INL/MIS-23-70961-Revision-0

5G Security and AI/ML

January 2023

Arupjyoti Bhuyan

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-23-70961-Revision-0

5G Security and AI/ML

Arupjyoti Bhuyan

January 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Dr. Arupjyoti (Arup) Bhuyan

Director, INL Wireless Security Institute (WSI)

5G Security and AI/ML

Idaho National Laboratory

INL Wireless Security Institute (WSI)

VISION: National Leadership on Wireless Security for Secure Adoption of Advanced Technologies including 5G, NextG/6G, Wi-Fi 6E and related Spectrum

MISSION: Provide best in class security research, assessments, evaluations, engineering support, and technology development to enable government and industry harvest the benefits of advanced wireless technologies

Innovative Research

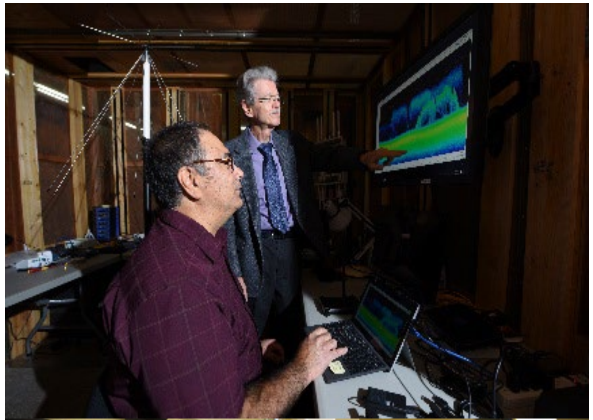
- Lab directed research on security of advanced technologies and secure spectrum use and sharing
- USG funded research, analysis, and engineering studies to address national security gaps in secure use of 5G & NextG technologies and spectrum
- Proof of Concept for development and deployment of secure real-world use cases with transformational technologies

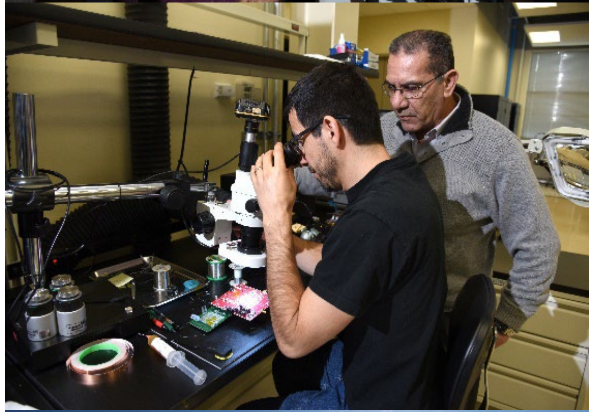
Evaluation & Validation

- Effective, accurate, responsive testing and verification
- Advanced Lab based systems for highly efficient and intrusive testing
- Unique Wireless Test Bed (WTB) with outdoor environment providing capability to test real world scenarios at scale
- WTB Spectrum flexibility with NTIA experimental station status

External Collaborations

- Academic and Industry Researchers in US
- Hosting of National Security workshops and Conference Tracks addressing key security topics with participation from US Government, Industry, and Academia
- International collaboration with wireless leaders in US Government partner countries





NOTABLE OUTCOMES: Diversely Funded RDD&D Portfolio supported by WSI as a National Authority on Wireless Security and utilizing resources across INL to exceed customer expectation

INL Wireless Security Workshops - National Leadership and Collaboration

- **Fifth WSI Workshop,** Salt Lake City, Sep 7-8, 2022: Wireless Security considerations for the Aviation Sector, sponsored by the Aviation Cybersecurity Initiative (ACI)
- **Fourth WSI Workshop,** VIRTUAL, March 30-21, 2022: Security of 5G connected vehicles critical to DoD, DOT and others; Summary of R16 3GPP security standards
- **Third WSI Workshop,** VIRTUAL, Jun 16-17, 2021: Security challenges in Open RAN and Open 5G; Initial discussion on 6G security
- **Second WSI Workshop,** VIRTUAL, Nov 17-18, 2020: Security challenges and progress: 1) 5G Devices and Network; 2) Cellular Drones; 3) 5G Shared and Unlicensed Spectrum; Virtual tours of 7 leading national 5G facilities
- **First WSI Workshop,** Salt Lake City, Feb 27-28, 2020: Security and spectrum challenges in securely harnessing the power of 5G; Tour of UofU' s Platform for Open Wireless Data-driven Experimental Research (POWDER)

Published recommendations on 1) critical 5G security challenges to be addressed; 2) 3GPP security improvements and necessary work to ensure their proper utilization; and 3) approaches to engage with U.S. Government (USG) to secure 5G

WSI Collaborators

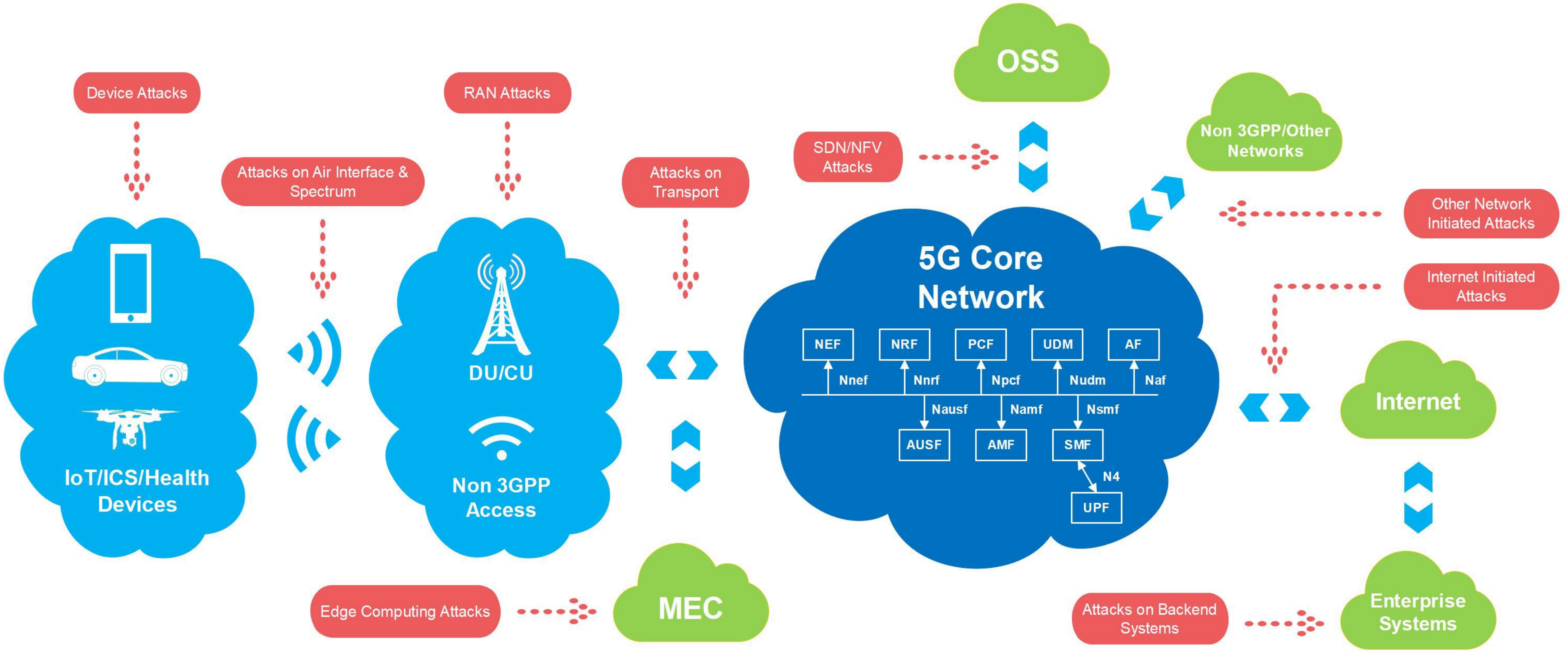
- **University partners —** Univ. of Utah, NCSU, FIU, Mississippi State, VCU, Utah State, UTSA, BSU, ISU, Univ. of Idaho, Virginia Tech, Purdue, University of California San Diego (UCSD), University of Southern California (USC)

