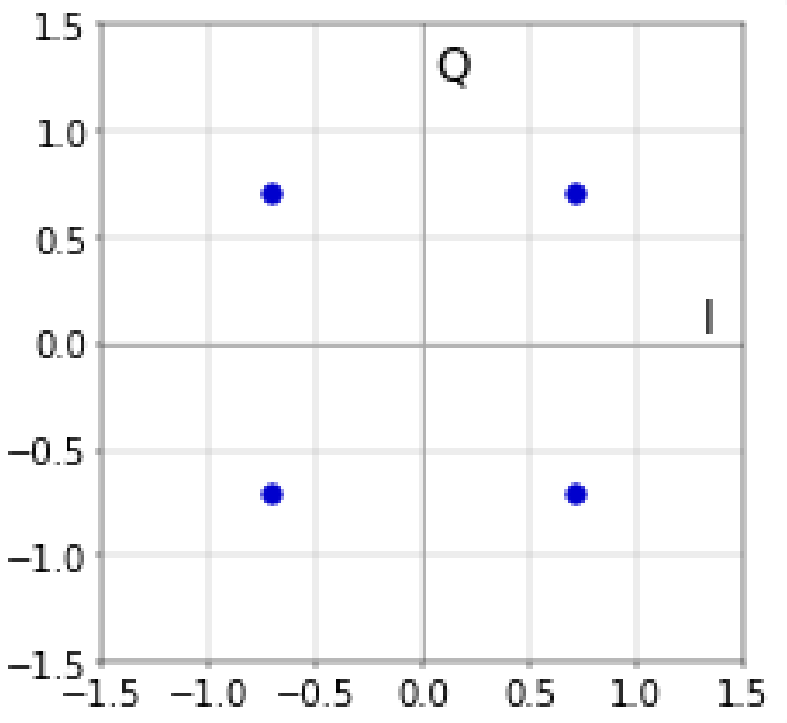
Introduction



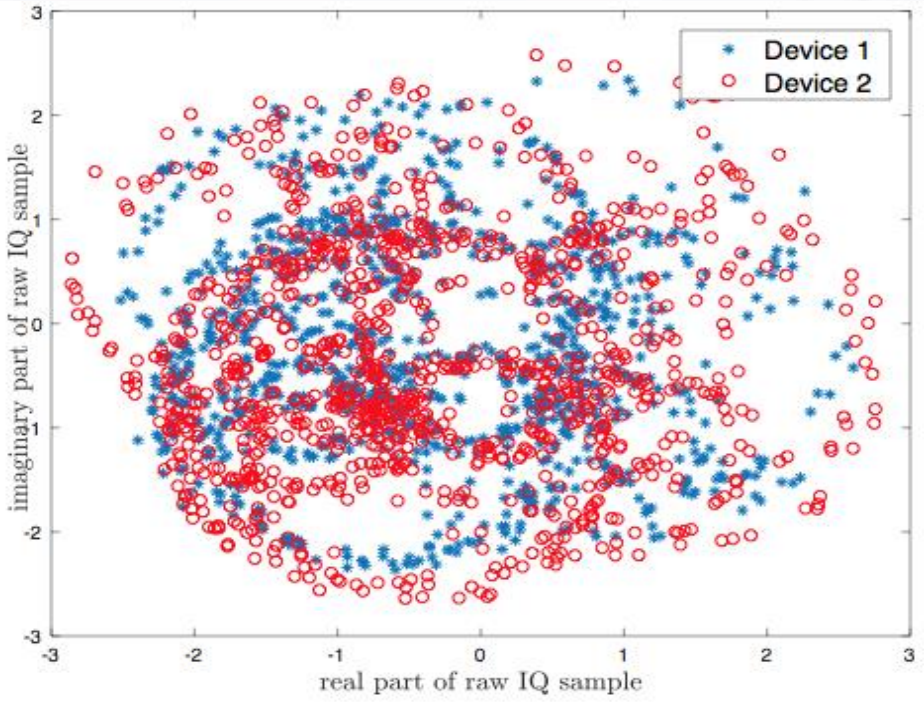
Takeaway 1: Future (6G) networks will have programmability at all levels. Can be exploited for offense and defense!

Introduction

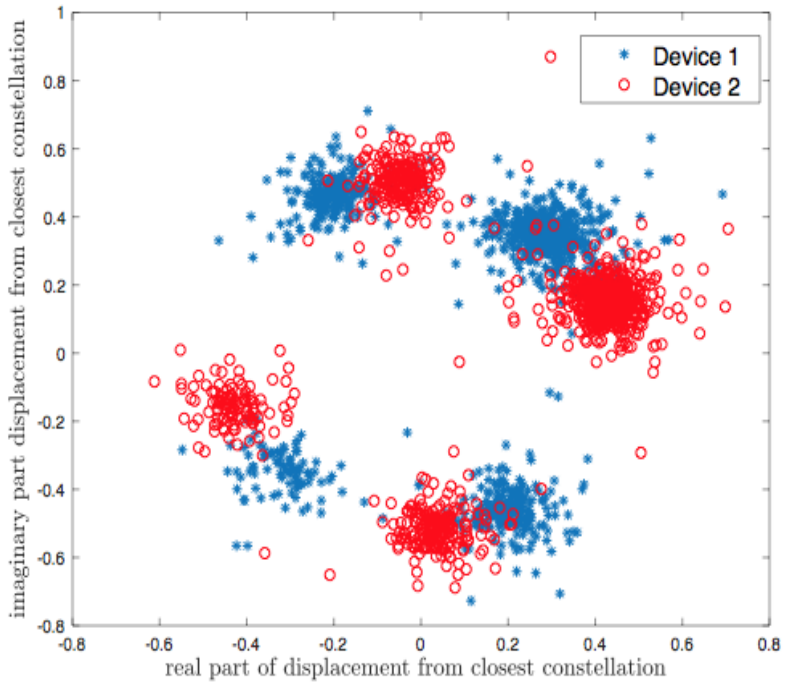
Wireless channel majorly distorts transmissions – this is "expected behavior"



Transmitted Constellation



Received Constellation due to Channel



Recovered Constellation

Takeaway 2: Any adversarial actions further complications signal recovery

Spoofing and “Fingerprinting” at the Device Level

Institute for the Wireless Internet of Things
at Northeastern University

Need for Unique Emitter Identification

Shopping Mall

NYC Subway Station

Super Bowl

Number of connected sensing devices worldwide will increase to >200 billion by 2025

T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. R. Chowdhury, and S. Ioannidis, "Deep Learning for RF Fingerprinting: A Massive Experimental Study," IEEE Internet of Things Magazine, vol. 3, no. 1, pp. 50-57, April 2020. PDF

DoD Example: Identifying UAVs (same make/model)

TC

Login

Search

Disrupt Berlin 2019
Startups
Apps
Gadgets
Videos
Audio
Extra Crunch
Newsletters
Events
Advertise
—
Crunchbase
More

Analysis backs claim drones were used to attack Venezuela's president

Natasha Lomas @riptari / 6:48 am EDT • August 8, 2018

Comment

DJI M600

https://techcrunch.com/2018/08/08/analysis-backs-claim-drones-were-used-to-attack-venezuelas-president/

https://www.defenseone.com/threats/2017/10/pentagons-ied-hunters-have-new-target-drones/142051/

What is an RF Fingerprint?

