Institute for the Wireless Internet of Things at Northeastern University

Securing the Open RAN

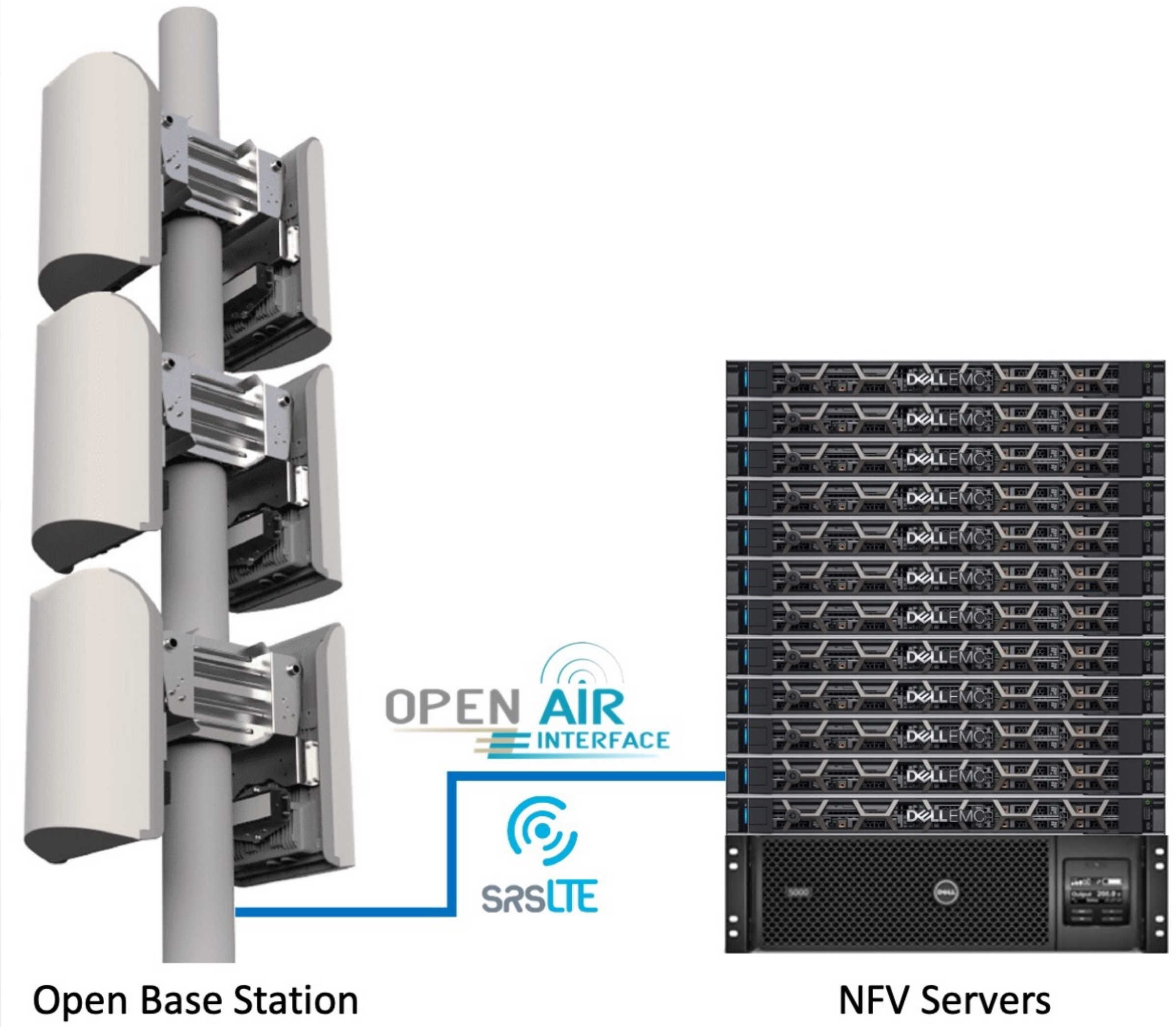