- **Industry partners —** QC, Verizon Wireless, Ericsson, Nokia, Mavenir

Summary of Key WSI Programs

- DOD OUSD: 5G Operate Through Program (Untrusted Operators)
- DOJ: Spectrum agile video surveillance communications
- DHS/FAA: Aviation Cyber Initiative (ACI)
- NTIA/ITS: 2022 Open 5G Challenge - Security Subject Matter Expert (SME)
- DOE-CIO: Lead two of five nationwide Advanced Technology Initiatives on secure use of Advanced Wireless Technologies
- NSF: Collaboration with ISI/USC and Univ of Utah for two projects awarded in Phase 1 of Spectrum Innovation Initiative National Radio Dynamic Zones (SII-NRDZ)
- Internal R&D Investment: Lab Directed R&D (LDRD) research on Secure Wireless Communications and Dynamic Spectrum Sharing with university collaboration

5G Network & Attack Surfaces

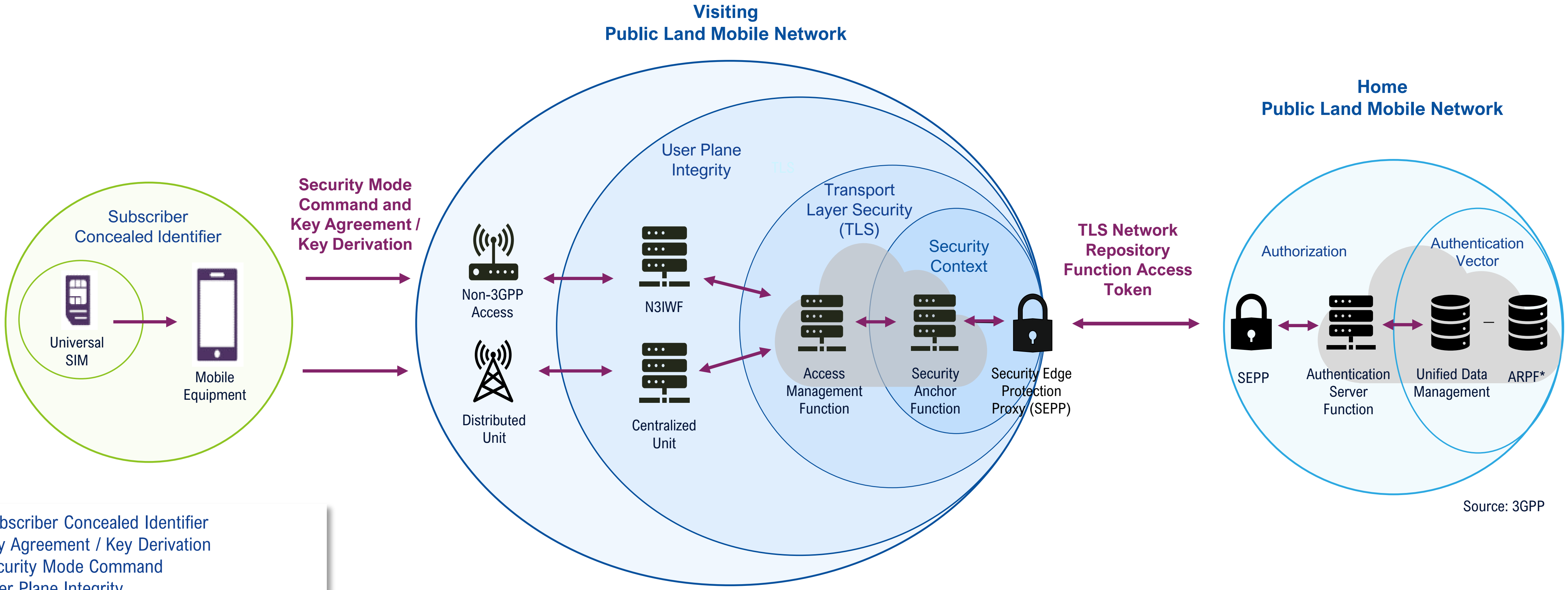


IoT: Internet of Things
ICS: Industrial Control System

MEC: Multi-access Edge Computing

SDN: Software Defined Networking
NFV: Network Function Virtualization
OSS: Operational Support System

5G Security Improvements (3GPP SA3)



Source: 3GPP

SUCI	Subscriber Concealed Identifier
Ka/Kd	Key Agreement / Key Derivation
SMC	Security Mode Command
UPI	User Plane Integrity
AMF	Access Management Function
SEAF	Security Anchor Function
TLS	Transport Layer Security
SEPP	Security Edge Protection Proxy
Auth	Authorization
AV	Authentication Vector
UDM	Unified Data Management
ARPF	Authentication Credential Repository and Processing Function
NRF	Network Repository Function