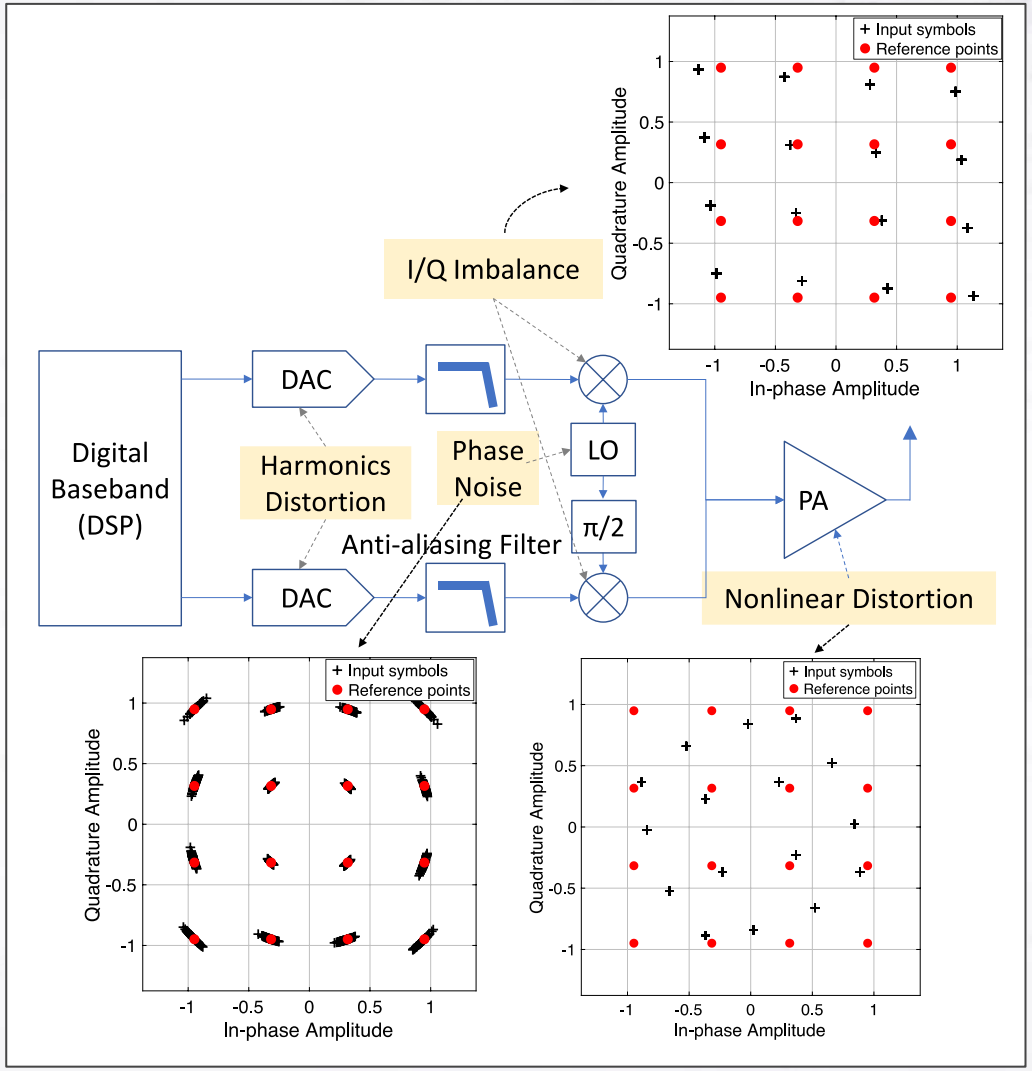
IoT authentication mechanism rely on

Cryptography

(application layer operation) energy and computationally expensive

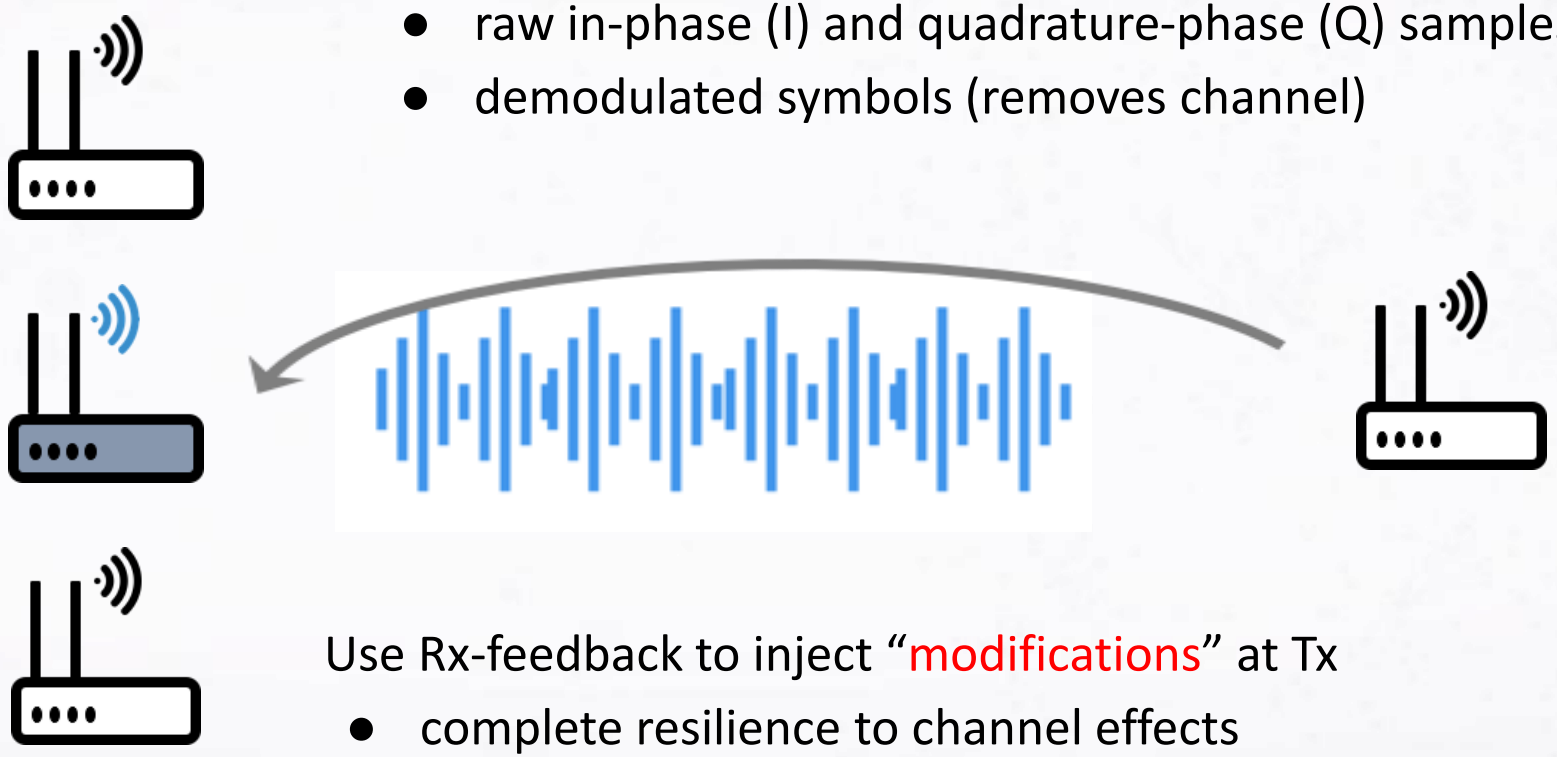
Solution

(physical layer operation) rely on unique device-characteristics of the radio



K. Sankhe, M. Belgiovine,F. Zhou, S. Riyaz, S. Ioannidis, and K. R. Chowdhury, "ORACLE: Optimized Radio clAssification through Convolutional neuraL nEtworks," IEEE INFOCOM 2019, Paris, France, May. 2019. PDF

How to Detect an RF Fingerprint?



Deep Learning for detecting unique Tx-signatures

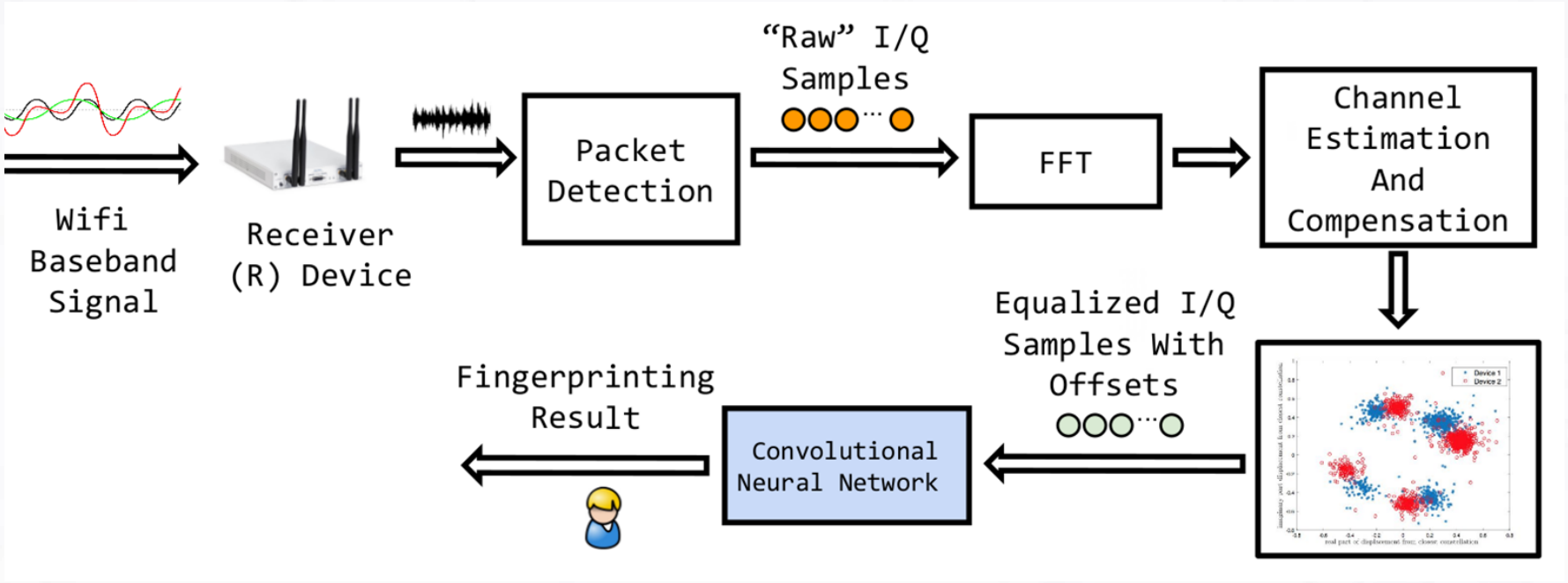
- raw in-phase (I) and quadrature-phase (Q) samples
- demodulated symbols (removes channel)

Use Rx-feedback to inject "modifications" at Tx

- complete resilience to channel effects

A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, J. Dy, S. Ioannidis, K. R. Chowdhury, T. Melodia, "Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting," IEEE INFOCOM 2020, Toronto, Canada, July 2020. PDF

How to Detect an RF Fingerprint?