NSF Workshop on Next-G Security

Tommaso Melodia

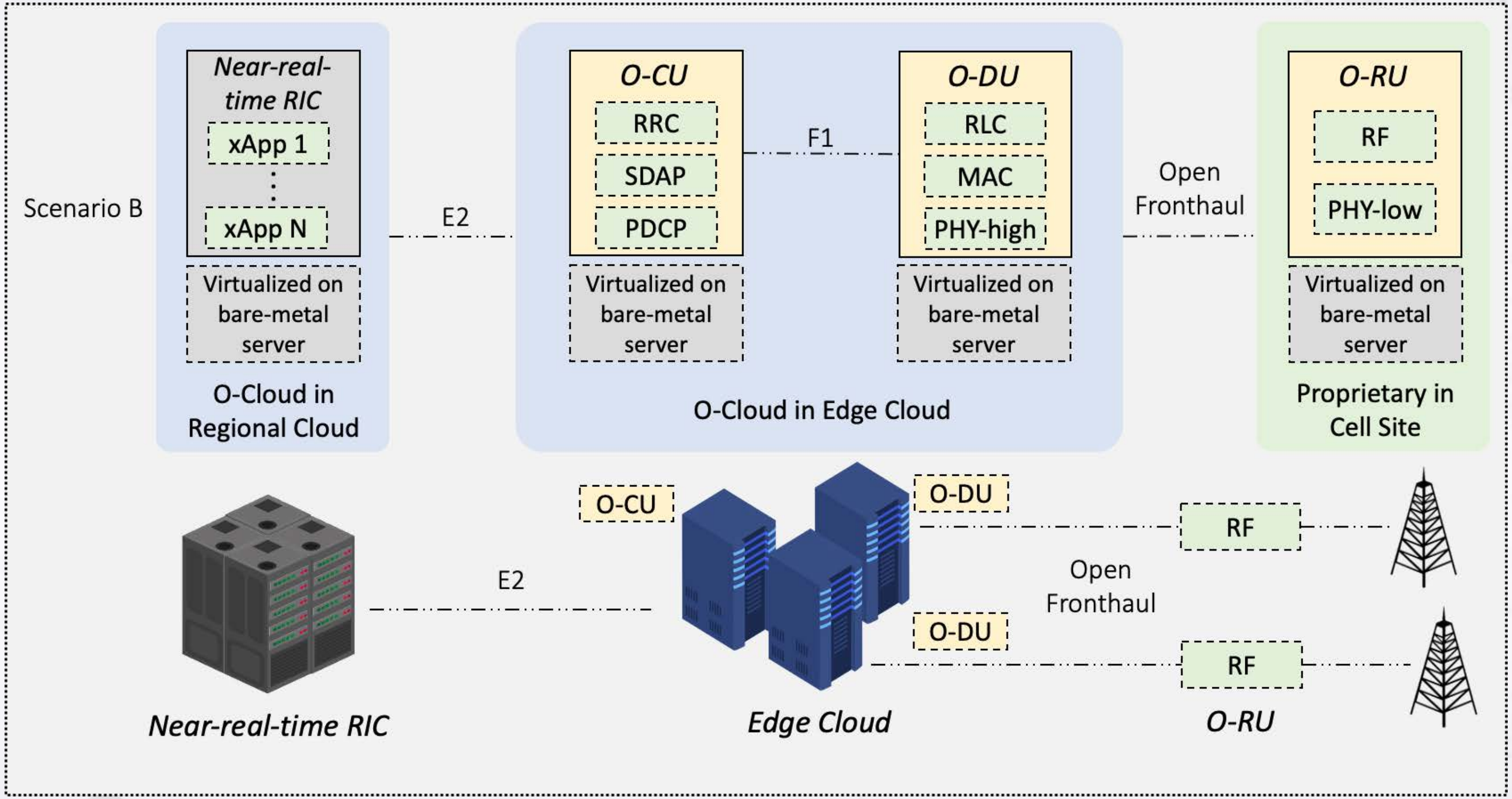
Vertical Disaggregation

Traditional approach

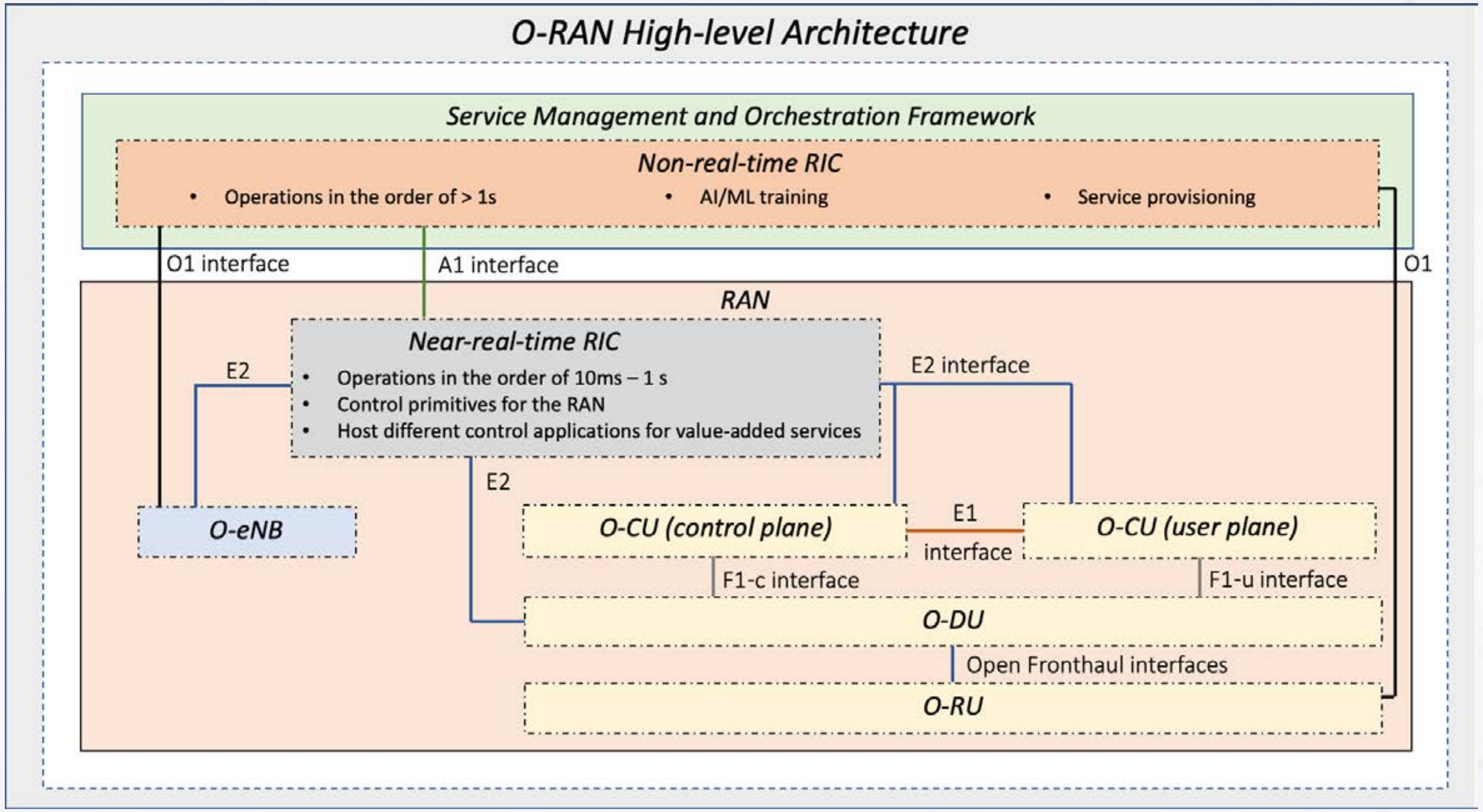
