Security of Open Radio Access Networks

Hanna Bogucka

08.05.2023

All things wireless

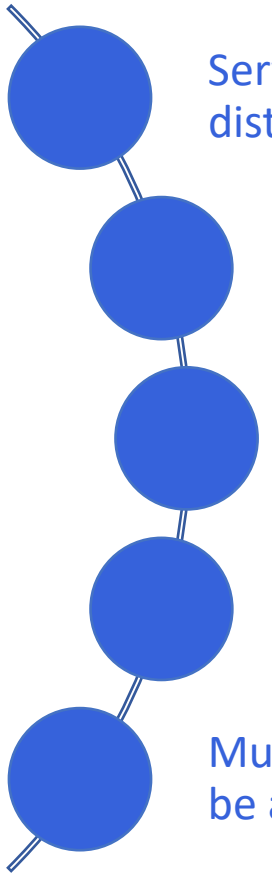
Content

- Open RAN
- Overview of security issues in RAN
- ORAN security risks and opportunities
- ORAN security activities
- Example xApps and rApps for security

RIMEDO LABS

rimedolabs.com

Security challenges of future network architecture



Service-Based Architecture (SBA) independence from infrastructure; decomposed, virtualized and distributed network functions.

Communication based on the Application Programming Interface (API); Poorly encrypted or insecure APIs can put network resources at risk of attack.

Private, corporate, industrial and IoT networks and applications. Companies with critical IT infrastructure have to take responsibility on internal and external security.

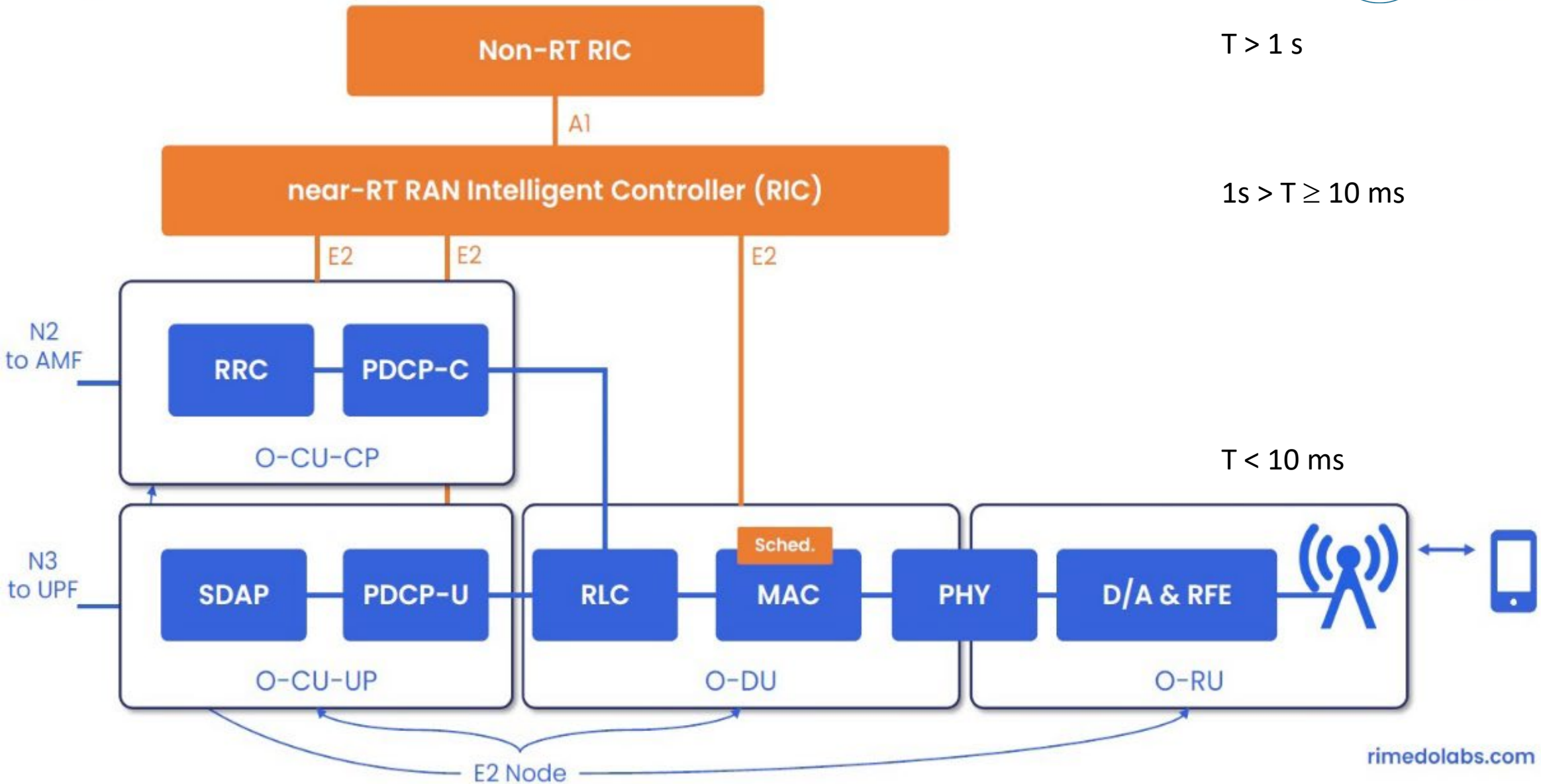
RAN and Open-RAN. Radio segment is inherently exposed to attacks related to the universal availability of the transmission medium (jamming, unauthorized access, eavesdropping, etc.).

