Commonwealth Cyber Initiative

AI Architectures for Next Generation Networks: Focus on ORAN

Luiz DaSilva

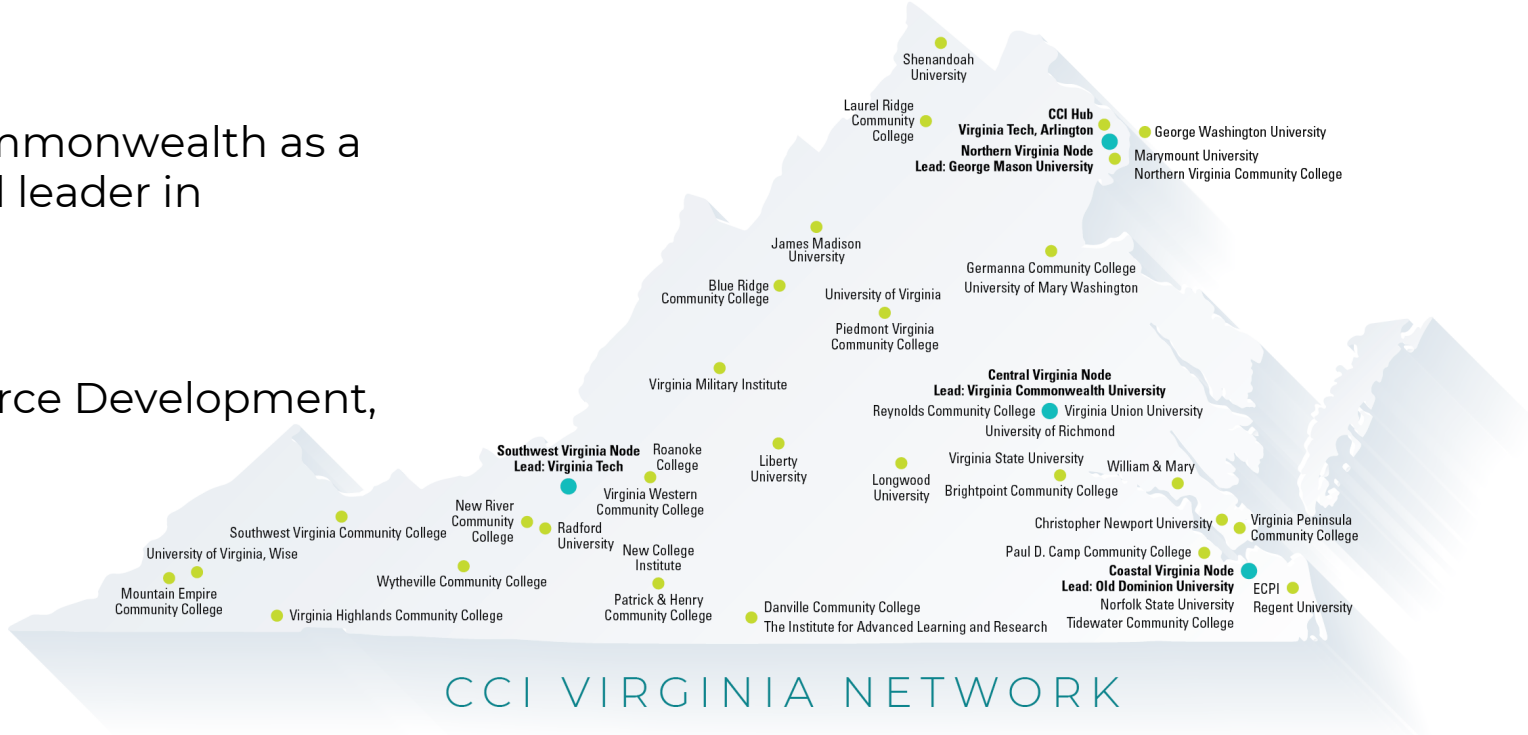
Executive Director, Commonwealth Cyber Initiative

Bradley Professor of Cybersecurity, Virginia Tech

The Commonwealth Cyber Initiative

Vision:
Positioning the commonwealth as a globally recognized leader in cybersecurity