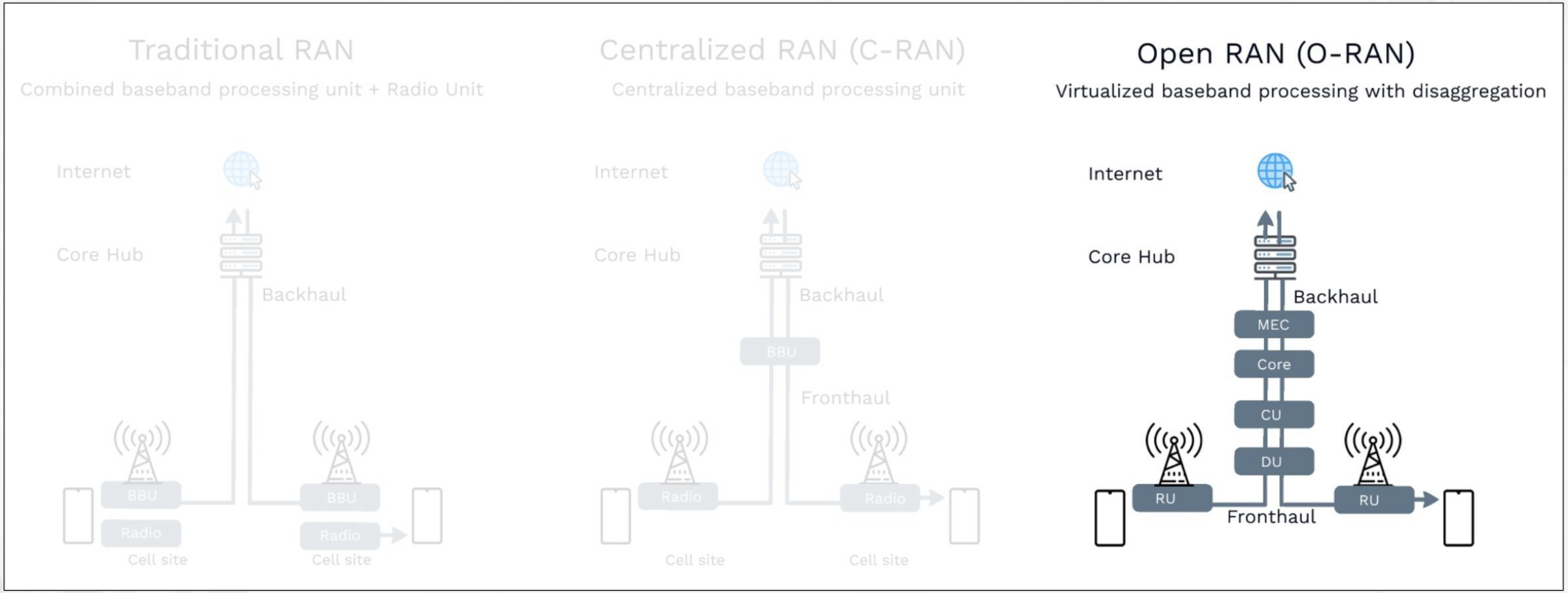
Extensive prior work with complete bibliography here:

https://docs.google.com/document/d/1to_HkgJdLqtaENyG65NgKIyqRjEk_o9RB9_-LSEp5A0/edit?usp=sharing

Exploiting Disaggregation in Future 6G Cellular Networks

Institute for the Wireless Internet of Things
at Northeastern University

O-RAN Example: Disaggregated Architecture

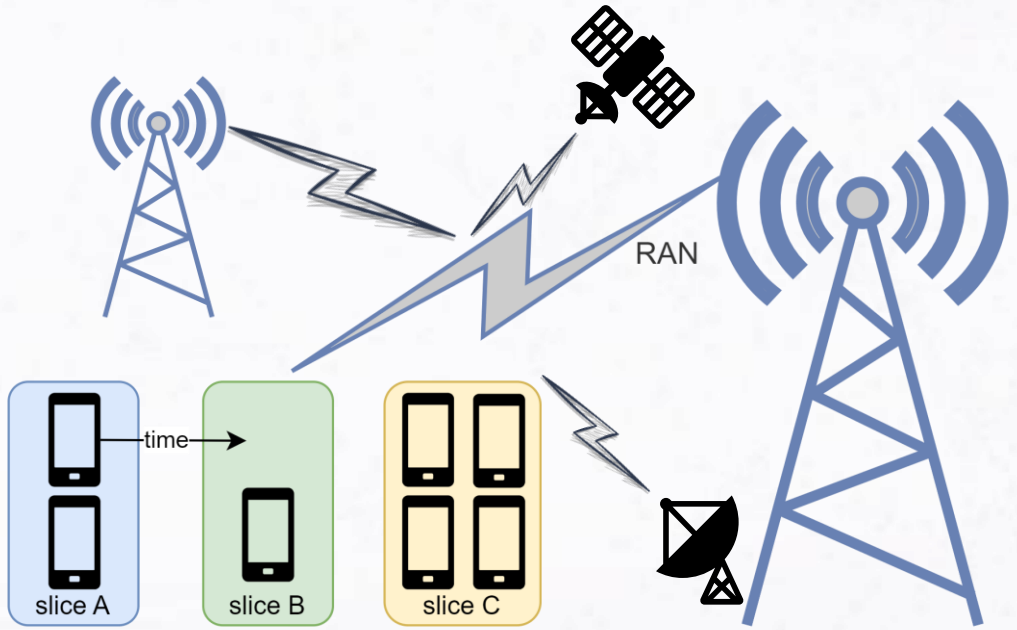


J. Groen, S. D'Oro, U. Demir, L. Bonati, D. Villa, M. Polese, T. Melodia, and K. R. Chowdhury, "Securing O-RAN Open Interfaces," IEEE Transactions on Mobile Computing, accepted, April 2024. PDF

O-RAN Background: Disaggregated Architecture

M. Belgiovine, J. Gu, J. Groen, U. Demir, and K. R. Chowdhury, "MEGATRON: Machine Learning in 5G with Analysis of Traffic in Open Radio Access Networks," *International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2024.

The growing demand on finite spectrum resources necessitates innovative interference detection and mitigation strategies.

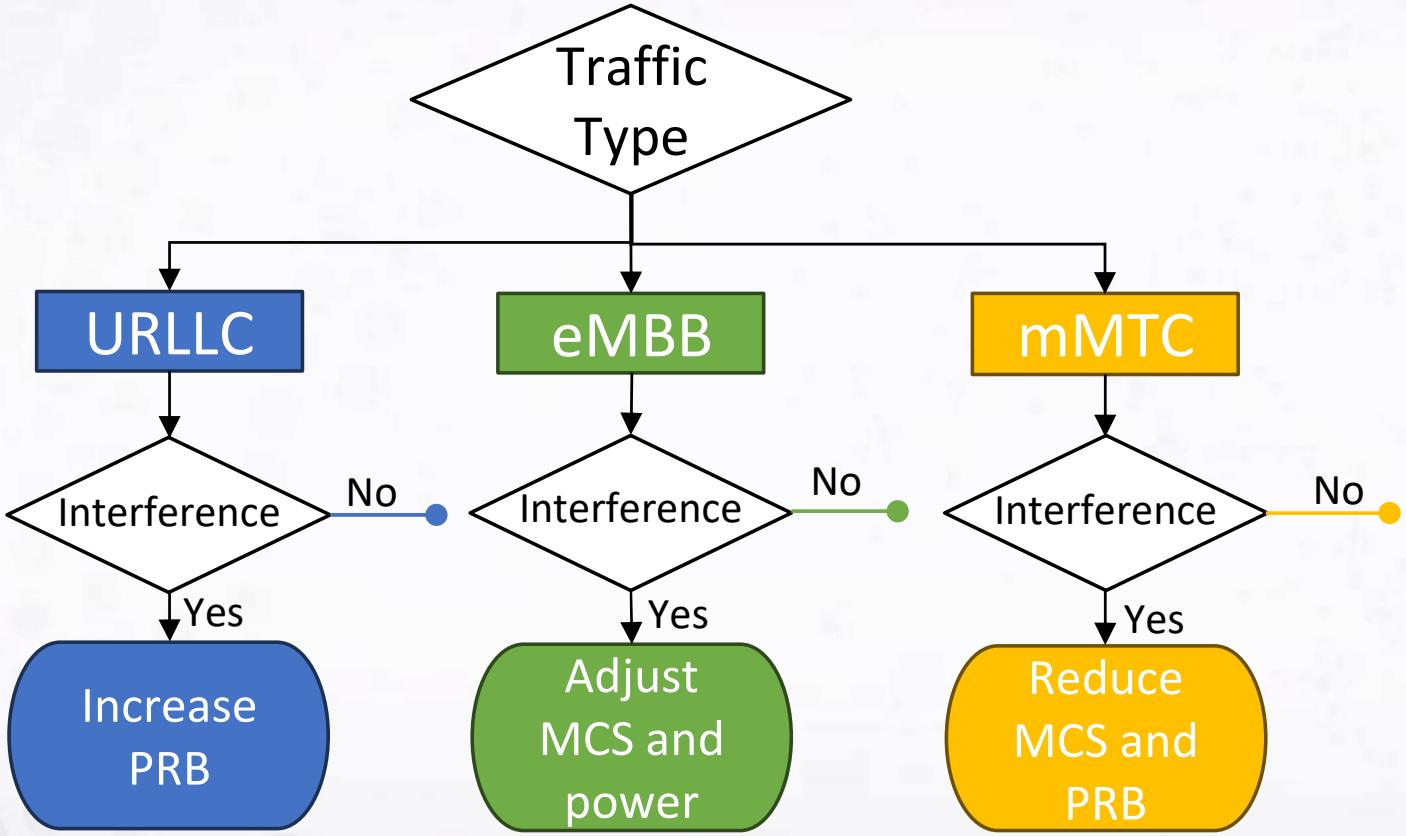


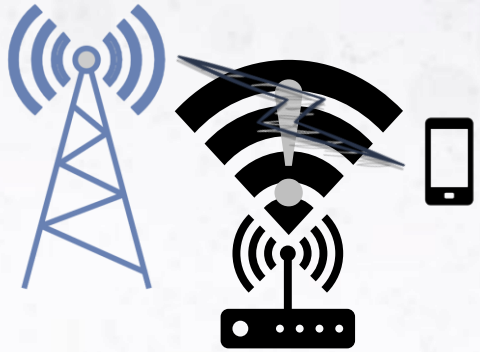
A. Chiejina, B. Kim, K. Chowdhury, and V. K. Shah, System-level Analysis of Adversarial Attacks and Defenses on Intelligence in O-RAN based Cellular Networks, in *ACM WiSec 2024*.