Multi-Access Edge Computing (MEC). In a decentralized approach, significant parts of the network can be attacked at any time from anywhere.

TIMEDO LABS

The last two strictly address RAN and O-RAN including its ***openness and intelligence***.

Open-RAN

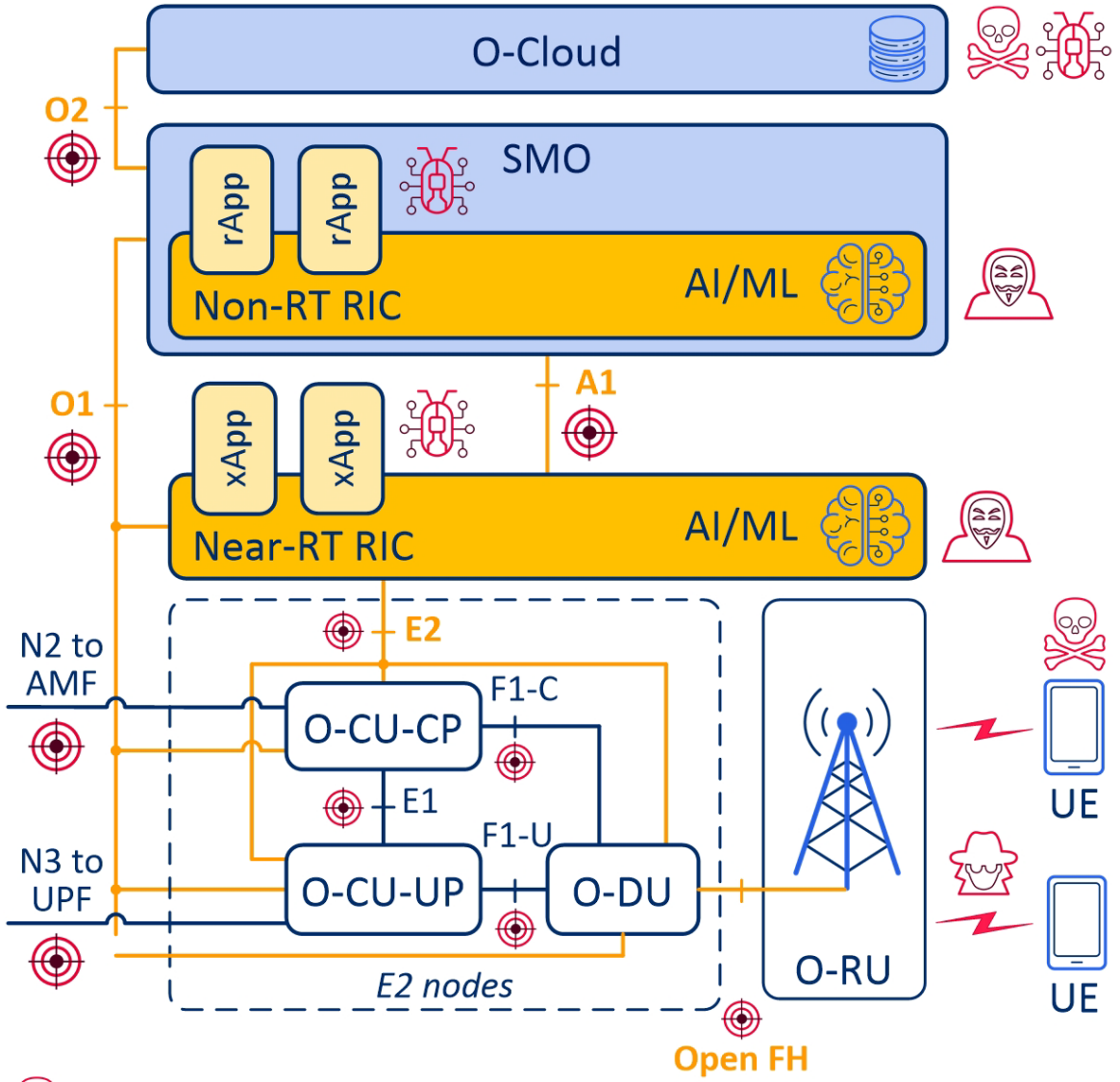


T > 1 s

1s > T ≥ 10 ms

T < 10 ms

O-RAN security



Poisoning and evasion attacks

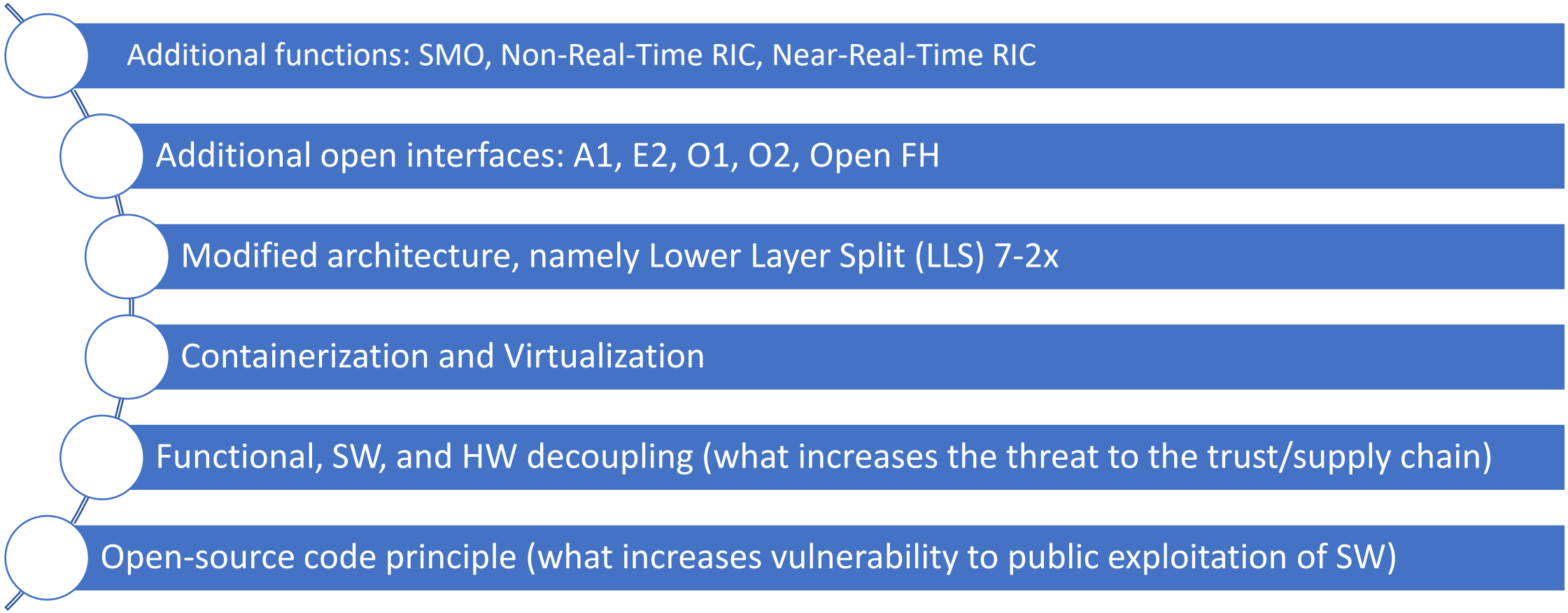
Radio communication attacks

Attacks on open interfaces

SW and API attacks

Inference attacks

O-RAN groups of threat surfaces



TIMEDO LABS

O-RAN security stakeholders and initiatives

Security Focus Group (SFG, WG11), founded by the O-RAN Alliance

The operators have committed (in “Open RAN Technical Priorities Focus on Security,”) to cooperating with national authoritiesofficially asked for O-RAN to be included in the GSMA Security Assurance Scheme and the EU Agency for Cybersecurity's 5G Certification Scheme.

Vendors and manufacturers have also noticed the O-RAN opportunities in helping secure the future of telecoms, as declared by several white papers and guiding documents

Governmental institutions. For example, UK Government published a Policy paper on “Open RAN principles”. USA, Australia, and Canada released joint statements on Telecommunications Supplier Diversity and O-RAN security.

O-RAN security opportunities by O-RAN Alliance

*"O-RAN Alliance recognizes that the attack surface of RAN systems is expanded due to open and cloud-based architectures, but transparency of new open interfaces will increase scrutiny and monitoring of vulnerabilities and failures. Openness also brings more competition to the telecommunication industry because implementation of security solutions will not be bound to products of just one vendor…"**

"…following all the security standards and specifications from SFG and 3GPP, and adopting a zero-trust approach and an end-to-end security governance over the implementation, makes O-RAN systems as secure, or even more secure, as traditional proprietary RAN systems." *

O-RAN Alliance SFG uses a risk-based approach compliant with the ISO 27005 methodology using a Zero Trust Architecture, defined by the National Institute of Standards and Technology.

* As indicated in the White Paper by O-RAN Alliance Security Focus Group (SFG)