Needed 5G Security for Mission Critical Communication

- Optional 3GPP security procedures*
  - ✓ User plane encryption
  - ✓ Integrity Protection for user data
- 5G Network Slicing for customized security policy
  - ✓ Secondary authentication
  - ✓ Authentication, Authorization and Accounting Server (AAA-S)
- 5G Network Configurations
  - ✓ Certificate management
  - ✓ Encryption scheme (avoidance of Null Encryption)
- Application layer solutions – Security Apps
- ***AI/ML based solutions for detection and mitigation of attacks including zero-day attacks***

* Reference: CSRIC Report on RECOMMENDATIONS FOR IDENTIFYING OPTIONAL SECURITY FEATURES THAT CAN DIMINISH THE EFFECTIVENESS OF 5G SECURITY

3GPP Network Data Analytic Function (NWDAF)

The NWDAF provides analytics to 5GC NFs and OAM (3GPP TS 23.288, TS 29.520 in Release 17)

- DCCF: Data Collection and co-ordinating function
- MFAF: Messaging Framework Adaptor Function
- ADRF: Analytics Data Repository Function
- AnLF: Analytics logical function - performs inference, derives analytics information (i.e. derives statistics and/or predictions)
- MTLF: Model Training logical function trains Machine Learning (ML) models and exposes new training services (e.g. providing trained ML model)
- OAuth2 protocol is used with Network Repository Function (NRF) as authorization server

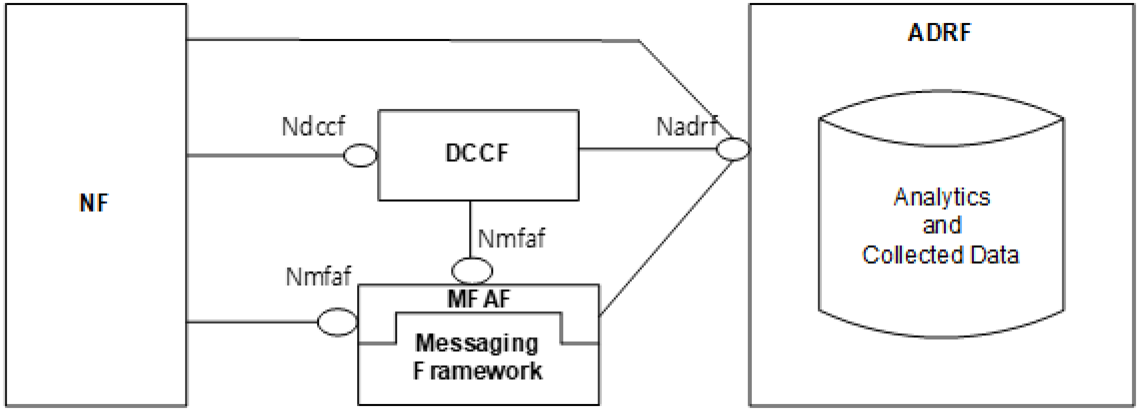
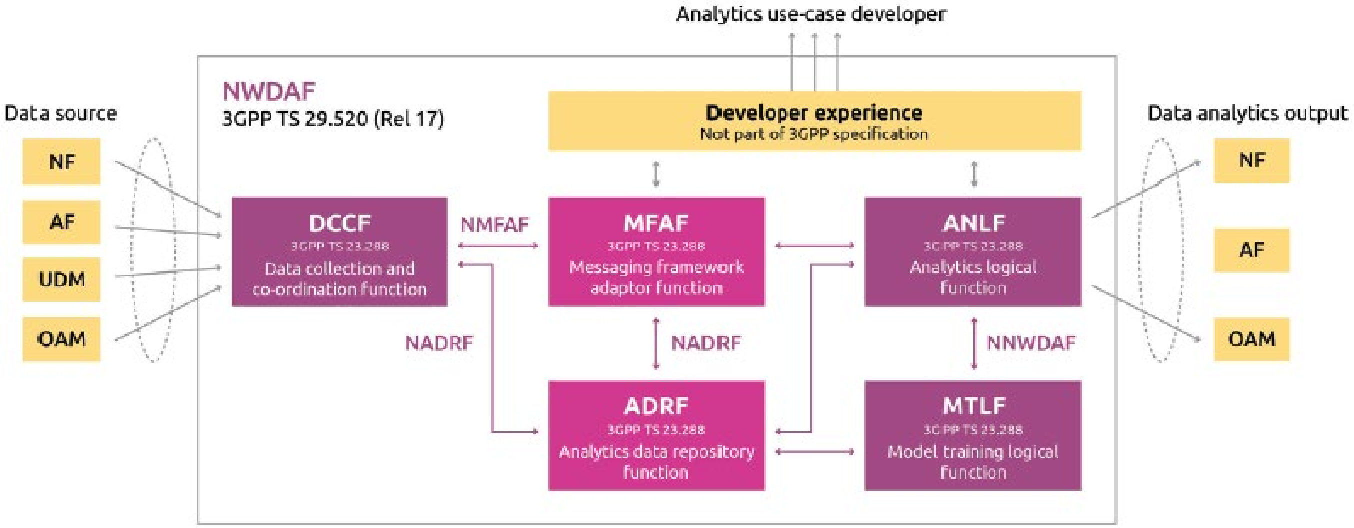


Figure 4.2.1-1: Data storage architecture for Analytics and Collected Data

TS 23.288


Analytics use-case developer
Data source
NF
AF
UDM
OAM
NWDAF
3GPP TS 29.520 (Rel 17)
Developer experience
Not part of 3GPP specification
DCCF
3GPP TS 23.288
Data collection and co-ordination function
NMFAF
MFAF
3GPP TS 23.288
Messaging framework adaptor function
ANLF
3GPP TS 23.288
Analytics logical function
NADRF
NADRF
NNWDAF
ADRF
3GPP TS 23.288
Analytics data repository function
MTLF
3GPP TS 23.288
Model training logical function
Data analytics output
NF
AF
OAM

From Capgemini Engineering NWDAF component-level architecture – source 3GPP

Supported data analytics in R17 TS 23.288

- Network Slice load level information (not subscriber specific)
- Service experience for a Network Slice and Application
- Network Function load analytics (can be UE/SUPI specific)
- Network Performance Analytics for a single or group of UEs located in an “Area of Interest”
- UE related analytics including **“Abnormal Behaviour”**
- User Data Congestion based on UE Identity
- QoS sustainability over a period of time
- Dispersion analytics to identify location where UE(s) are active
- Performance of WLAN connection of UE
- User plane performance (rate, delay, packet loss) for UE(s) associated with a UPF
- Session management Congestion Control & Redundant Transmission