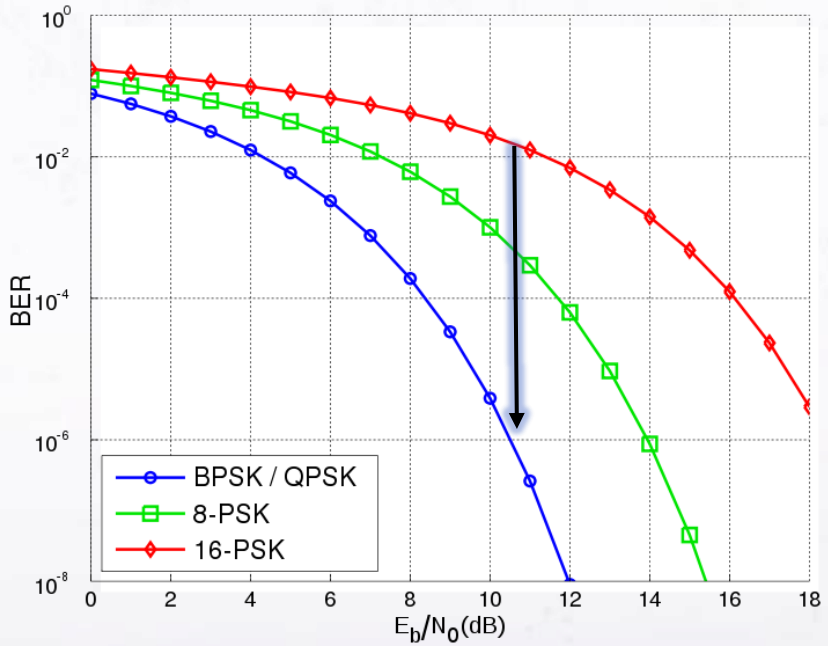
Institute for the Wireless Internet of Things at Northeastern University

Complex Relationships Between Parameters

14



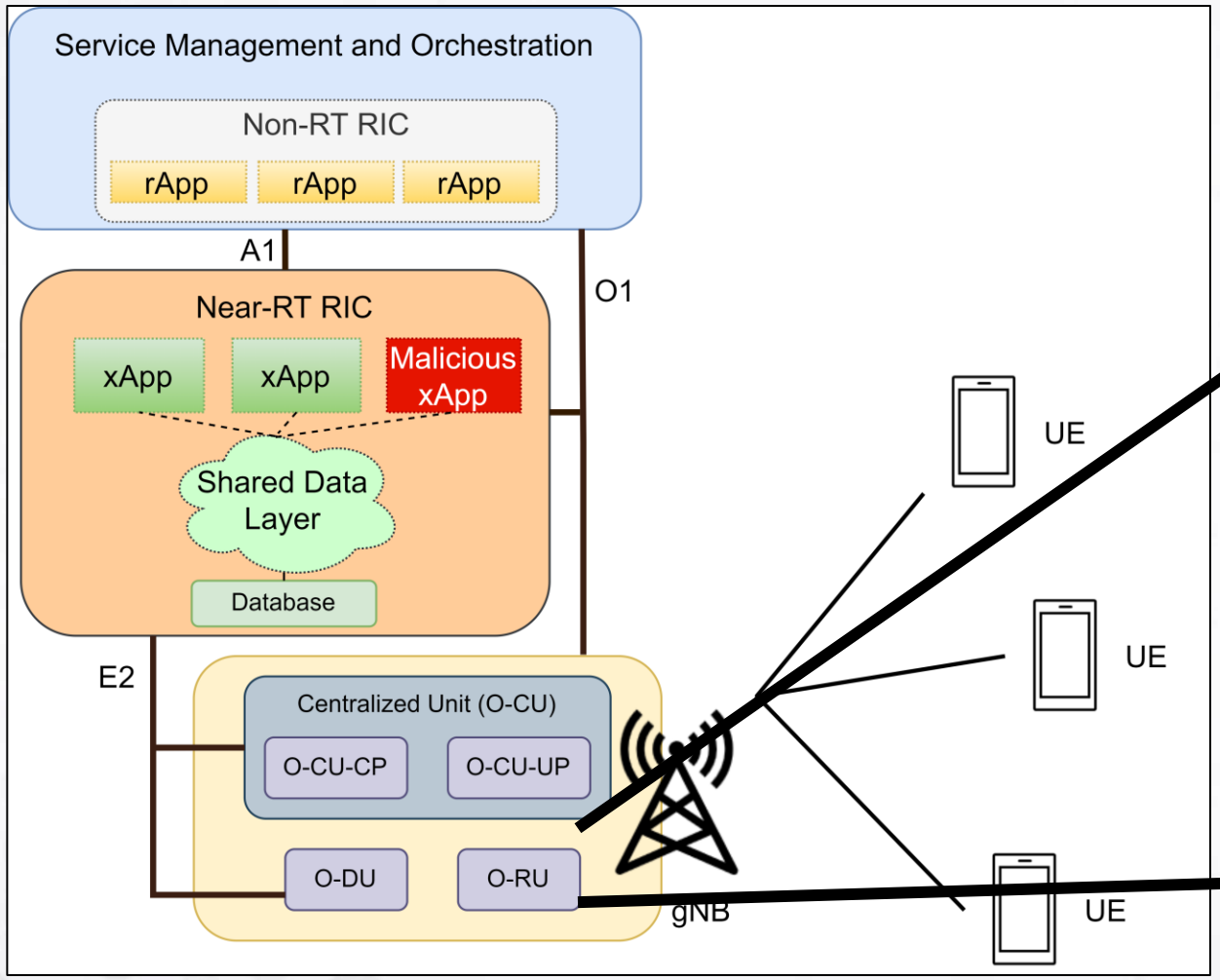




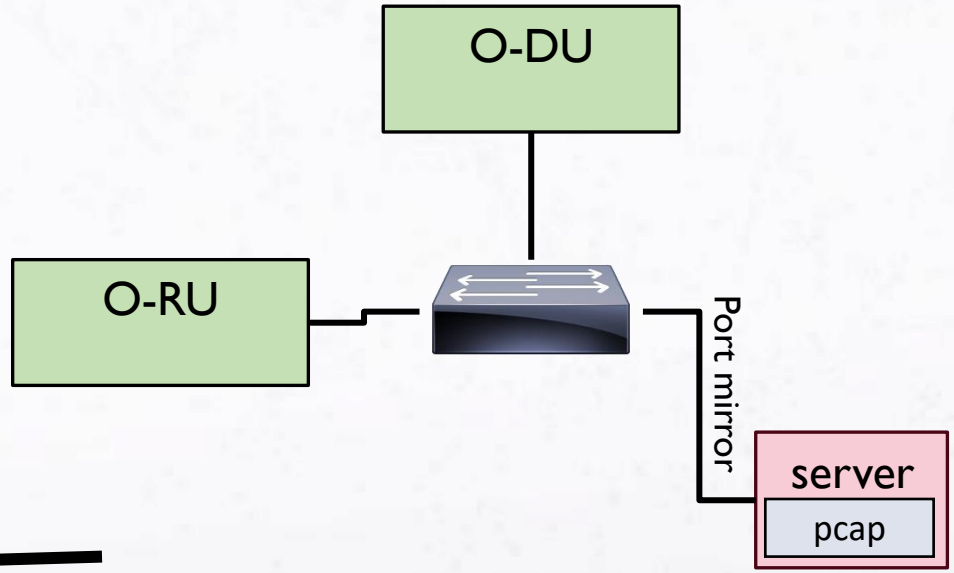
J. Groen, A. Chiejina, W. Liu, D. Muruganandham, V. K. Shah, K. R. Chowdhury, "IMPACT xApp: Interference Mitigation with POwer Adaptation and Classification of Traffic", RIC Forum 2024 - NTIA Institute for Telecommunication Sciences RIC Forum, Dallas, TX, USA, Mar. 2024. PPT