TIMEDO LABS

O-RAN security opportunities

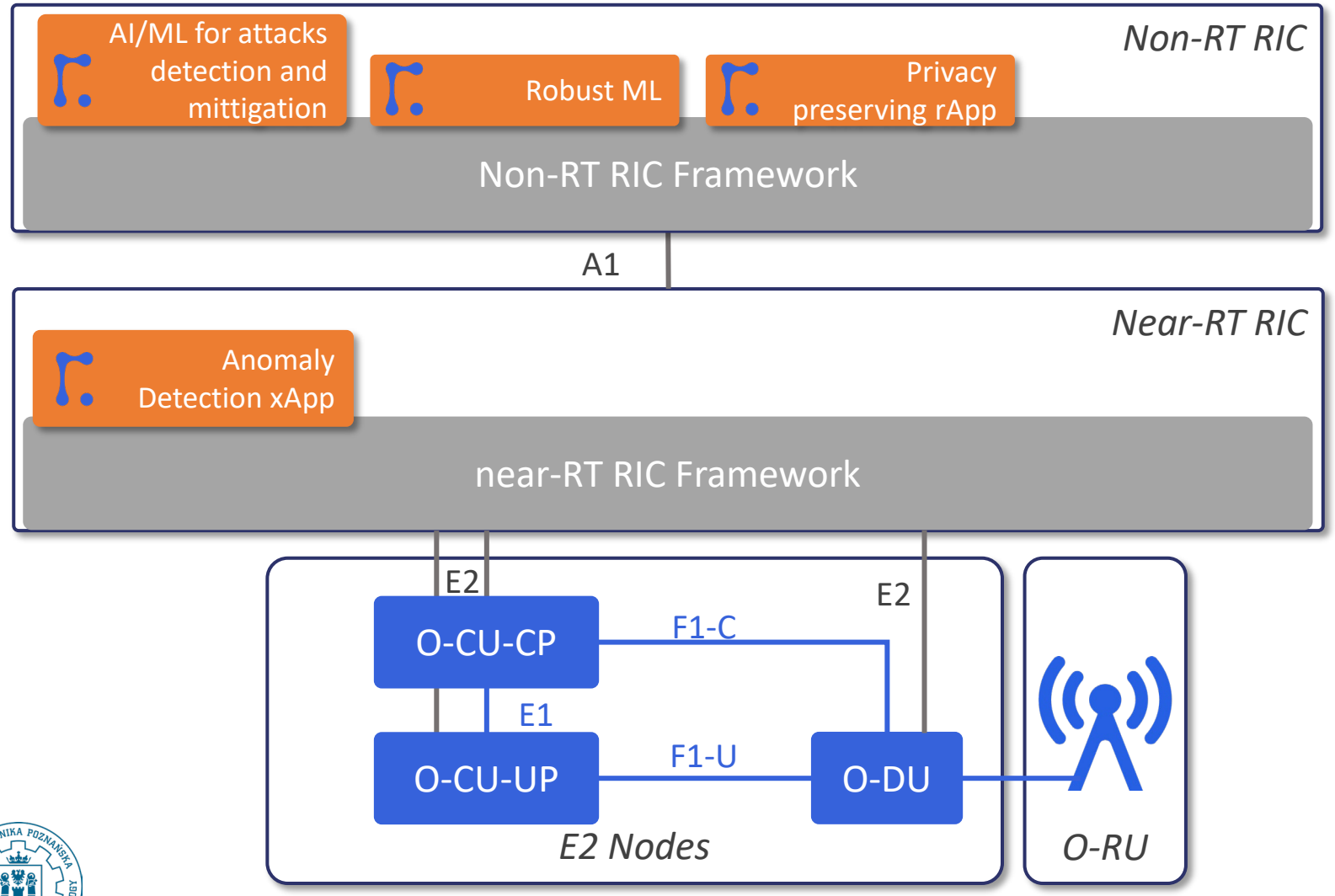
O-RAN architecture creates security opportunities (not just security issues, as usually considered).

O-RAN architecture allows for running the specialized programming modules/applications (xApps) in Near-RT RIC, which can be developed to continuously monitor and analyze security threats and protect RAN from malicious and illegal access to network segments.

O-RAN makes it possible to detect threats much faster before they affect the operation of the entire network.

