Security and AI-Enabled Cellular RAN

T. Charles Clancy, PhD
Senior VP & General Manager, MITRE Labs

NSF NextG Workshop, October 2020

Approved for Public Release
Distribution Unlimited
Case Number **20-02772-4**

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

AI/ML in 5G+

Radio Access Network

Non-Real Time
- Edge-scale resource management
- >100 ms

Near-Real Time
- Tower-level resource management
- 10-100 ms

O-RAN RIC

Core Network

Scalable Orchestration
- Automate the complexity of network orchestration

Intelligent Application Edge
- Enable real-time intelligence for 5G use cases, e.g. MMTC and URLLC

Real Time
- Frame-level resource management
- <1 ms

Emerging 6G Concepts

Mandate Driven Architectures
- Packet-level QoS specifications with network optimized per-flow to support

O-RAN Reference Architecture

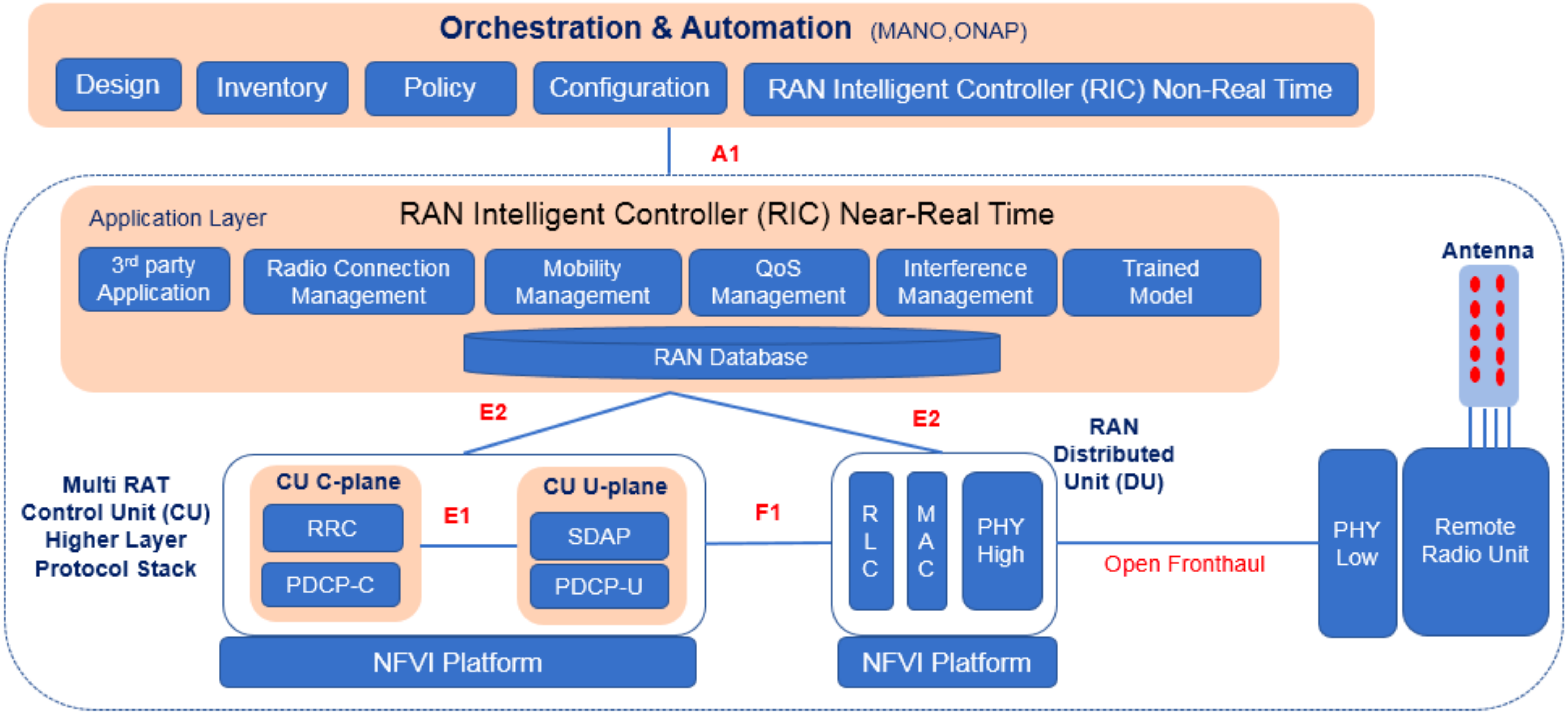
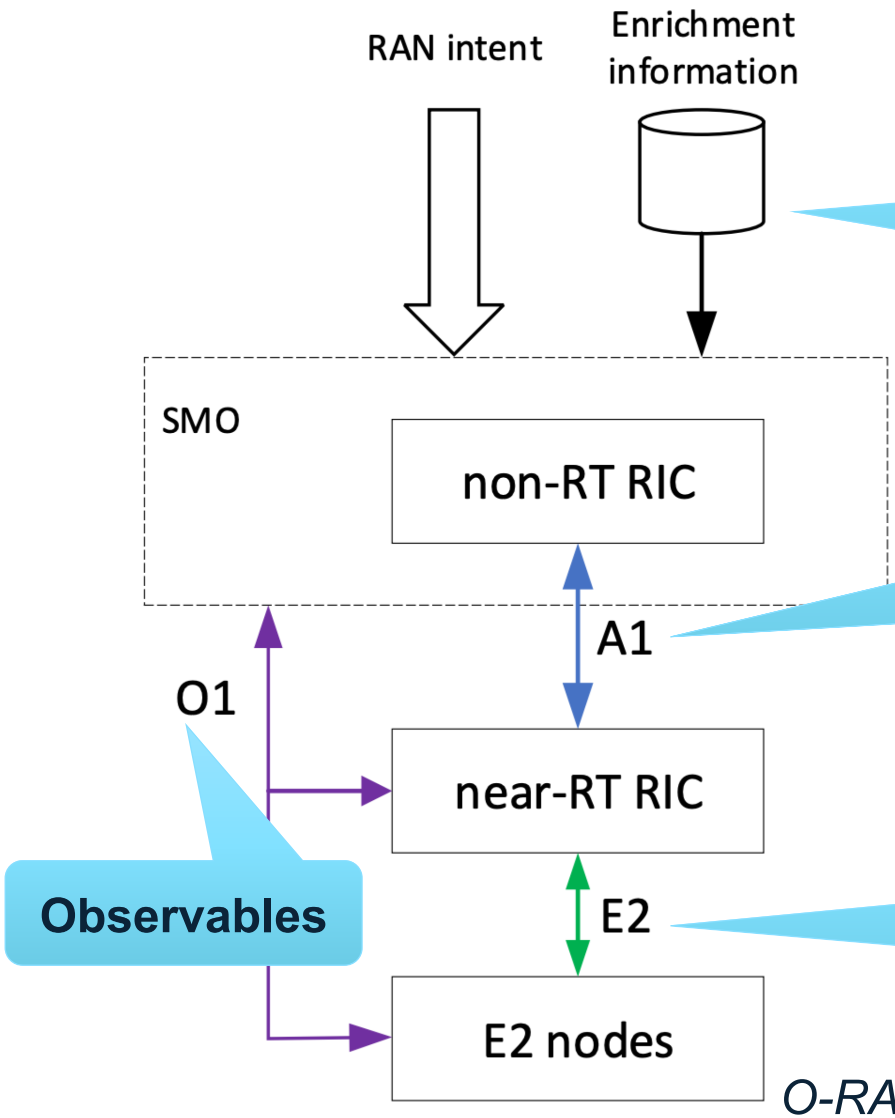