Virtualized RAN



Horizontal Disaggregation



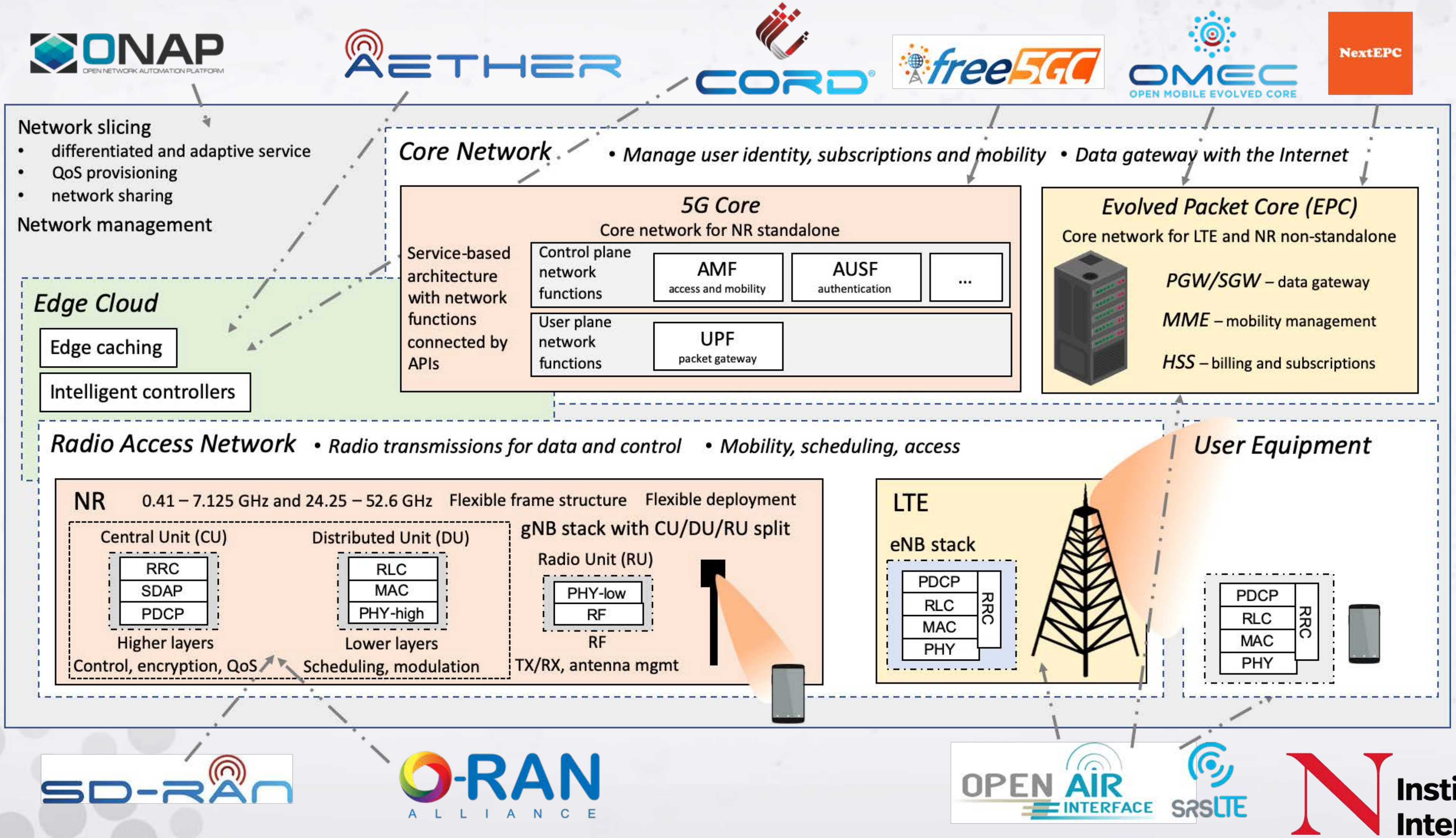
O-RAN – ''Horizontal Disaggregation'' and Abstraction