O-RAN Security #1 : Disaggregated Architecture

15

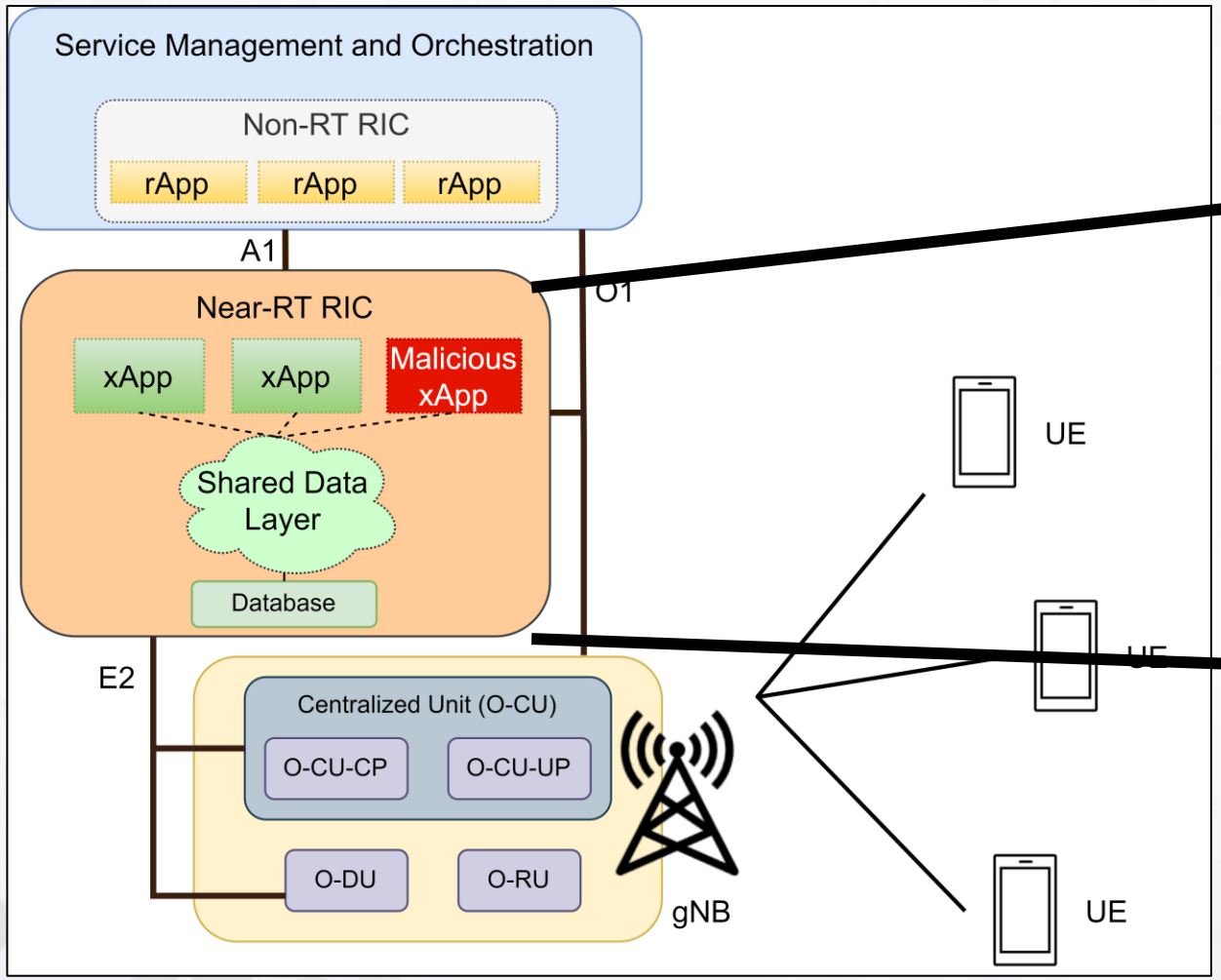


Private 5G network implementing 7.2x split



J. Groen, B. Kim, and K. R. Chowdhury, "The Cost of Securing O-RAN," IEEE Intl. Communications Conference (ICC), May. 2023. PDF

O-RAN Security #2 : Radio Intelligence Controller (RIC)



- RAN Intelligent Controllers
- Run custom intelligence, management and control of the network
- Near-Real-Time (10ms-1s)
- Non-Real-Time (>1s)

Y. Rumesh, D. Attanayaka, P. Porambage, J.E. Pinola, J.B. Groen, and K. Chowdhury, "Federated Learning for Anomaly Detection in Open RAN: Security Architecture Within a Digital Twin," 2024 EuCNC & 6G

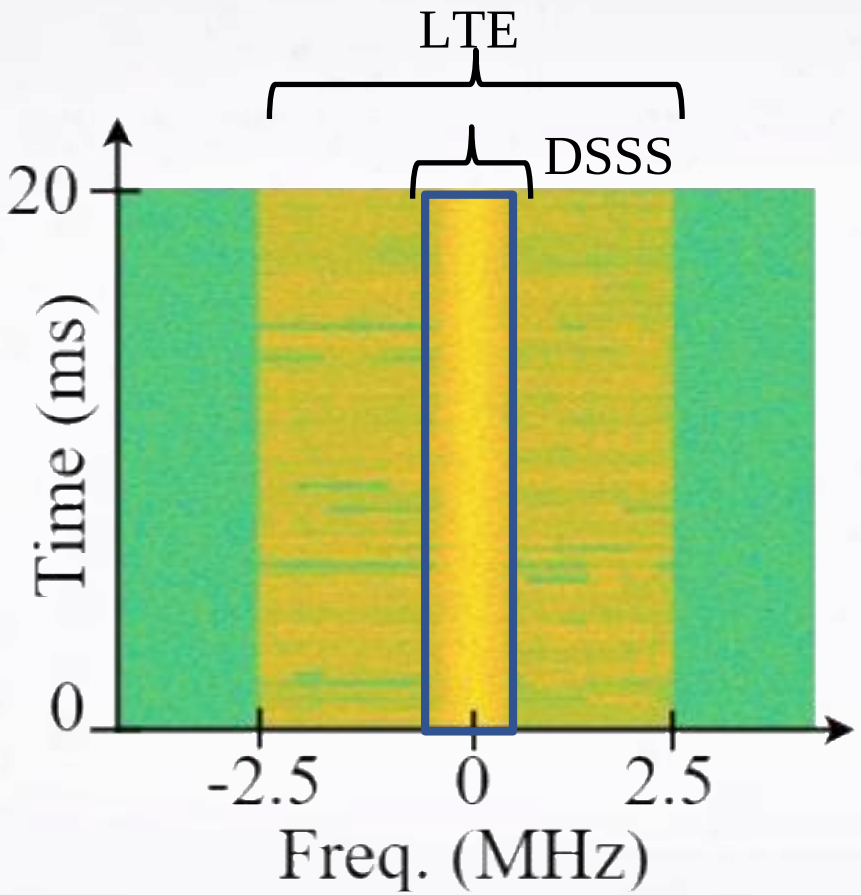
Jamming and Anomalous Signals

Institute for the Wireless Internet of Things
at Northeastern University

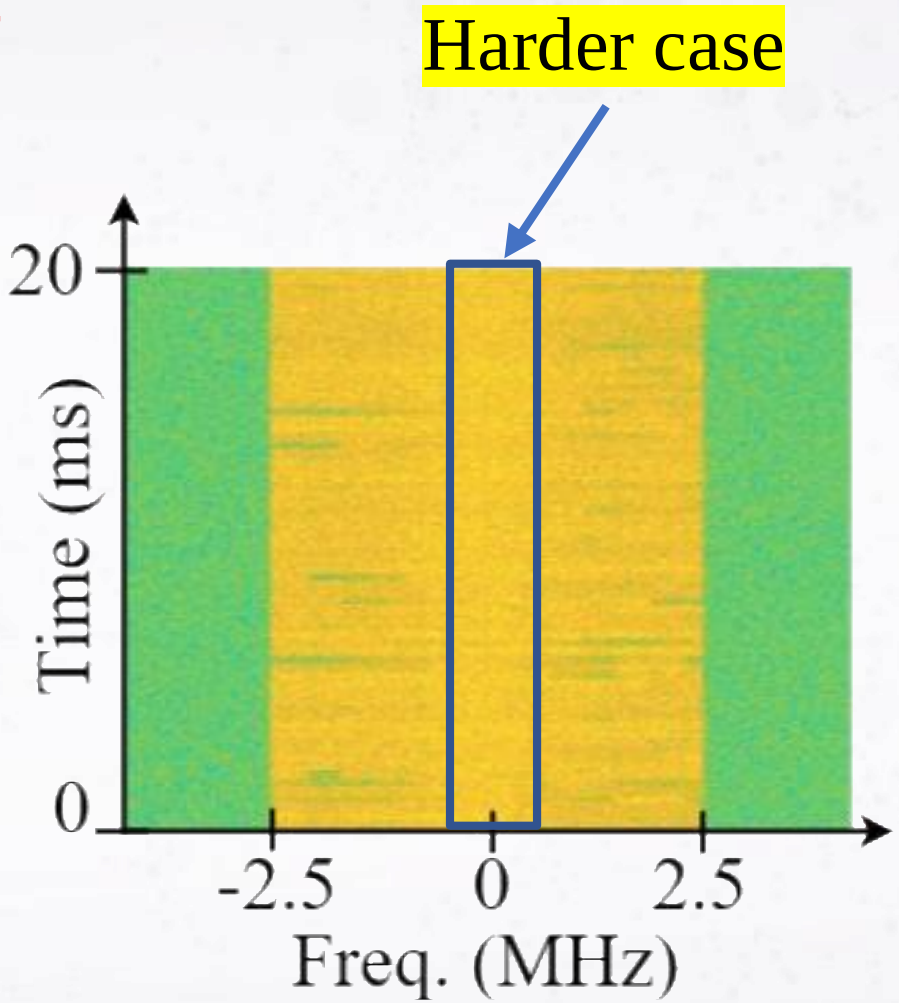
Distributed Jamming

S. Mohanti, C. Bocanegra, S. Garcia, K. Alemdar, and K. R. Chowdhury, “SABRE: Swarm-based Aerial Beamforming Radios: Experimentation and Emulation,” IEEE Transactions on Wireless Communication, vol. 22, no. 9, pp. 7460-7475, Sept. 2022. PDF