Image Credit: http://www.techplayon.com/open-ran-o-ran-reference-architecture/

MITRE

O-RAN Interfaces & Policies



Intent Policies

High-level declarative policies (e.g. SLA)

Declarative Policies

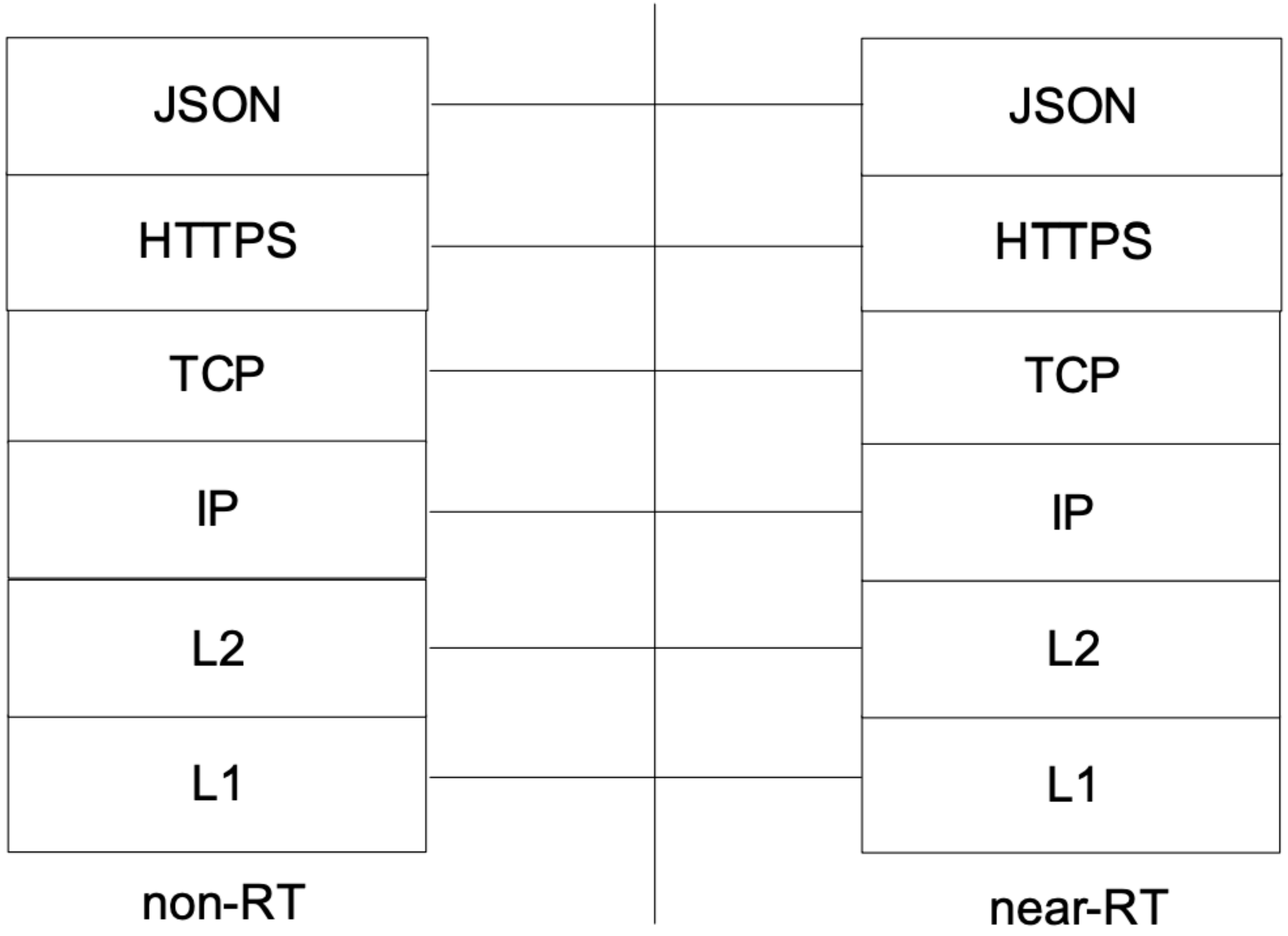
Express resources (traffic, efficiency) and objectives (QoS, QoE, KPI, KQI) for those resources, but not how to achieve them

Imperative Policies

Governs the specific state of resources based on events, conditions, and actions

O-RAN Alliance, “A1 interface: General Aspects and Principles”, September 2019

O-RAN Interfaces & Policies (2)



Policy create procedure;
Policy query procedure;
Policy update procedure;
Policy delete procedure;
Policy feedback procedure;