O-RAN ALLIANCE

Institute for the Wireless Internet of Things at Northeastern

End-to-End Programmable, Virtualized



Institute for the Wireless Internet of Things at Northeastern

L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "*Open, Programmable, and Virtualized 5G Networks: State-of-the-Art and the Road Ahead,*" **Computer Networks (COMNET)**, vol. 182, Dec 2020.

Implications of Open RAN and Virtualization

1. End-to-end Virtualization, Open RAN, and service-based architecture result in new security challenges

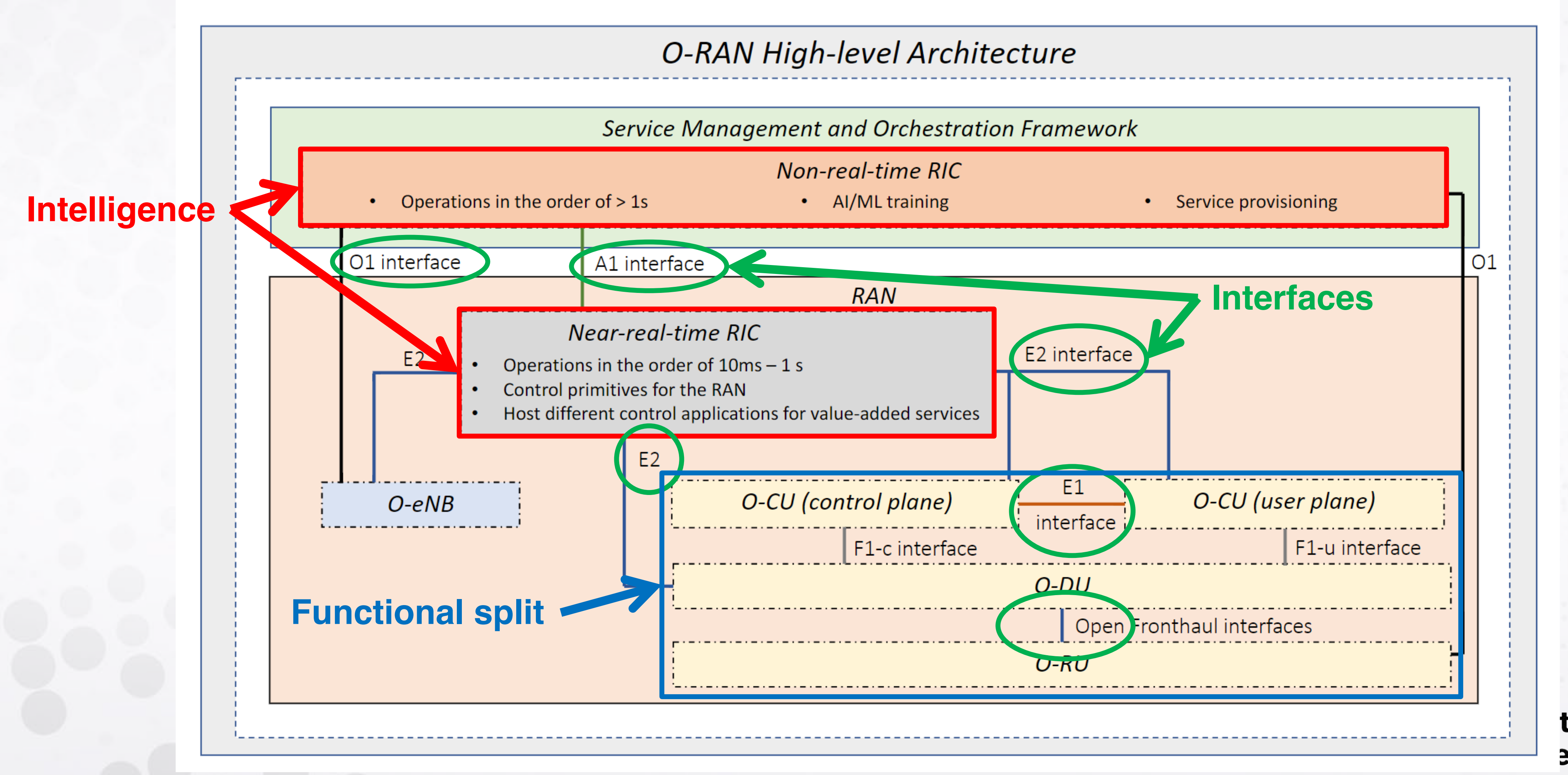
2. Softwarization and Open RAN open exciting opportunities for security research