Anomalous Signal #1: “Noise-like” Spread Spectrum



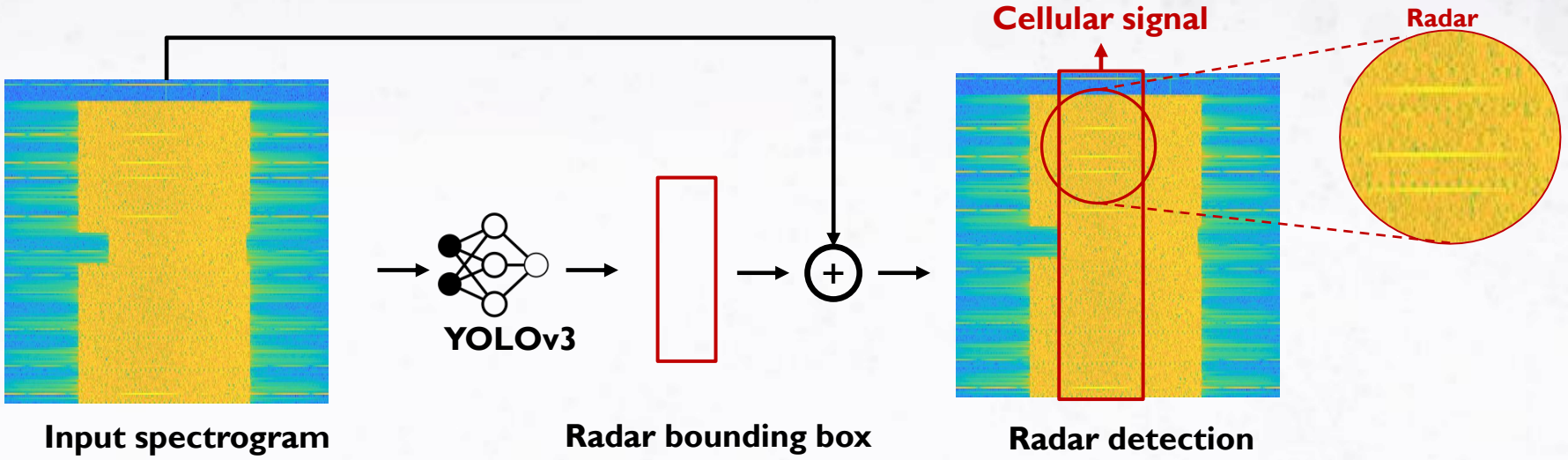
Signal to Interference (SIR)
Ratio -0.91 dB



Signal to Interference (SIR)
Ratio -0.091 dB

D. Roy, V. Chaudhary, C. Tassie, C. Spooner, and K. R. Chowdhury, “ICARUS: Learning on IQ and Cycle Frequencies for Detecting Anomalous RF Underlay Signals,” IEEE Conference on Computer Communications (INFOCOM), May. 2023. PDF

Anomalous Signal #2: Radar

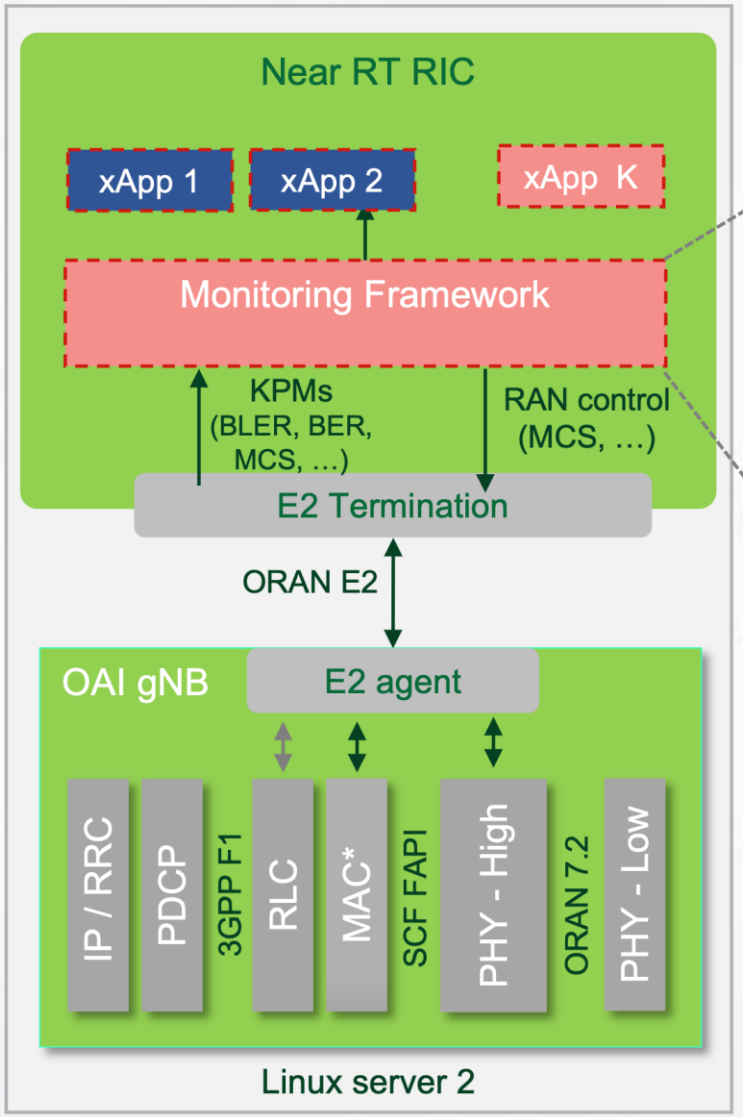


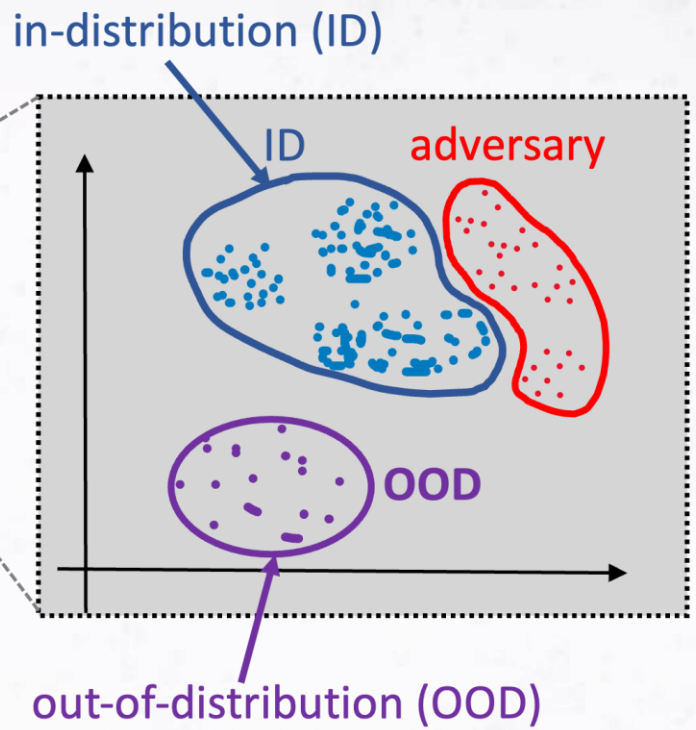
G. Reus-Muns, P. Upadhyaya, U. Demir, N. Stephenson, N. Soltani, V. K. Shah, K. R. Chowdhury, "SenseORAN: O-RAN based Radar Detection in the CBRS Band," IEEE Journal on Selected Areas in Communications (JSAC), July 2023. PDF

N. Soltani, V. Chaudhary, D. Roy, and K. R. Chowdhury, "Finding Waldo in the CBRS Band: Signal Detection and Localization in the 3.5 GHz Spectrum," IEEE Global Communications Conference (Globecom), Dec. 2022. PDF