Open RAN Architecture

O-RAN ALLIANCE WHITE PAPER

O-RAN Minimum Viable Plan and Acceleration Towards Commercialization

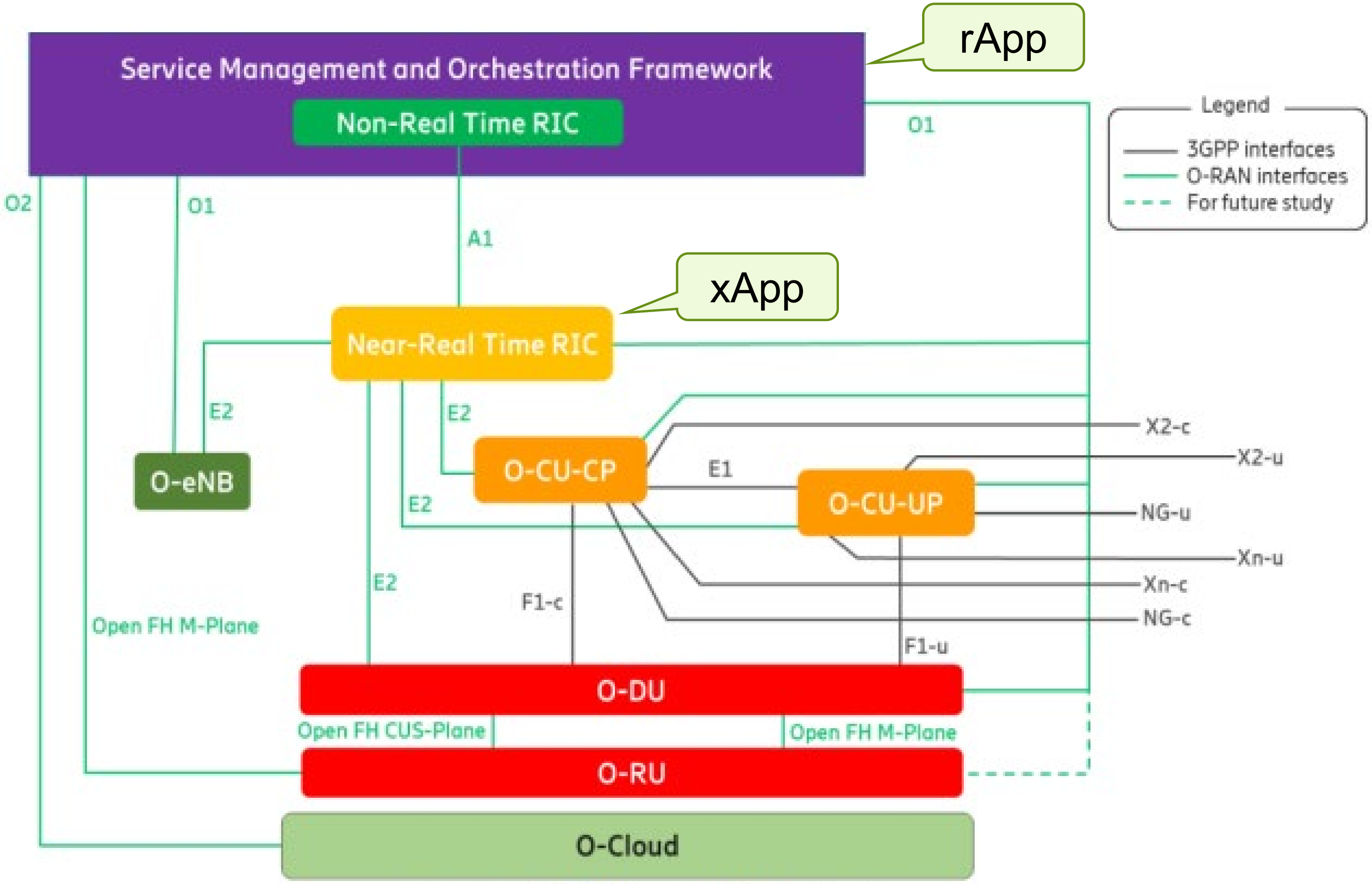


Figure 2: O-RAN Logical Architecture

LDRD: 5G Attack Detection Implementation with Machine Learning

- INL LDRD: Matthew Anderson, PI
- 3rd party attacks on 5G core network exploiting implementation vulnerabilities
  - ✓ Reconnaissance: Information extraction
  - ✓ Network reconfiguration: 5GC Network Function (NF) insertion and deletion
  - ✓ Denial of Service (DOS): Crashing NF with malformed request
- Autoencoder and a β-variational autoencoder trained with normal data deployed on FPGA evaluation boards
- Inference accuracy and performance compared with NVIDIA A100 GPU implementation
- 5GAD-2022: Dataset of 5G network traffic for use with machine learning tools to benchmark attack detection https://github.com/IdahoLabResearch/5GAD
- Globecom 2022 Paper: Machine Learning 5G Attack Detection in Programmable Logic

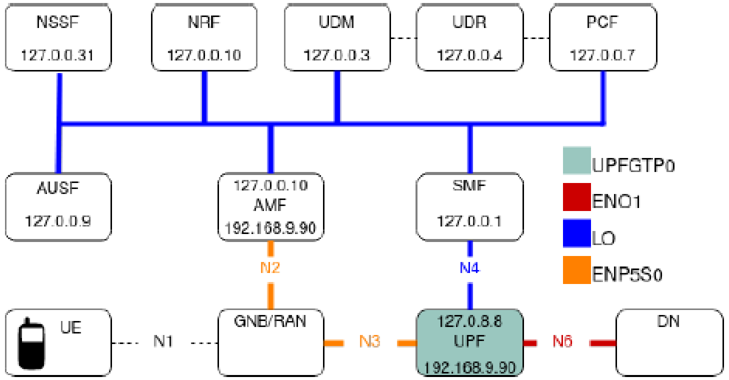


Fig. 1: The 5G Network with IP addresses as used in the 5GAD-2022 dataset.