3. Virtualization enables opportunities to test at scale

Institute for the Wireless Internet of Things at Northeastern

New security challenges

Expanded Threat Surface



Example: O-RAN Lower Layer Split (LLS) 7-2x

- O-RU can access O-DU through Open Fronthaul Interface
  - Manipulate parameters
  - Reconfigure the node
  - Management traffic to Northbound Interface – Man in the middle attack

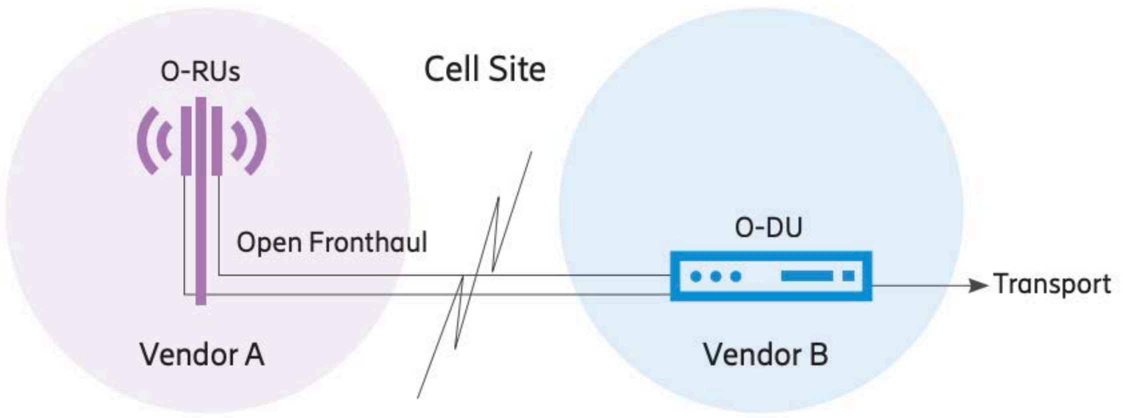


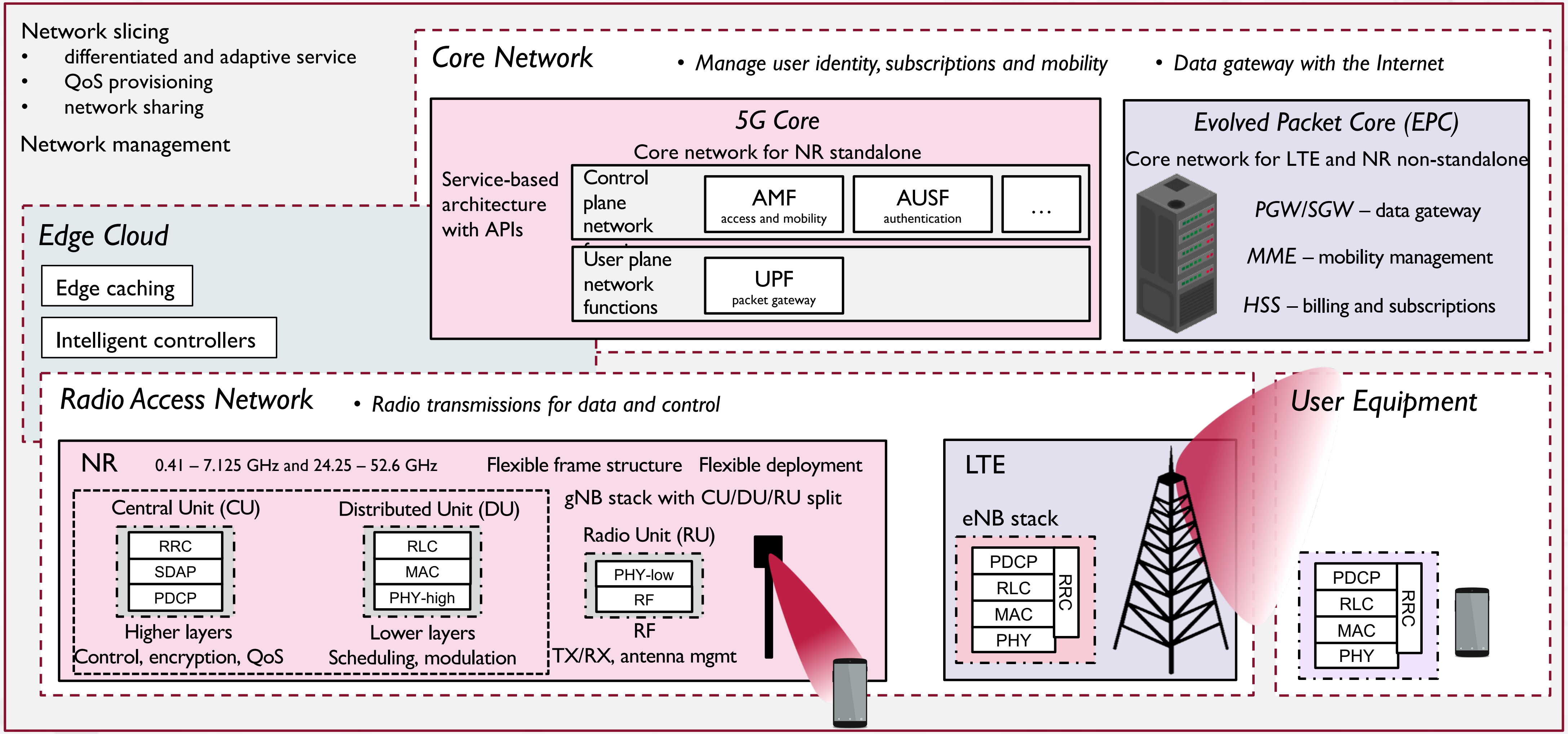
Figure 4: O-RAN Open Fronthaul