Mission Lines:
Innovation, Workforce Development, and Research



45 Higher Education Institutions
300+ Faculty members

Focus Areas in Research

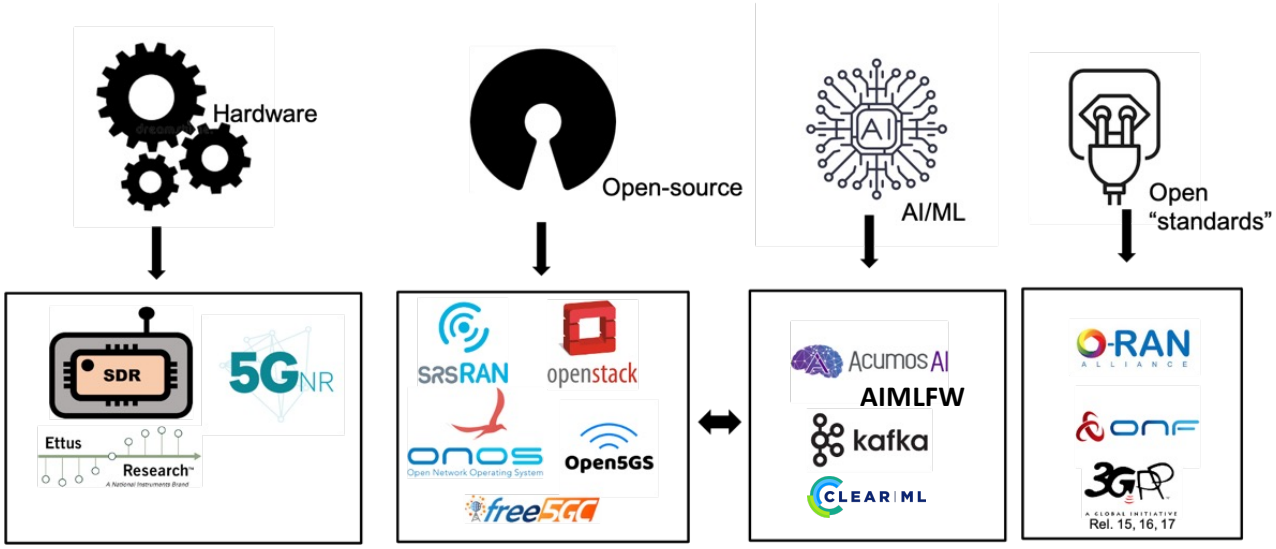
6G

- AI-native
- Secure by design
- Disaggregation, virtualization
- Managing complexity

AI

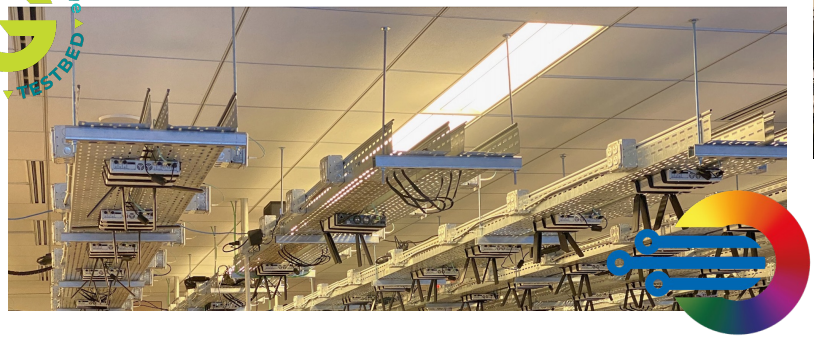
- AI for cybersecurity
- Cybersecurity for AI