Next Steps and Open Research Challenges

Designing a Threat Analysis Framework





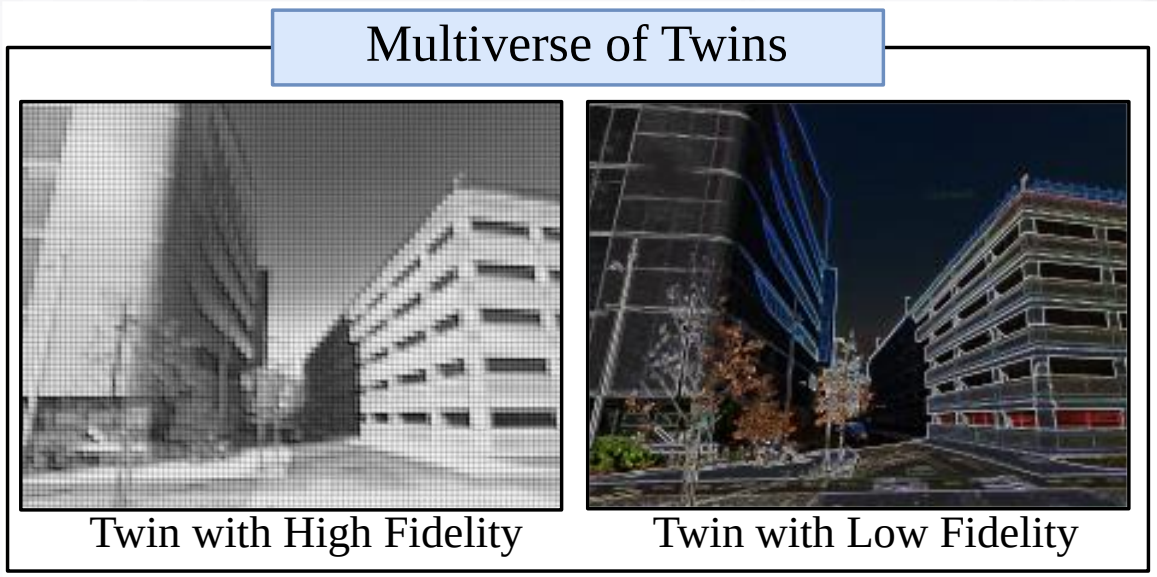
Open-source IP

Existing xApp

Proposed work

Institute for the Wireless Internet of Things at Northeastern

Creating Digital Twins for Macro-Behavior Modeling



Detect Unseen Scenarios

↓

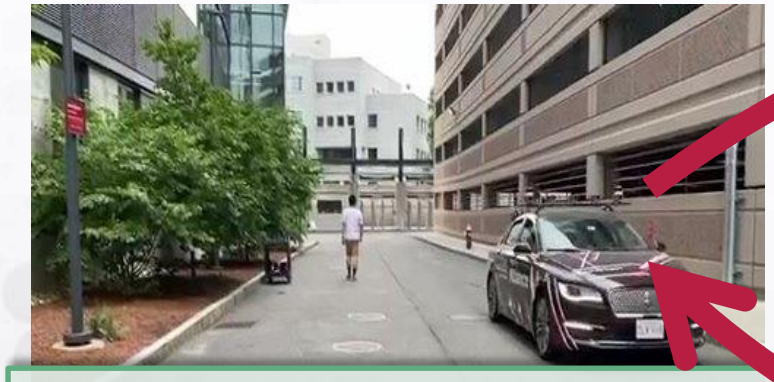
Create a Digital World

↓

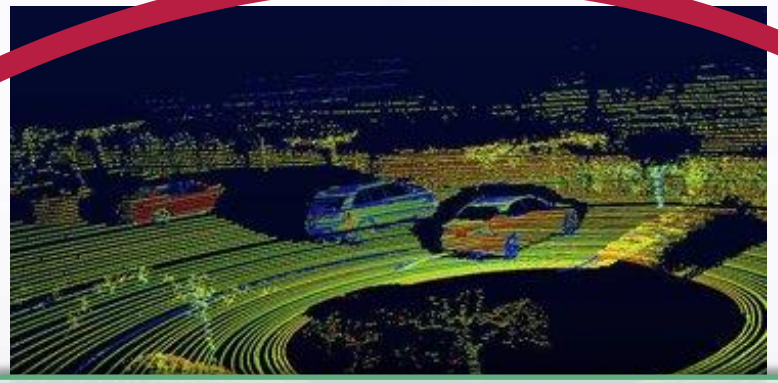
Run Ray Tracing

↓

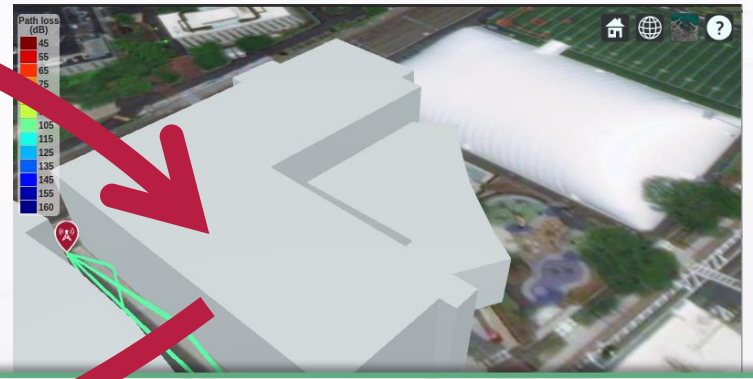
Beam Profiles



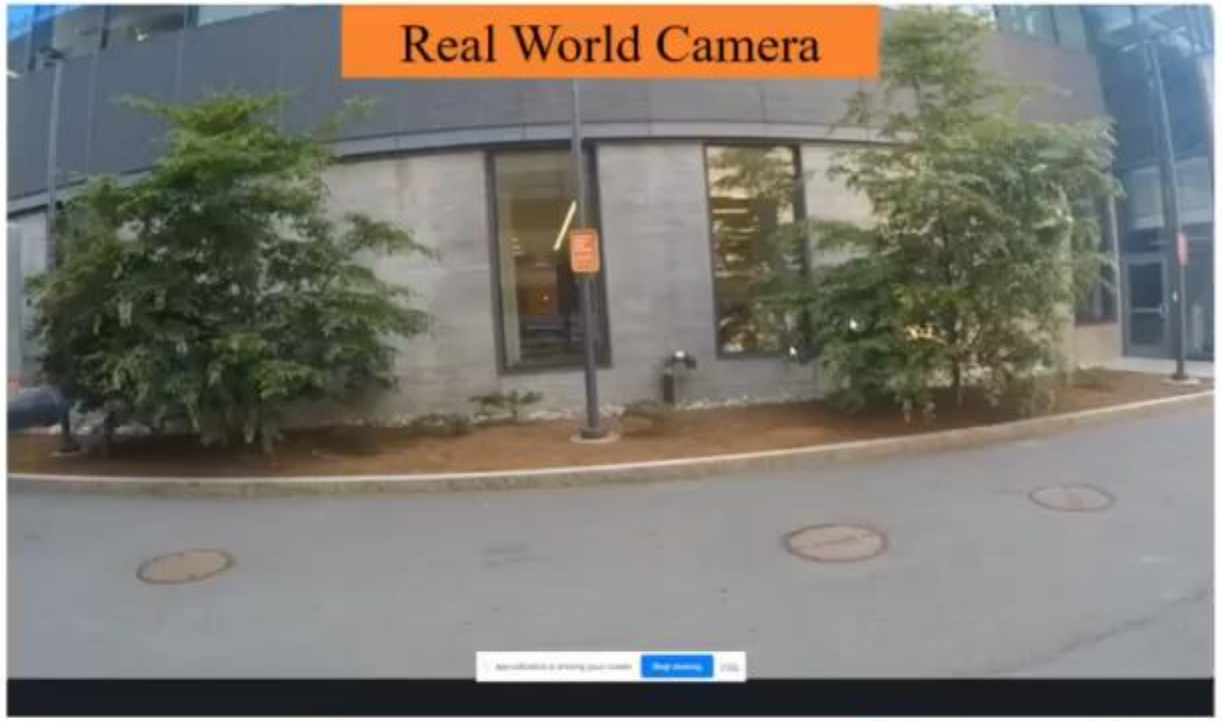
Step 1. Trained DL models for local decisions- mmWave beamforming using fusion of LiDAR, Camera, GPS