Ericsson, "Security Considerations on Open RAN"

Intelligence In the Open RAN

4. AI in the core: orchestration, slicing

3. AI at the edge: RAN optimization, caching, edge services



2. AI in the RAN: scheduling, mobility, access

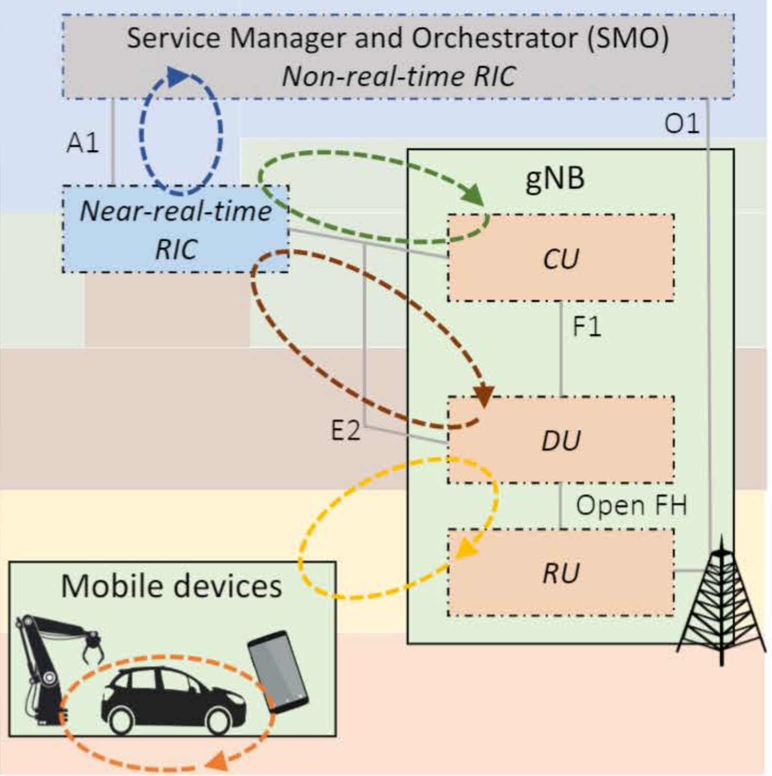
1. AI on mobile devices: real-time, waveform-based adaptation

L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "*Open, Programmable, and Virtualized 5G Networks: State-of-the-Art and the Road Ahead,*" **Computer Networks (COMNET)**, vol. 182, Dec 2020.