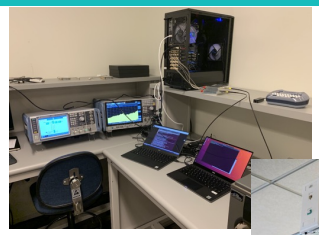
Building an Open xG Testbed



Open Network Testbed

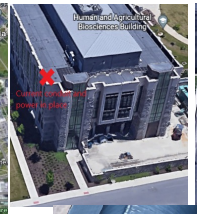
OTIC: Indoor Testbed





OPEN TESTING AND INTEGRATION CENTRE

Outdoor Testbed



O-RAN ALLIANCE

Member since 2021

SRS SOFTWARE RADIO SYSTEMS

CCI-SRS Lab announced in 2023

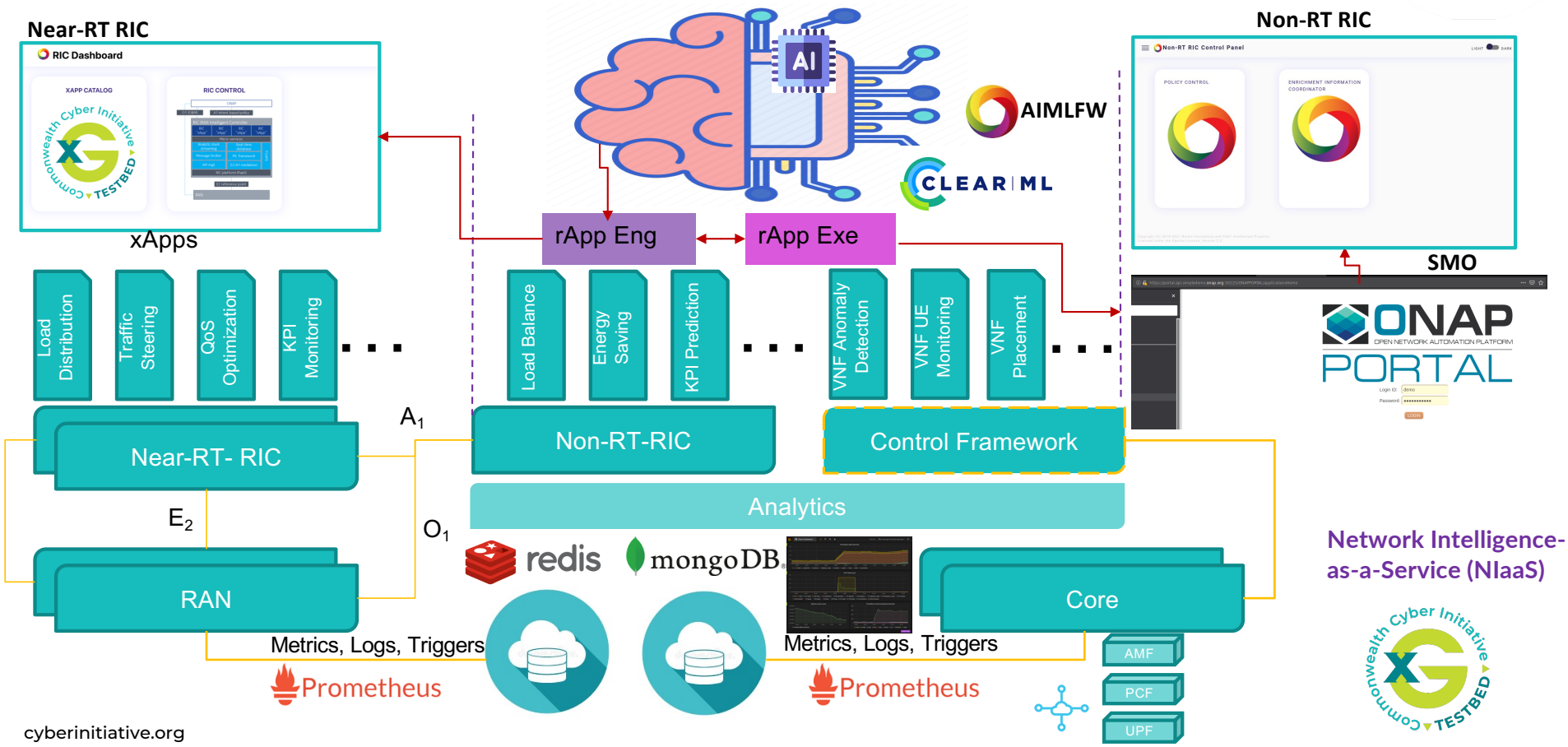
NEXT G ALLIANCE

Member since 2021

national spectrum consortium®

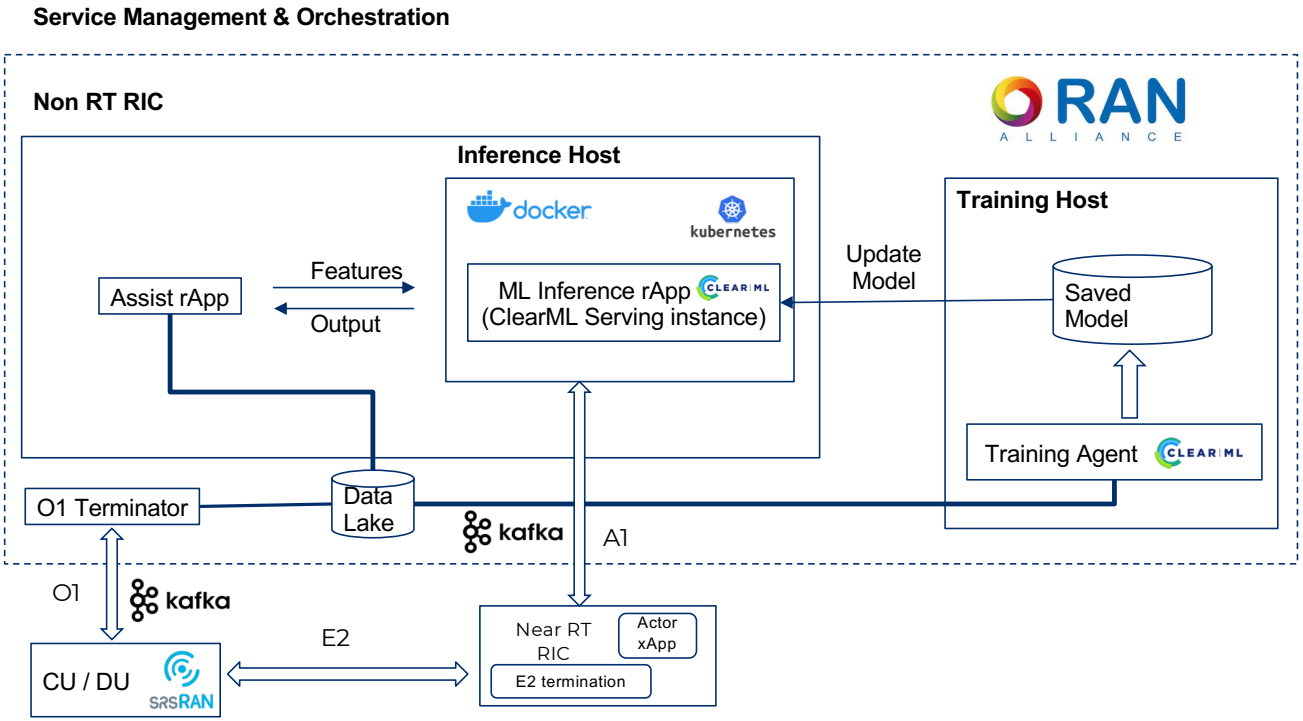
Member, with a seat in the NSC O-RAN advisory board