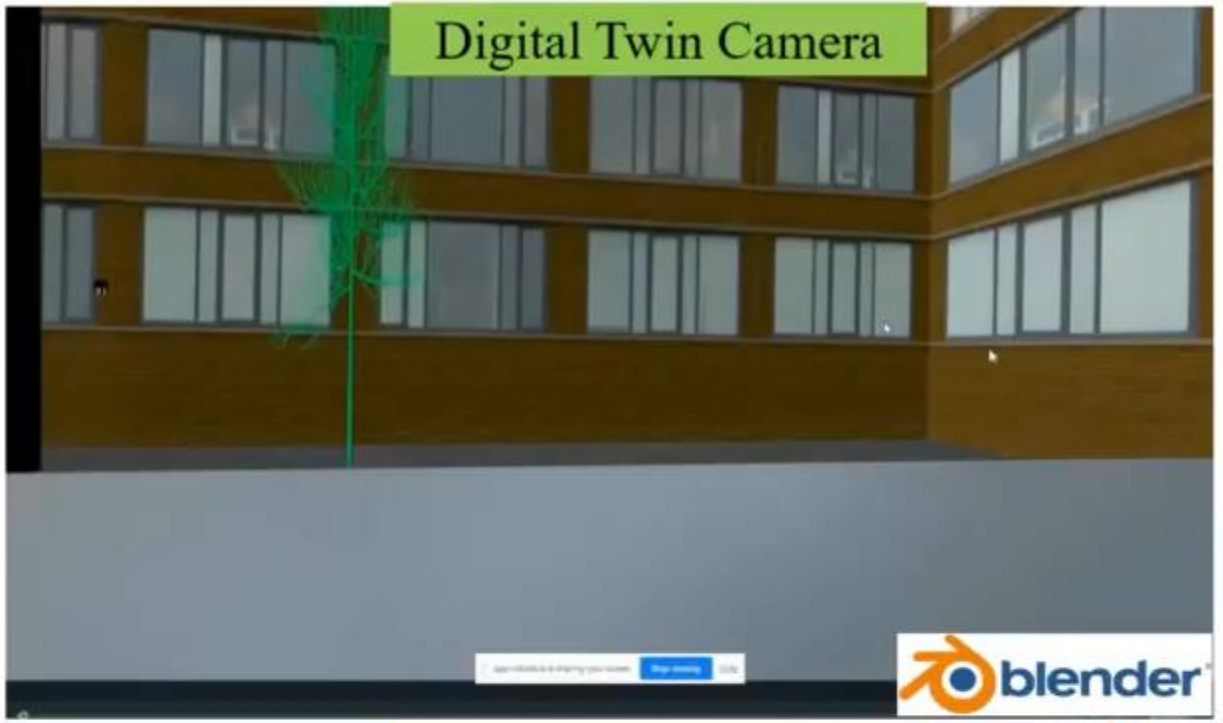


Step 2. Measuring the prediction confidence to detect unseen scenarios

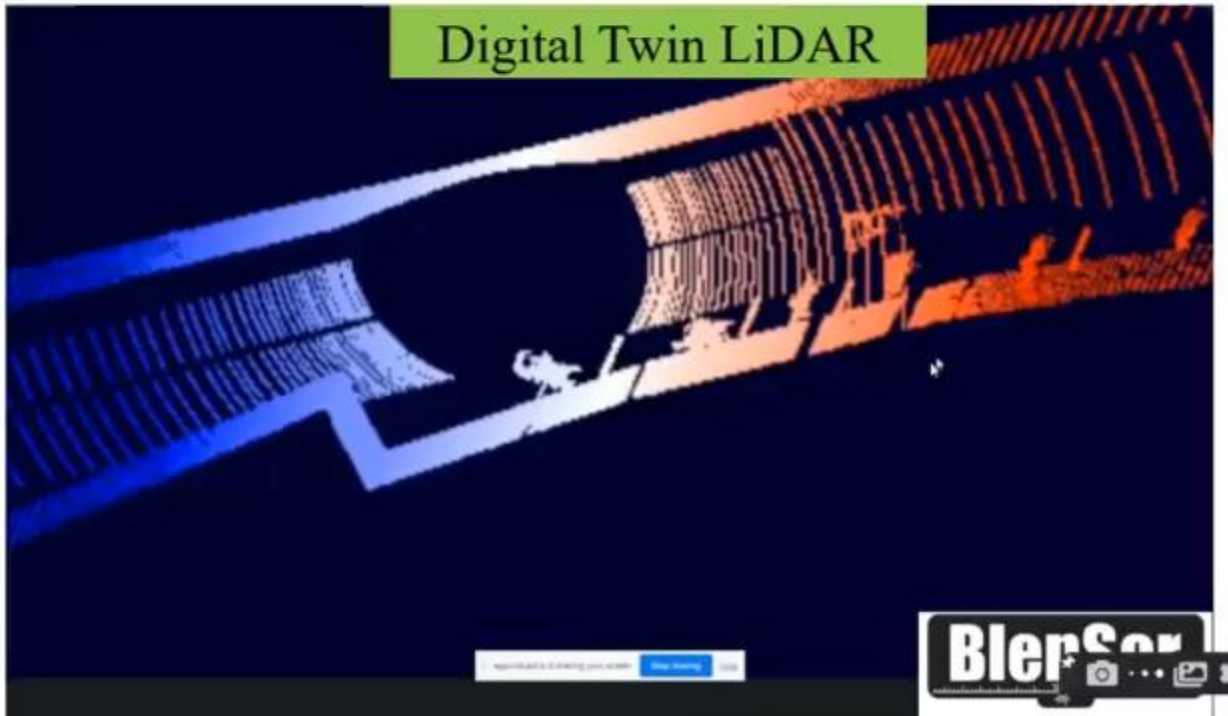


Step 3. Relay new conditions to Edge, predict optimal beam via GPU accelerated ray tracing, update CNN

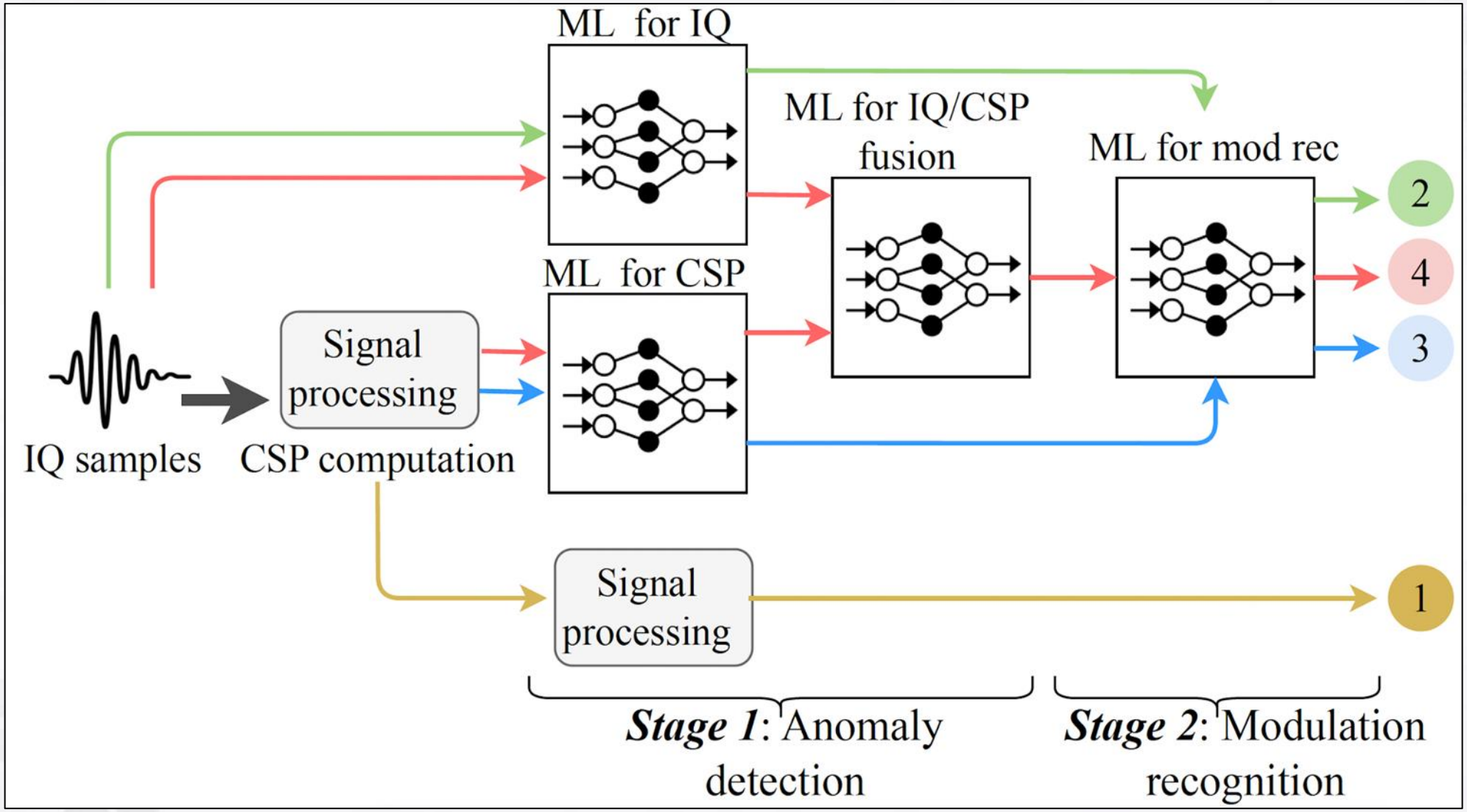

Real World Camera


Digital Twin Camera
blender


Real World LiDAR

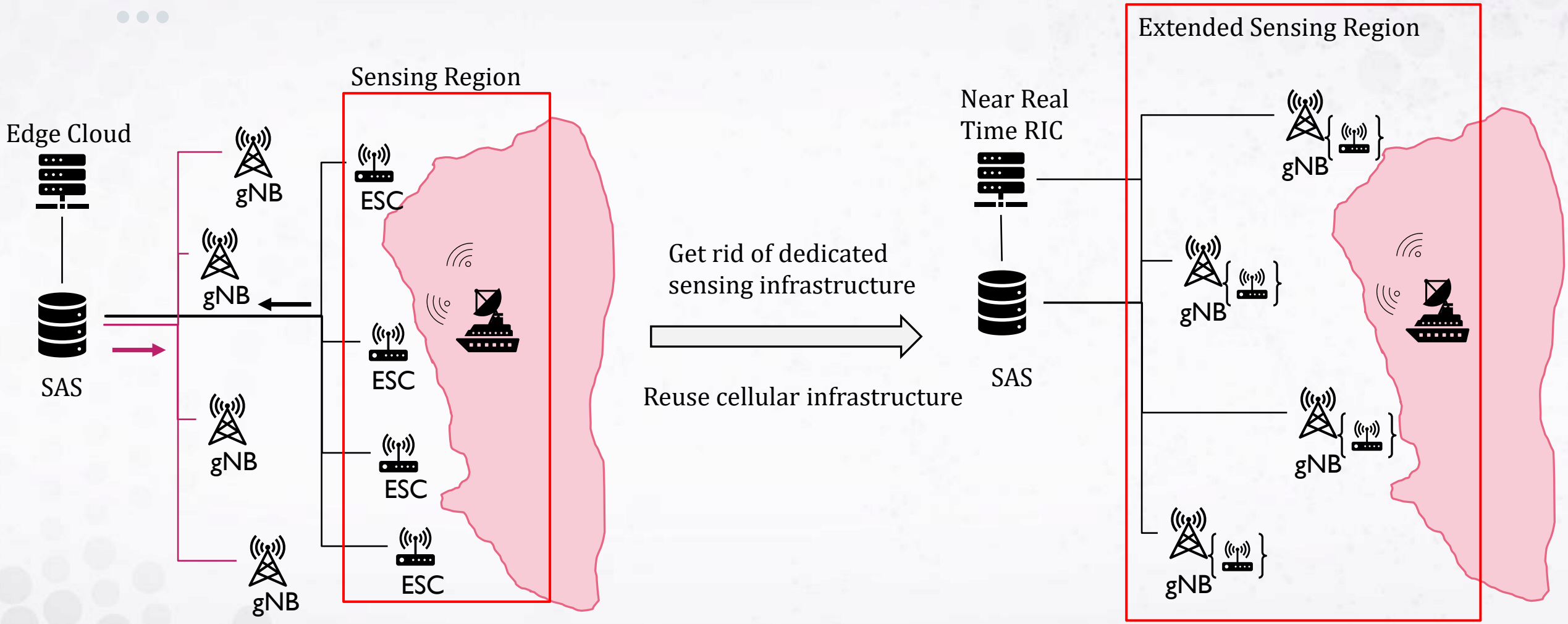

Digital Twin LiDAR

Multi-modal Signal Analysis



Base Stations as “Sensors”, Distributed Sensing

26



Institute for the Wireless Internet of Things
at Northeastern University

Q&A