O-RAN Alliance, "A1 interface: General Aspects and Principles", September 2019

O-RAN RIC Use Cases

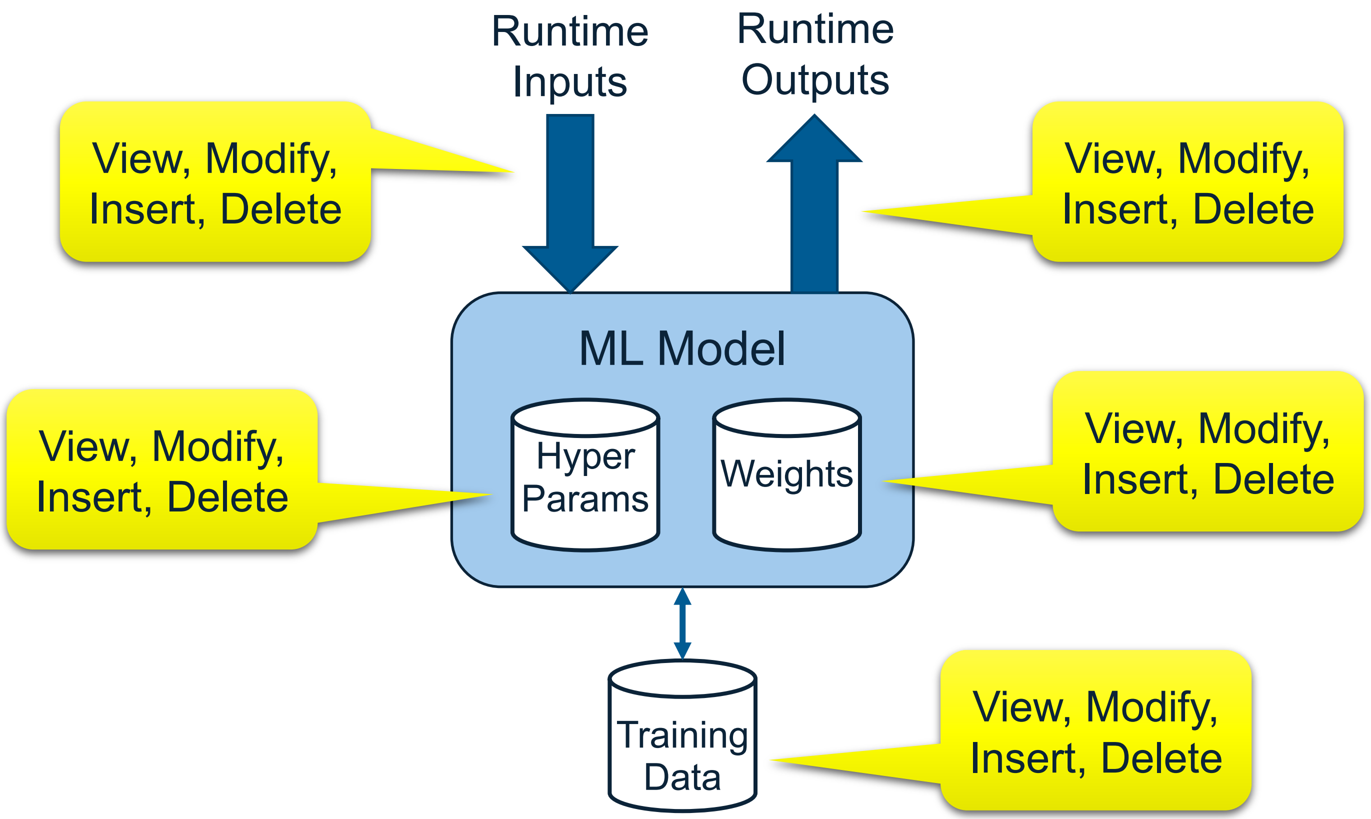
- Phase 1
  - Traffic Steering
  - QoE/QoS Optimization
  - Massive MIMO Optimization
- Phase 2
  - RAN Slice SLA Assurance
  - V2X Handover
  - UAV Resource Management

Explicit support for Machine Learning (ML) based approaches to automation, training off the observables (O1)