Control Loop Software Design

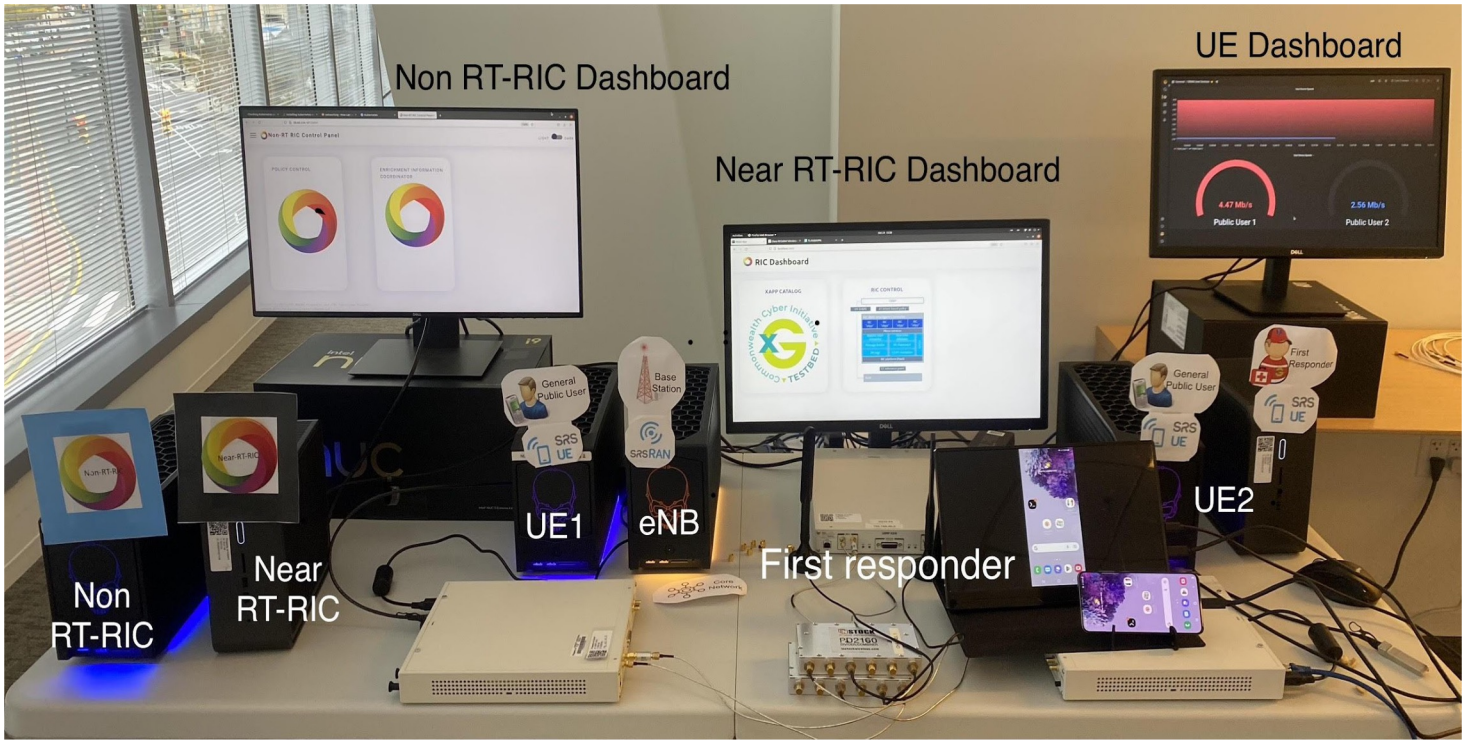


Network Intelligence-as-a-Service (NIaaS)

AI/ML Framework Integration - Current



AI/ML- Driven E2E Control Loop for O-RAN



Ref: Jaswanth S. R. Mallu, Joao F. Santos, Aloizio P. da Silva, Prateek Sethi, Vikas Radhakrishnan, Luiz DaSilva, "*AI/ML Data-driven Control Loop for Managing O-RAN SDR-based RANs*," IEEE INFOCOM Demo, New York, USA, 17 – 20 May 2023.

Disaggregated ORAN Controller

Research problem:
Optimizing deployment of near-RT RIC on a distributed cloud infrastructure comprising multiple sites with different resource capabilities and costs

Adapting the near-RT RIC deployment to minimize cost while meeting latency requirements to the controlled nodes

Results:
In a cloud-native environment, disaggregated near-RT RIC results in cost savings around 60% as compared to a monolithic approach

Ref: G. Bruno, G. Almeida, A. Sathish, A. da Silva, L. DaSilva, A. Huff, K. Cardoso and C. Both, "*Evaluating the deployment of a disaggregated Open RAN controller on a distributed cloud infrastructure*," IEEE Transactions on Network and Service Management, 2024

NTIA Wireless Innovation Fund

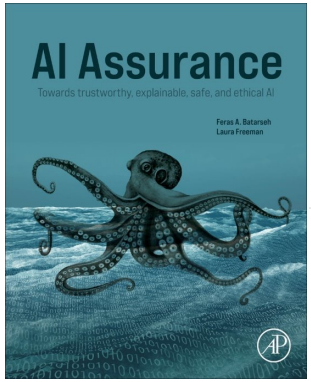
Funding Amount	Project Title and Description
$42M AT&T	Acceleration of Compatibility and Commercialization for Open RAN Deployments (ACCoRD)
$2M Booz | Allen | Hamilton®	Enhancing O-RAN Systems Against Sophisticated Attacks
$2M VIRGINIA TECH	Learning-Based ORAN Testing
$2M MICHIGAN STATE UNIVERSITY	AI Enabled Efficient Testing and Evaluation for RU, DU, and CU Components of 5G RAN
$2M VIRGINIA TECH	A Holistic Cybersecurity Framework for 5G RAN
$2M Cirrus360	Digital Twin to Predict System Failures

U.S. Commerce Secretary Gina Raimondo at T&E award announcement at CCI Hub (2024)