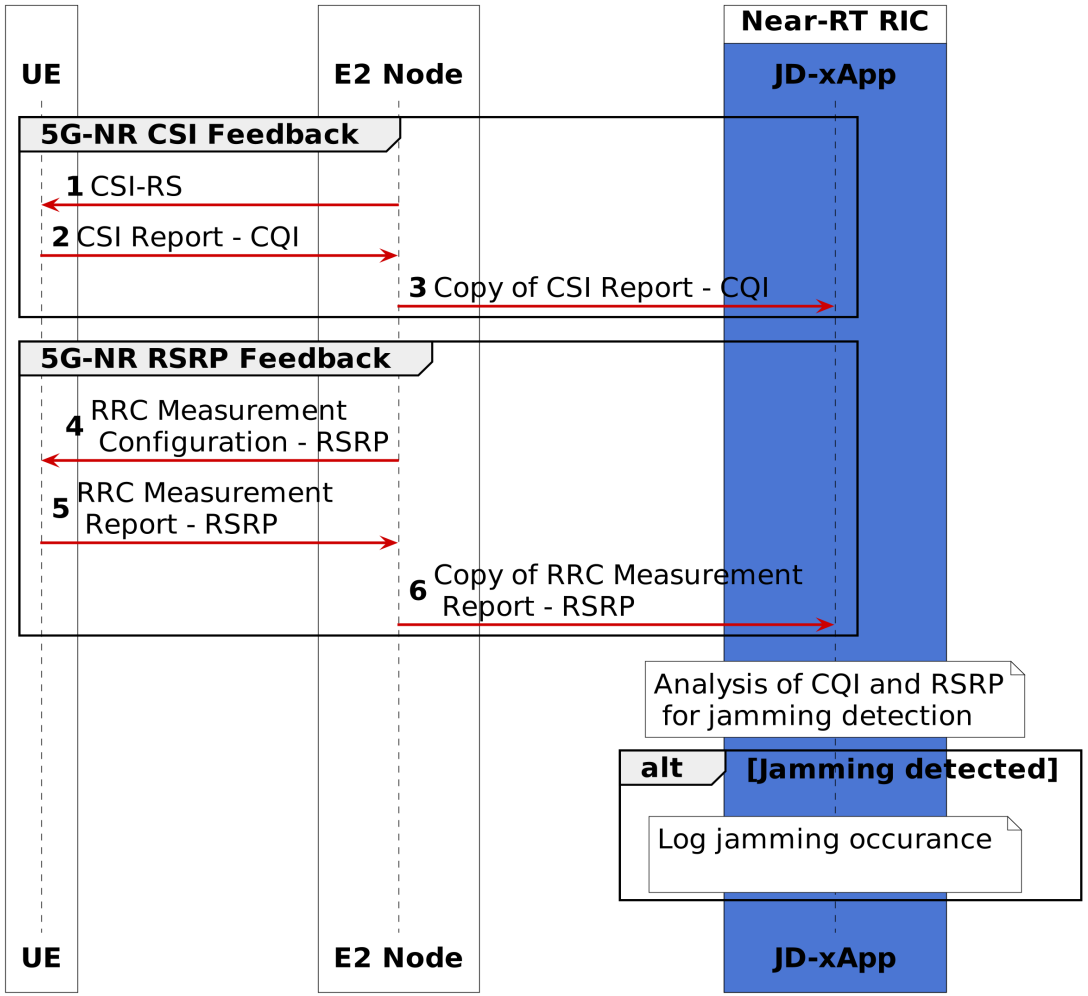
xApps and rApps can be developed for a specific types of threats in a given network. Due to the distributed architecture of the 5G/6G network and the use of MEC modules, threats can be detected closer to the place of their occurrence, which reduces the delay and the volume of control data.