O-RAN Alliance, "O-RAN Use Cases and Deployment Scenarios", February 2020

Generic ML Threat Models

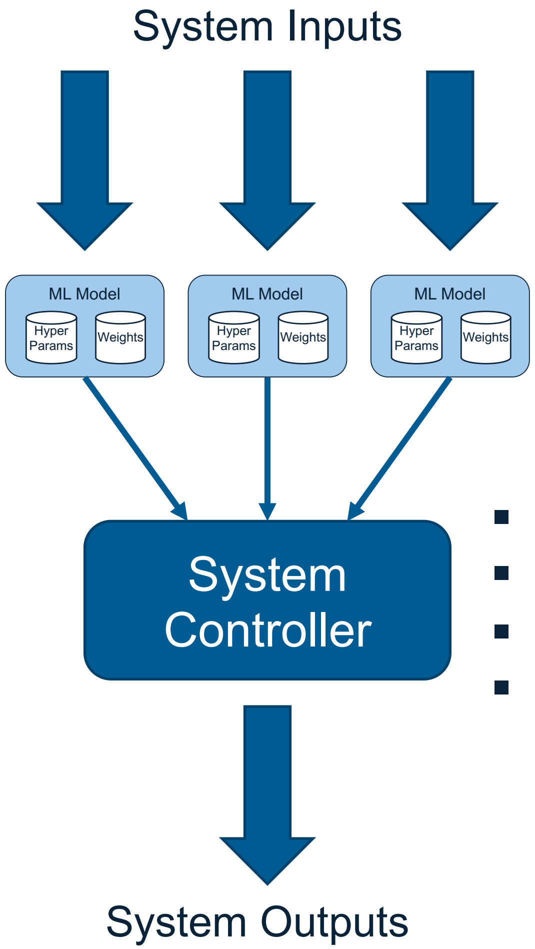
Potential Adversary Capabilities



Classes of adversary objectives

- Compromise Confidentiality:
  - RE model
  - RE training data
  - Estimate/anticipate inputs/outputs
- Compromise Integrity:
  - Produce incorrect outputs
  - Produce deterministic outputs
- Compromise Availability:
  - Degrade model performance
  - ML DoS?

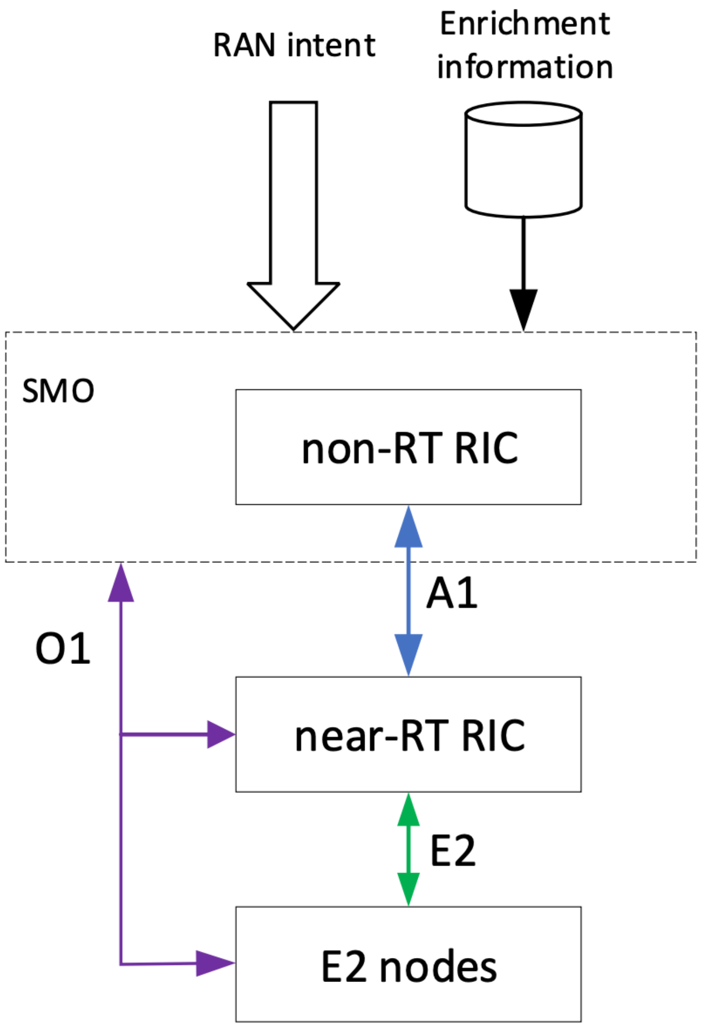
Generic AI System Threat Model



- Controller
- Policy
- RL
- FSM

- Same issues exist zooming out to larger AI systems
- View, modify, insert, delete – inputs, outputs, models, controller, etc
- Compromise Confidentiality:
  - RE system controller
  - Estimate/anticipate inputs/outputs
- Compromise Integrity:
  - Produce incorrect outputs
  - Produce deterministic outputs
- Compromise Availability:
  - Degrade system performance
  - Cause system failure