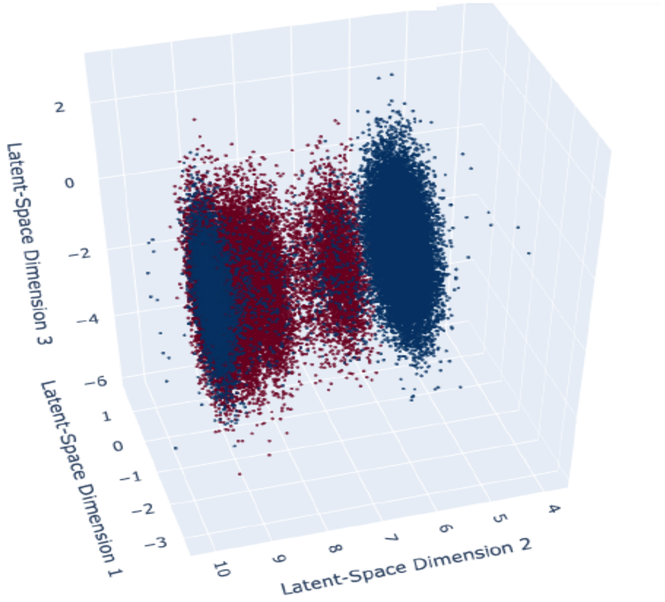
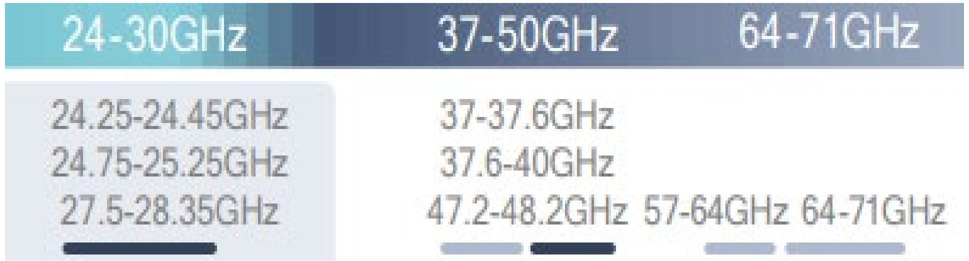


Fig. 3: Latent Space Generated from β-VAE. The red points represent anomalous packets and the blue points represent normal packets. Distinct clustering in the latent space between normal packets and anomalous packets is evident.

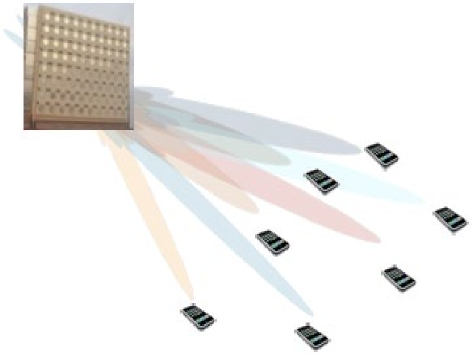
5G Spectrum – FCC Allocations

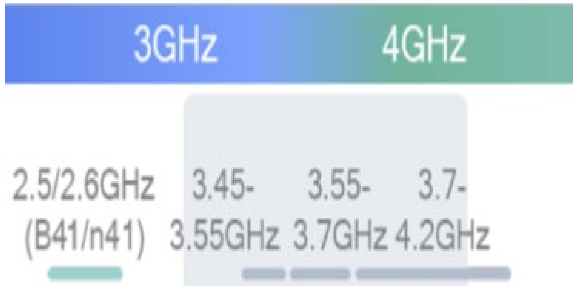
High-band (mmWave):

- ✓ 24 GHz, 28 GHz, upper 37 GHz (shared), 39 GHz, and 47 GHz bands – total of about 5 GHz licensed
- ✓ **Unlicensed**: 64-71 GHz: 7 GHz of new unlicensed spectrum, doubles existing 47-64 GHz band



From 3GPP 5G Implementation Guidelines, GSMA





Medium-band: 2.5 GHz, 3.3-3.45 GHz (shared with airborne radar), 3.45-3.55 GHz, 3.55-3.65 GHz (shared by CBRS PAL and GAA users), and 3.7-3.98 GHz/C Band, 5.905-5.925 GHz (C-V2X)

- ✓ **Unlicensed**: 5.925-7.125 GHz, 1200 MHz at 6 GHz (Wi Fi 6E, 5G-NR-U).

Wi-Fi
mmWave
Wi-Fi
mmWave
Wi-Fi
5G
mmWave
mmWave
Wi-Fi
mmWave
Wi-Fi
Sub-6 GHz

From https://www.androidauthority.com/what-is-5g-mmwave-933631/

Private 5G Networks

NR-U: New Radio in the Unlicensed Band, R16

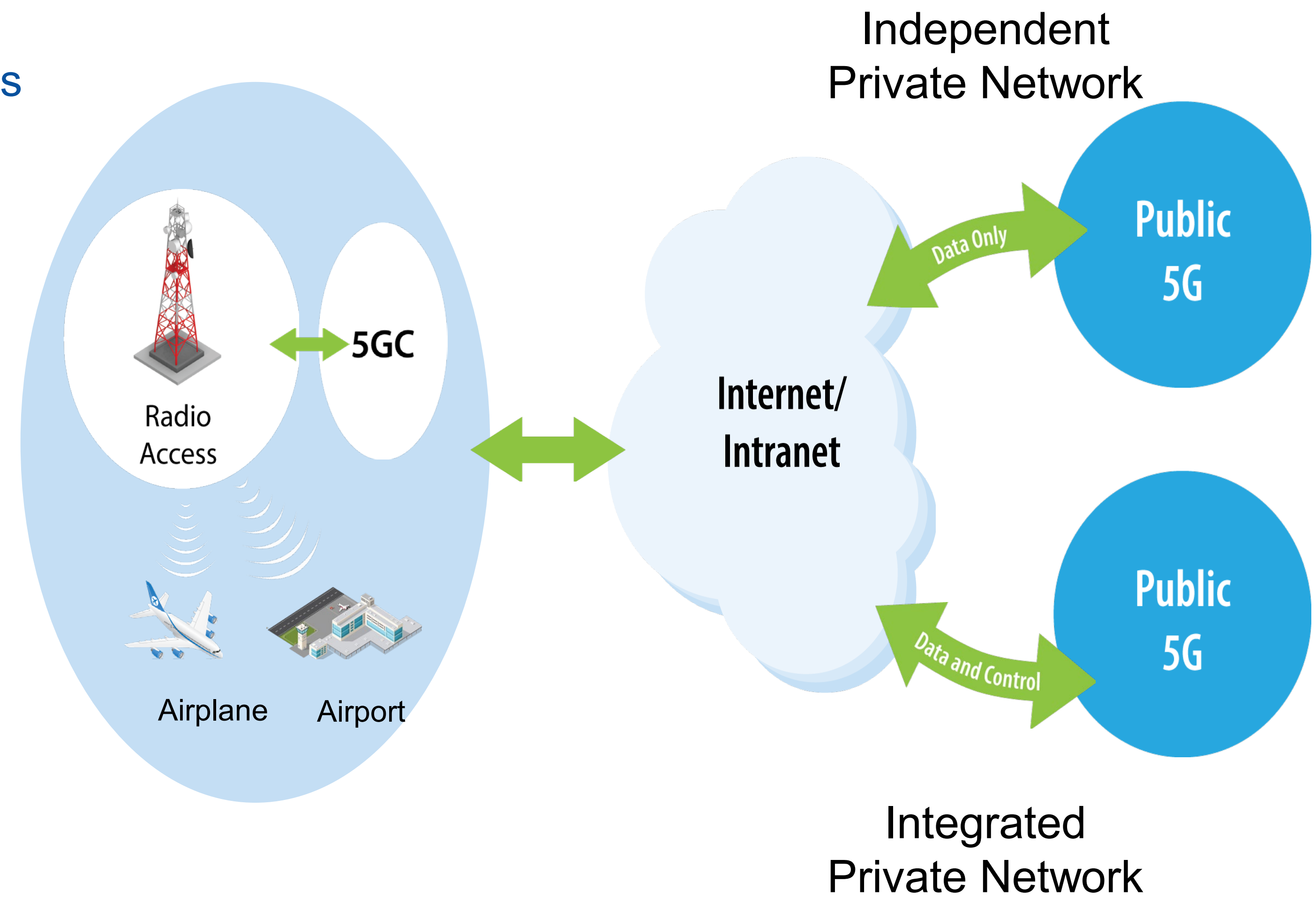
- ✓ Transformation of LTE Licensed Assisted Access (LAA)
- ✓ Standalone mode with **no licensed spectrum**