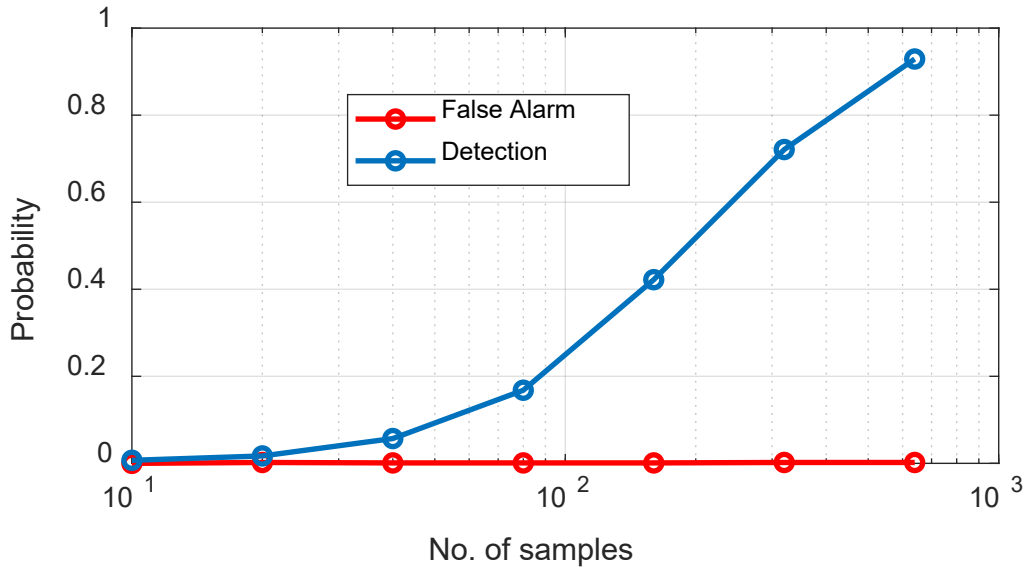
Example xApp/rApp for security