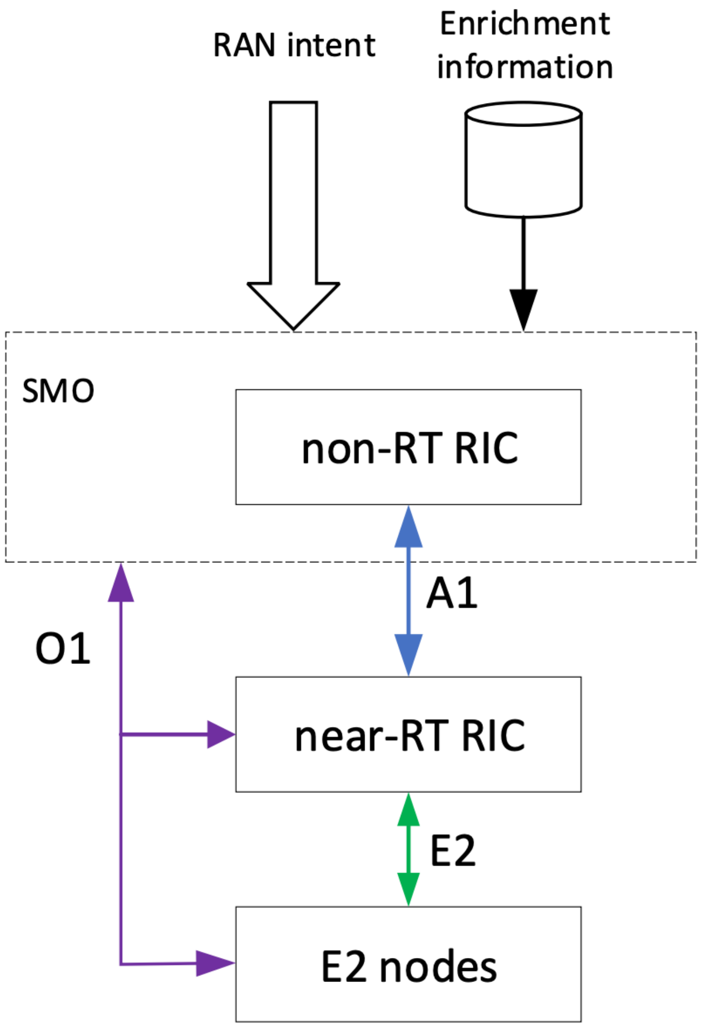
Attacker Objectives for RIC



- Compromise Confidentiality
  - Identify metadata about network users, to include sensitive classes like IIoT or public safety
- Compromise Integrity
  - Skew resource allocations in a greedy way or to potentially exploit billing
- Compromise Availability
  - Skew resource allocations to cause disruption to safety-critical services like IIoT, or mission-critical comms like public safety

MITRE

Attack Surface for RIC



- Key assumption: assume that all interfaces (e.g. A1, E2, O1) are sufficiently protected to prevent protocol exploitation
  - Leverage existing 3GPP security models for IPsec or TLS
  - Address PKI and key management issues
- Observables (O1)
  - Influence observables by creating artificial traffic demands in the network to influence model inputs
- Third Party Applications
  - The RIC envisions 3rd party "apps" – whole range of opportunities for exploitation
- System Inputs/Database
  - RAN intent
  - Enrichment information
  - AI/ML components used throughout the system

Hypothetical Example

- Metro-scale edge cloud environment
- ~100 different radio edge clouds operating within the edge cloud, each covering ~100 cell sites
- Multiple network slices operating over the 5G core: EMB + URLCC (CAV) + URLCC (UAS)
- Each network slice has own apps/models for controlling resource allocation

Hypothetical Example continued…

- UAS slice has unique challenges airborne LOS for low frequency reuse factors
- RIC anticipates path-aware resource allocation to combat this
- Spoofing UAS locations/paths to overlap can cause interference carve-out significantly depleting the eigen-capacity of MU-MIMO cells
- These hard constraints prevent other network slices (EMB, CAV) from operating effectively

Recommendations for O-RAN

- Basics
  - Import robust authentication and encryption for O-RAN interfaces from the current 3GPP standards
  - Address key management issues – O-RAN seeks to promote vendor diversity, so an approach inclusive of many vendors is required (CA?)
  - Code signing for third party apps, with some sort of testing regime
- AI Systems
  - Sophisticated AI-based controllers need fallback to policy-based controllers – less efficiency but greater predictability
  - Need for guardrails that can trigger human intervention

Broader Ecosystems

- RF Machine Learning
  - Growing set of literature on security concerns around RFML
  - Need to carefully assess these, particularly as they find their way into 6G
- AI for Scalable Orchestration
  - Current lack of systematic security features in Management and Network Orchestration (MANO) tools – e.g. ONAP, SDN controllers, etc
  - Need to firm up basic security principles before we can start to address AI
- Intelligent Application Edge
  - Many emerging edge computing frameworks – mix of IaaS/PaaS/SaaS
  - Some PaaS/SaaS AI frameworks, and no real security discussion yet

MITRE

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™