Network Configurations

- ✓ Isolated and Independent
- ✓ Hybrid - Integrated with public network

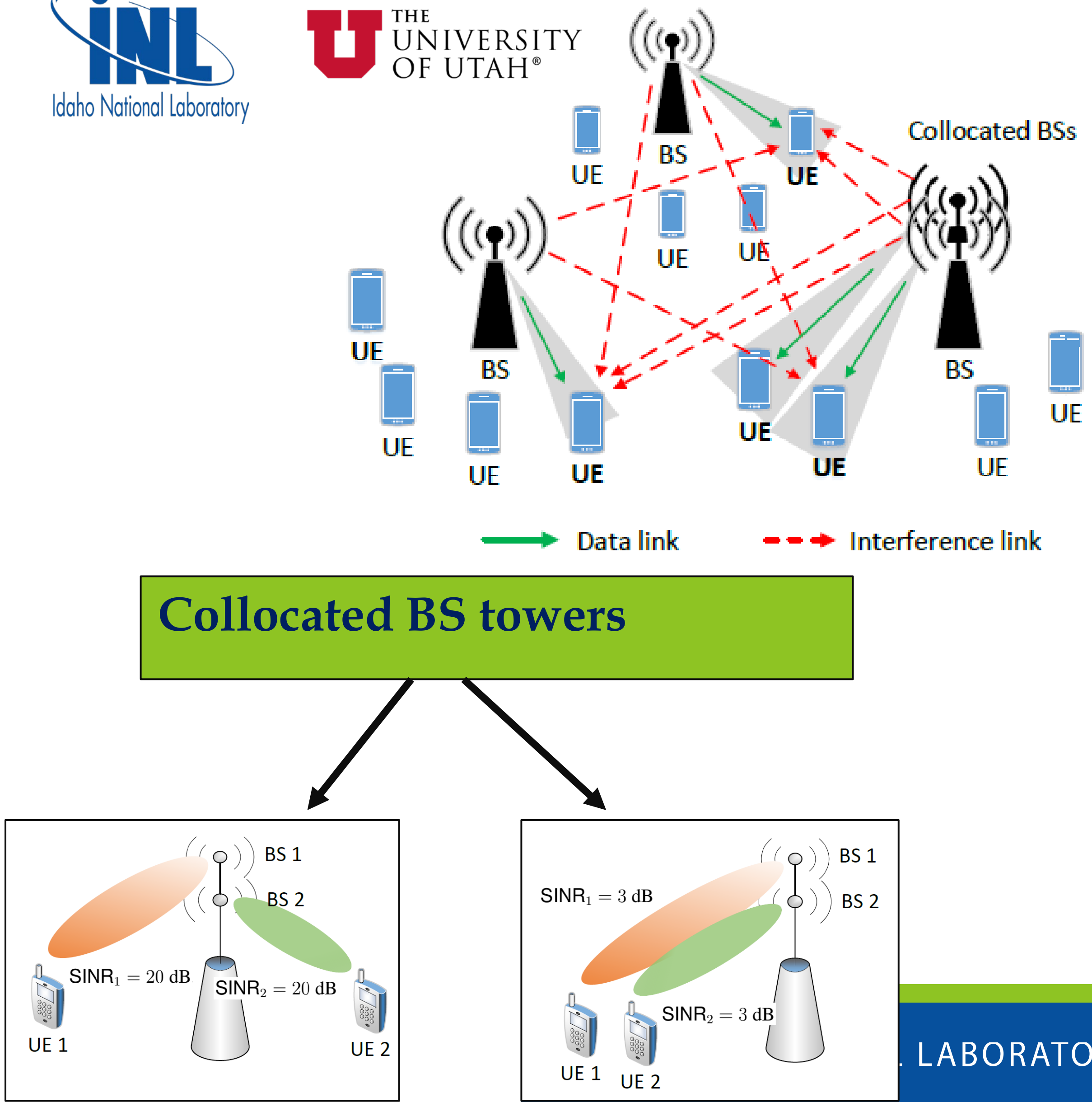
Use cases:

- ✓ Manufacturing - Industry 4.0
- ✓ Smart Warehouse – DoD 5G Use Case
- ✓ Other use cases: Hospitals, Airport, Smart Grid, Nuclear Plants, Mines …..