New Control Loops that need to be "secured"

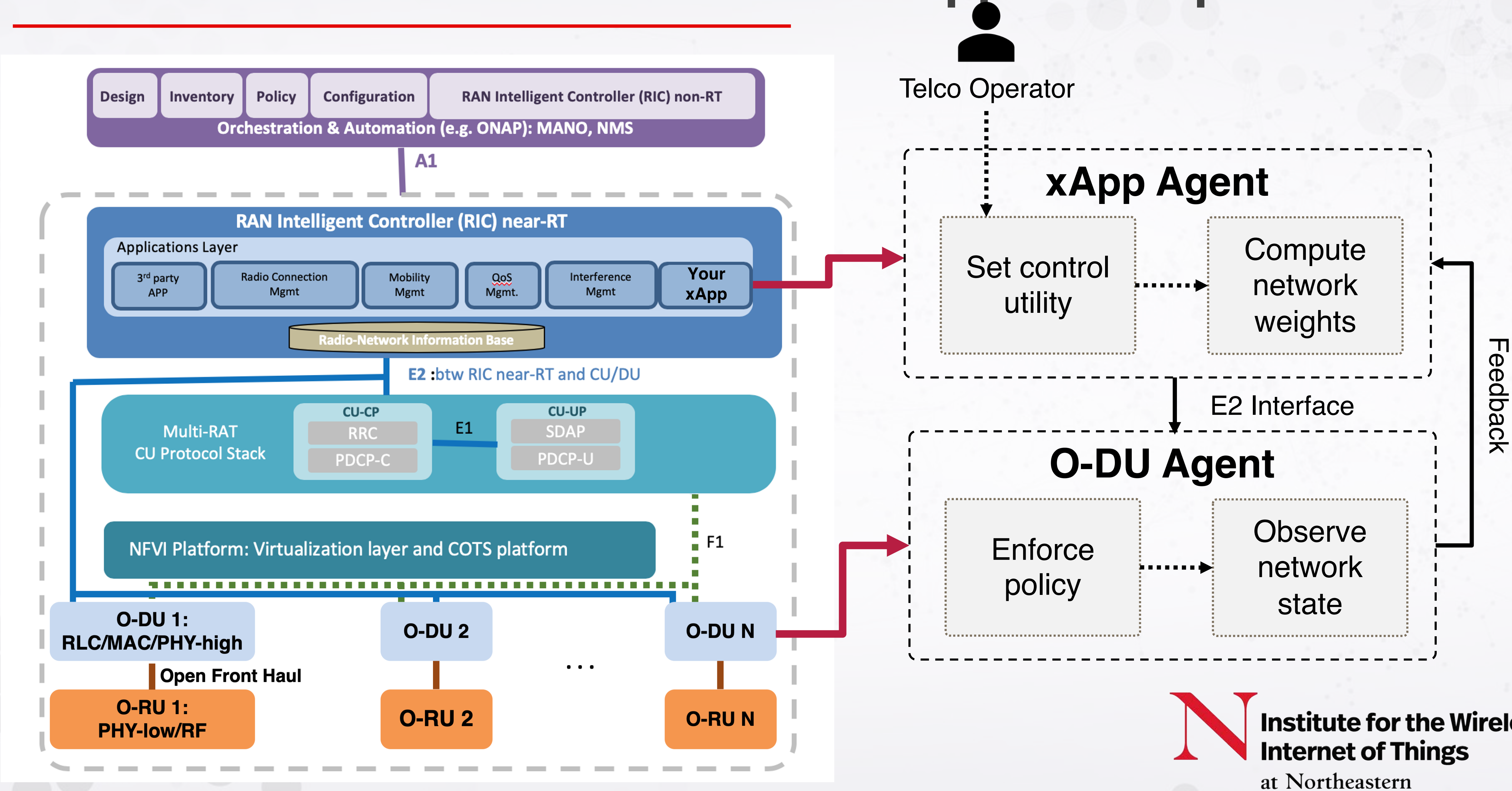
Control and learning objective	Scale	Input data	Timescale
Policies, models, slicing	> 1000 devices	Infrastructure-level KPIs	Non-real-time > 1 s
User Session Management e.g., load balancing, handover	> 100 devices	CU-level KPIs e.g., number of sessions, PDCP traffic	Near-real-time 10-1000 ms
Medium Access Management e.g., scheduling policy, RAN slicing	> 100 devices	MAC-level KPIs e.g., PRB utilization, buffering	Near-real-time 10-1000 ms
Radio Management e.g., resource scheduling, beamforming	~10 devices	MAC/PHY-level KPIs e.g., PRB utilization, channel estimation	TTI < 10 ms
Device DL/UL Management e.g., modulation, interference, blockage detection	1 device	I/Q samples	< 1 ms