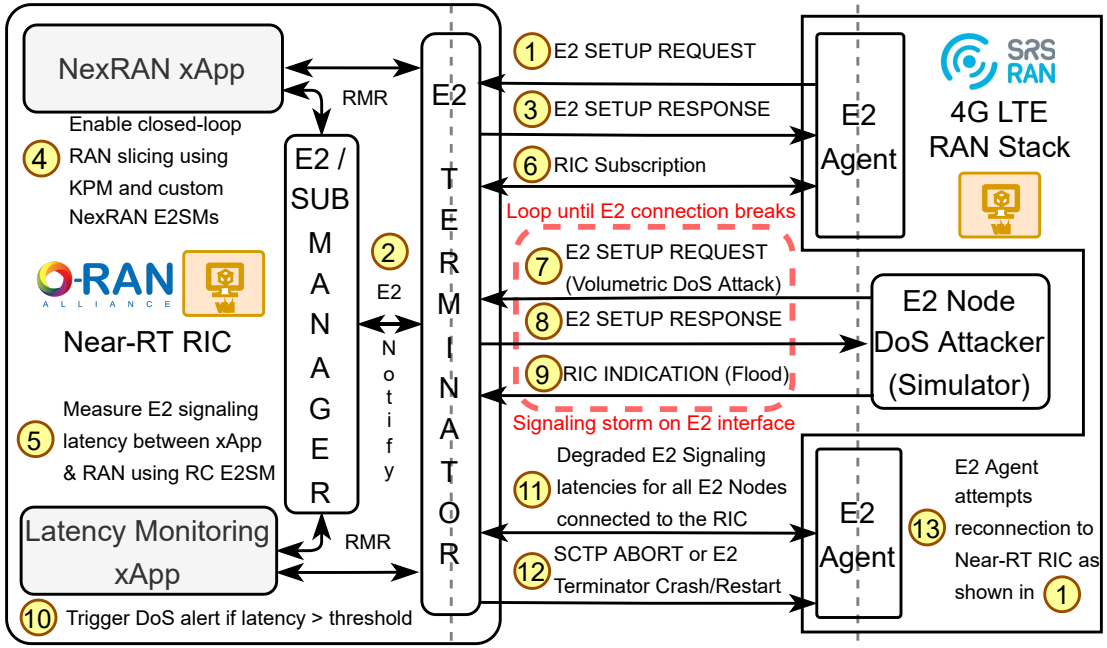
VIRGINIA TECH GEORGE MASON UNIVERSITY

Focus: AI for Cybersecurity & Cybersecurity for AI

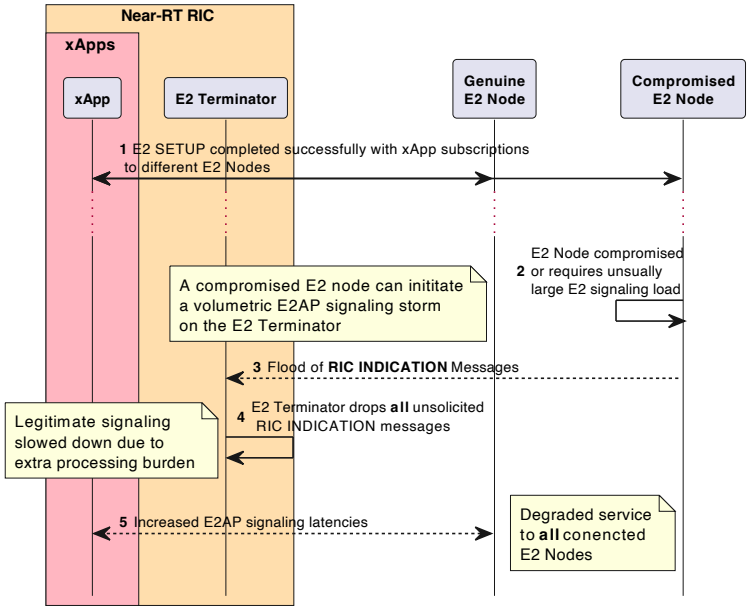
- Minimum perturbation
- Data poisoning attacks
- Incompleteness
- Data Imbalance
- DoS
- Ransomware
- And more…



Orchestrating E2 DoS Attack



Proof-of-concept DoS attack workflow on the experimental setup



Sequence workflow for a
Signaling Storm DoS attack

Work Presented and Results Discussed in O-RAN WG11 plenary

Commonwealth
Cyber Initiative