Secure mmWave Spectrum Sharing with Autonomous Beam Scheduling

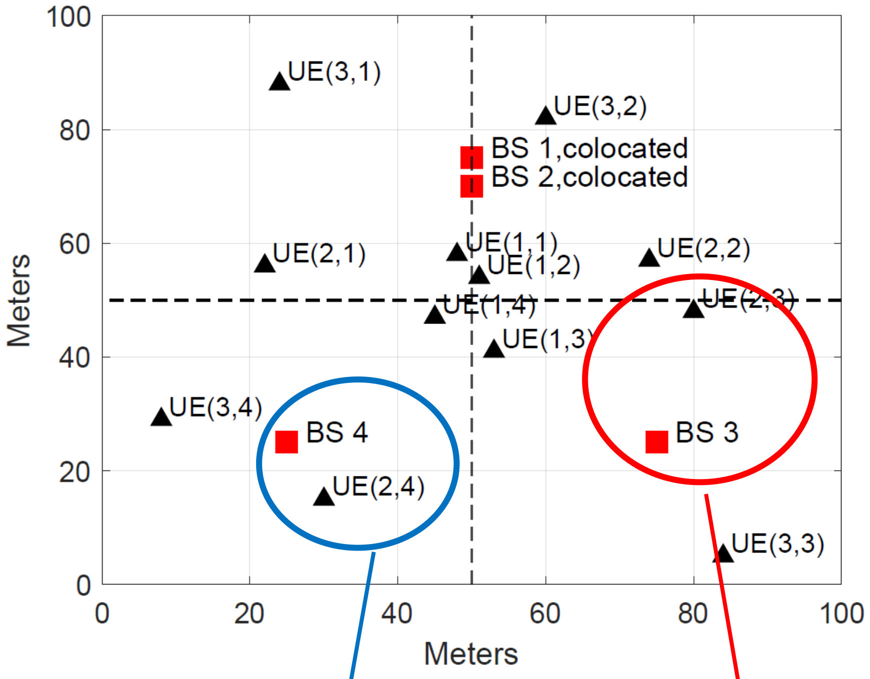
- ➢ INL LDRD collaboration with Univ of Utah
  - ✓ Professors Mingyue Ji, Sneha Kumar Kasera
  - ✓ Ph.D. Students: Xiang Zhang, Shamik Sarkar
- ➢ Secure mmWave Spectrum Sharing (SS) among multiple operators
- ➢ Base stations (BS) from multiple 5G networks utilize UE measurements to maximize total throughput independently
- ➢ Eliminates centralized mechanism such as the Spectrum Access Server (SAS)
- ➢ Does not rely on separate sensing network such as the Environmental Sensing Capability (ESC) for SAS



Collocated BS towers

Problem formulation

- ➢ Novel problem formulation based on the Lyapunov stochastic optimization framework
- ➢ Virtual queues to enforce average and peak power constraints
- ➢ Network utility decomposition into
  - ✓ Convex optimization to determine auxiliary variables
  - ✓ Non-convex stochastic optimization problem for optimal power allocation for beam scheduling
- ➢ Non-cooperative Game-based Distributed Beam Scheduling Framework for 5G Millimeter-Wave Cellular Networks, IEEE Transactions on Wireless Communications, vol. 21, no. 1, pp. 489-504, January 2022
- ➢ Use of non-cooperative game theory and Q-learning to solve the non-convex problem



UE (*i*, *j*): UE *i* associated with BS *j*

Cell-center UEs **Cell-edge UEs**

Payoff functions

BS payoff:

Power allocation

UE j_i is scheduled by BS i

$$R_i(\boldsymbol{p}) = \underline{\alpha_i} W \log\left(1 + \mathrm{SINR}_{j_i}\right) - \underline{\beta_i} p_i$$

α_i, β_i are weights,
trade-off: throughput VS. power consumption

Network payoff:

M: # of BSs

$$\bar{R} \triangleq \frac{1}{T} \sum_{t=1}^{T} \sum_{i=1}^{M} R_i(\boldsymbol{p}(t))$$

RF propagation model

✓ Antenna model

$$G(\theta) = \begin{cases} G^{\max}, & |\theta| \le \Theta/2 \\ G^{\min}, & |\theta| > \Theta/2 \end{cases}$$

Main to Side Lobe Ratio $\mathbf{MSR} \triangleq 10\,\lg\left(G^{\max}/G^{\min}\right)$

✓ Signal to Interference Noise Ratio at UE $_j$ served by BS $_i$

$$\mathbf{SINR}_{j,i_j} = \frac{p_{j,i_j} G^{\mathrm{UE}}_{j,i_j} G^{\mathrm{BS}}_{j,i_j} |h_{j,i_j}|^2 d^{-\eta}_{j,i_j}}{\sum_{\ell \in \mathcal{M}, \ell \neq i} p_{j_\ell,\ell} G^{\mathrm{UE}}_{j,\ell} G^{\mathrm{BS}}_{j,\ell} |h_{j,\ell}|^2 d^{-\eta}_{j,\ell} + \sigma^2}$$

✓ Small scale fading with Nakagami-m distribution

Q-learning

- Action-state value $Q(a_t, s_t)$

- *Epsilon-greedy* action selection:

$$a_t = \underset{a \in \boldsymbol{A}}{\operatorname{argmax}} Q(a, s_t), \qquad \text{with probability } 1-\varepsilon;$$

$$a_t = \text{randomly select}, \qquad \text{with probability } \varepsilon.$$

- Update rule:

$$Q(a_t, s_t) = (1 - l_r)Q(a_t, s_t) + l_r[r_{t+1} + \gamma \max_{a \in \boldsymbol{A}} Q(a, s_{t+1})]$$

- Q-learning converges under some mild conditions

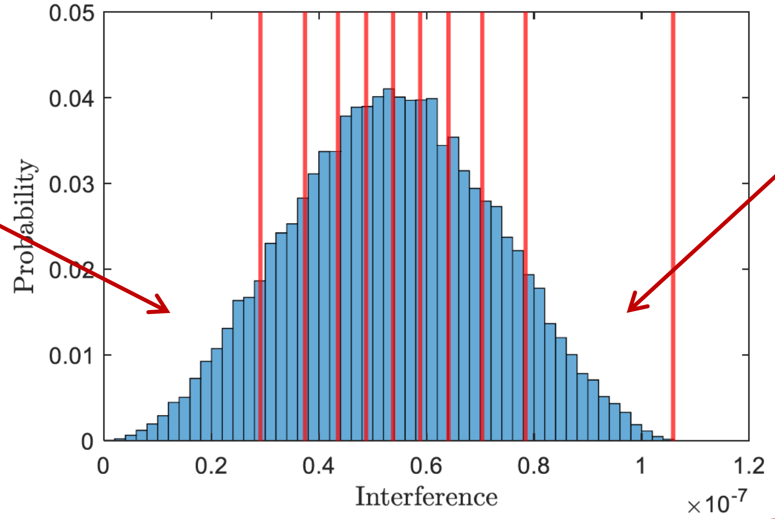
Action and State quantization

- Selectable power of transmission by an agent i.e., a base station is quantized

$$p_i^j = (j-1)\frac{p_i^{max}}{P_q - 1},\ j = 1,2,\dots,P_q$$

# of power levels

- State, or level of interference is also quantized (through training phase)