Architecture



Institute for the Wireless Internet of Things
at Northeastern

New Tenants in the Network – the xApp developer



Institute for the Wireless Internet of Things at Northeastern

Implications of RIC and Intelligence

- New threats
  - Third-party Near-RT RIC apps: potential carrier for attacks
  - Near-RT RIC signaling conflicts with gNodeB control plane
  - Multiple RIC xApps: conflicting signals, inconsistent/incorrect behavior
  - Denial of Service Attacks through xApps
  - Privacy Concerns: UE identification in the RIC
  - xApps can be configured through A1 interface to track users
  - Adversaries can inject data to get xApps to learn incorrect behaviors
- Research Opportunites
  - Forecasting threats
  - Closed-loop detection and mitigation of cross-layer attacks
  - Software-defined Reconfiguration
  - Joint optimization of RAN resources and of VNF to counter attacks
  - Adversarial Learning

Testing at Scale

PAWR PLATFORMS WERE CHOSEN TO BE GEOGRAPHICALLY DIVERSE AND RESEARCH FOCUS INDEPENDENT

POWDER

Salt Lake City, UT

Software defined networks and massive MIMO

COSMOS

West Harlem, NY

Millimeter wave and backhaul research

AERPAW

Raleigh, NC

Unmanned aerial vehicles and mobility

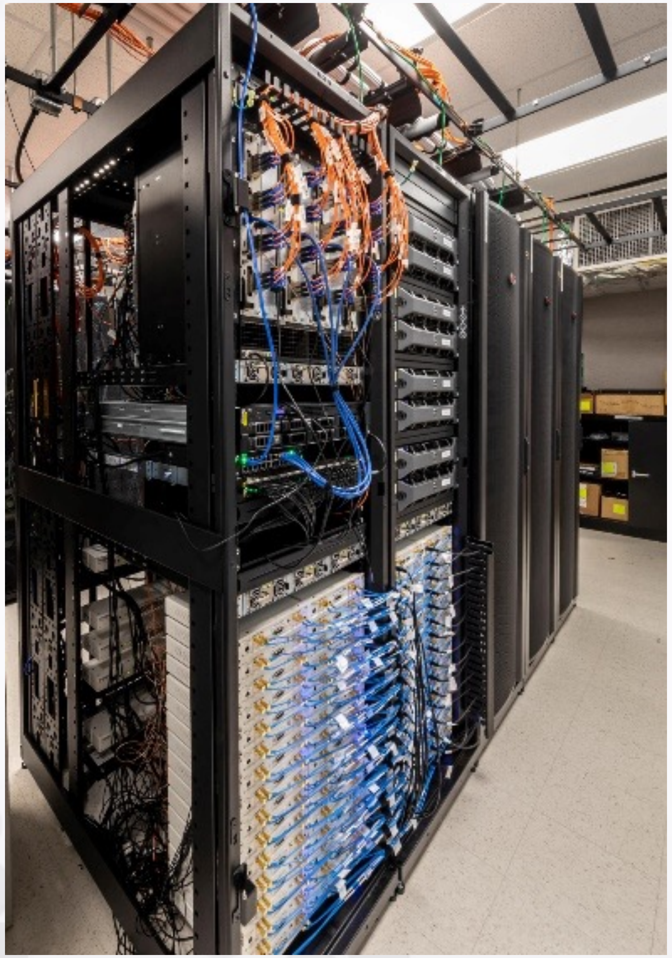
Rural Broadband Platform

TBD

Coming late 2020

Colosseum – *World's largest RF emulator, located at Northeastern University in Boston*

COLOSSEUM: The World's Largest Network Emulator



- 256 USRP X310s → 128 as user devices, 128 as part of Colosseum Massive Channel Emulator (MCHEM)
- 65,536 100 MHz emulated RF channels
- 21 racks of radios, 171 high-performance servers w/ CPUs / GPUs
- Full-mesh networking capability
- Massive Computing and support resources: (CPU, GPU, FPGA)
  - 900 TB of Network Attached Storage (NAS)
  - 320 FPGAs
  - 18 10G switches
  - 25 clock distribution systems
  - 52 TB/s of digital RF data