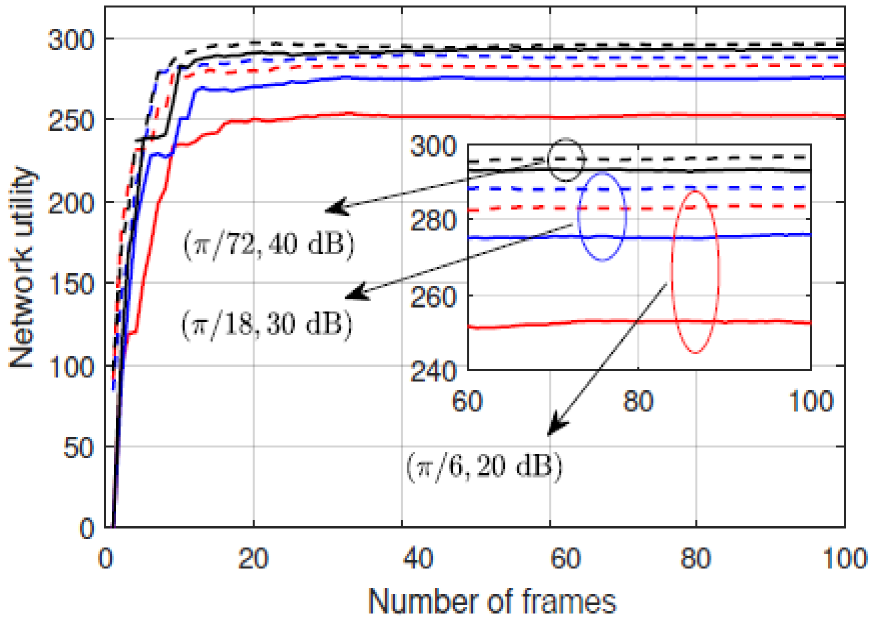
State 1

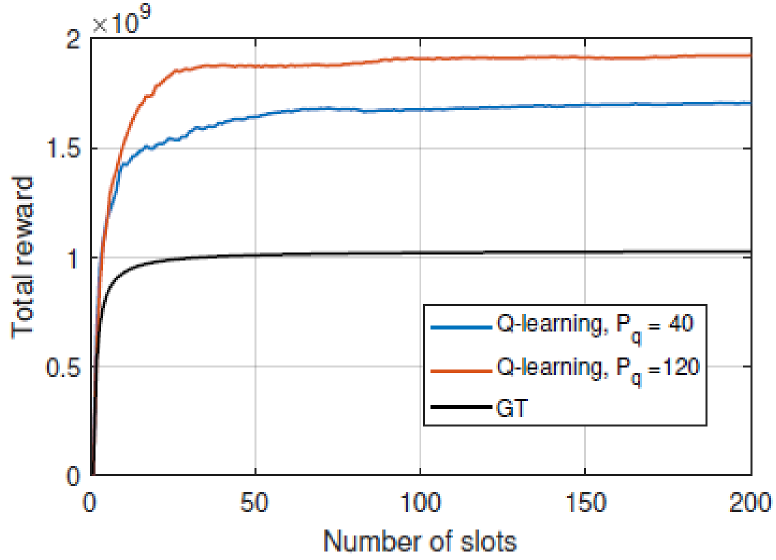
State 10

$I_q = 10$

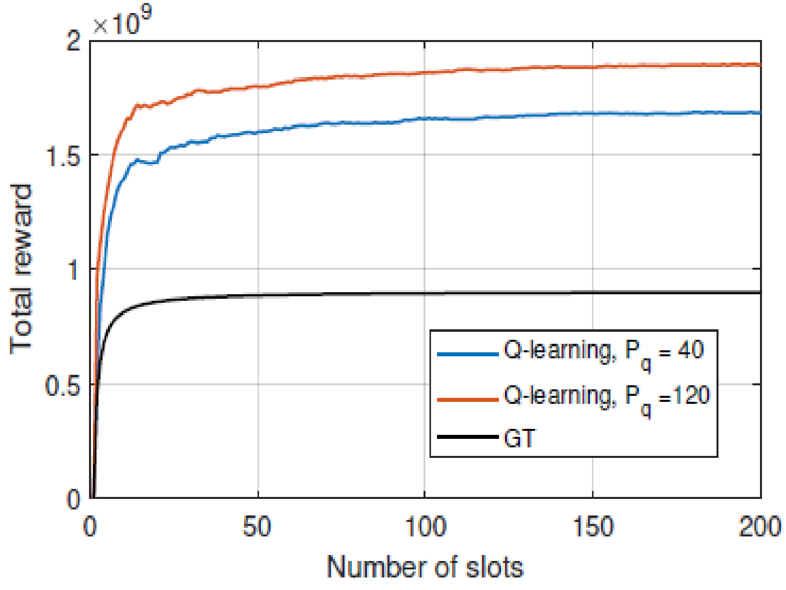
# of percentiles

Q-learning comparison with Game Theory





(a) $\beta = 0$.



(b) $\beta = 0.01BW$.

- ✓ Shared bandwidth W = 400 MHz at 37 GHz, $p^{max} = 39$ dBm

Publications on Spectrum Sharing

1) Advances in Secure mmWave Spectrum Sharing with Autonomous Beam Scheduling, 2022 IEEE Wireless and Microwave Conference. April 2022.

2) Non-cooperative Game-based Distributed Beam Scheduling Framework for 5G Millimeter-Wave Cellular Networks, IEEE Transactions on Wireless Communications, vol. 21, no. 1, pp. 489-504, January 2022.

3) Uncoordinated Spectrum Sharing in Millimeter Wave Networks Using Carrier Sensing, IEEE Transactions on Wireless Communications, vol. 21, no. 10, pp. 8368-8384, October 2022.

4) A Q-Learning-Based Approach for Distributed Beam Scheduling in mmWave Networks, IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), December 2021.

5) A Non-cooperative Game-based Approach to Distributed Beam Scheduling in Millimeter-Wave Networks, Asilomar Conference on Signals, Systems, and Computers, IEEE Signal Processing Society, Nov 2021.

6) A Stochastic Optimization Framework for Distributed Beam Scheduling in 5G mm-Wave Networks over non-cooperative Operators, Asilomar Conference on Signals, Systems, and Computers, IEEE Signal Processing Society, November 2020.

7) Enabling Uncoordinated Spectrum Sharing in Millimeter Wave Networks Using Carrier Sensing, Asilomar Conference on Signals, Systems, and Computers, IEEE Signal Processing Society, November 2020.

arupjyoti.bhuyan@inl.gov

630-803-9111 (cell)

Idaho National Laboratory