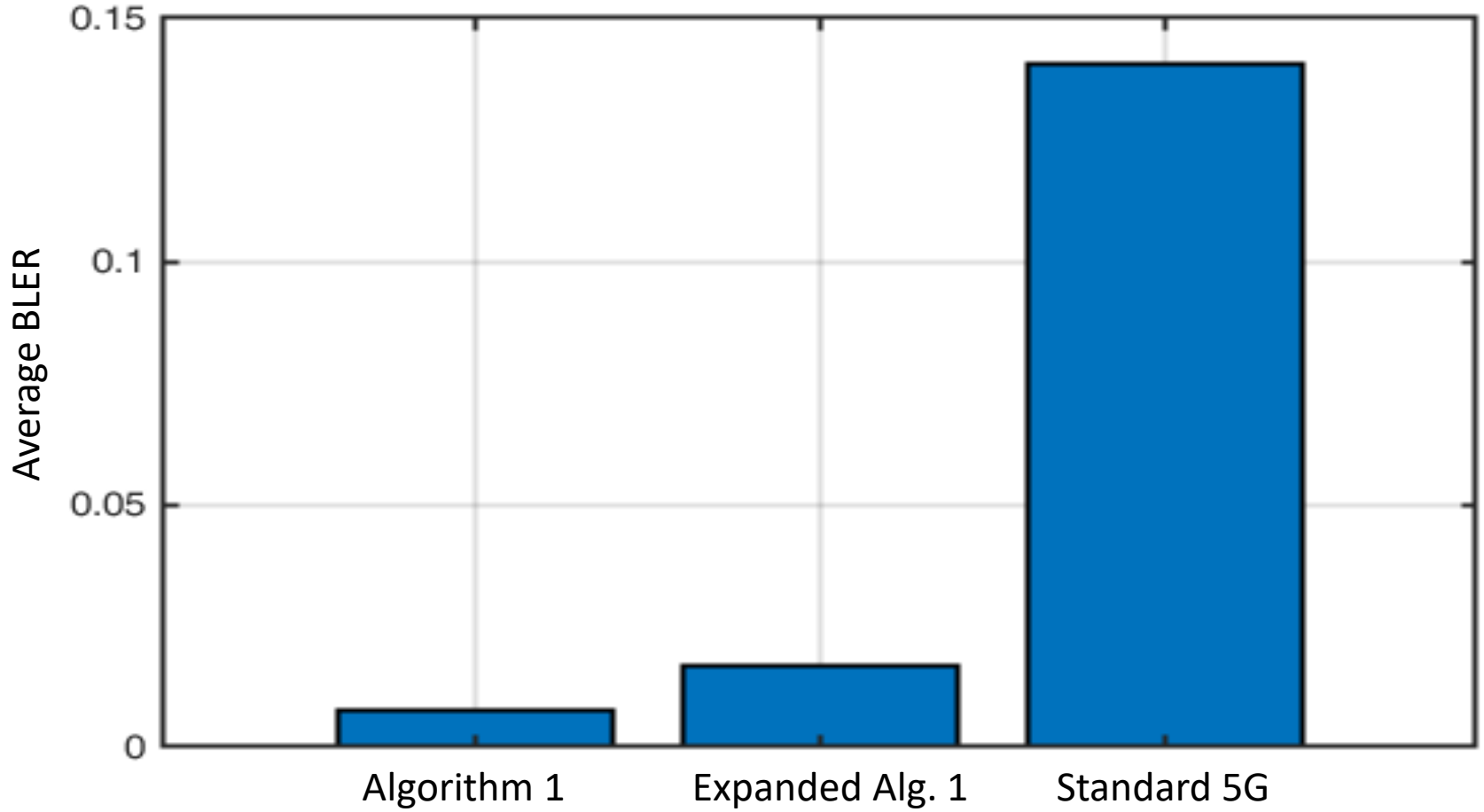
TIMEDO LABS

Jamming detection and mitigation example



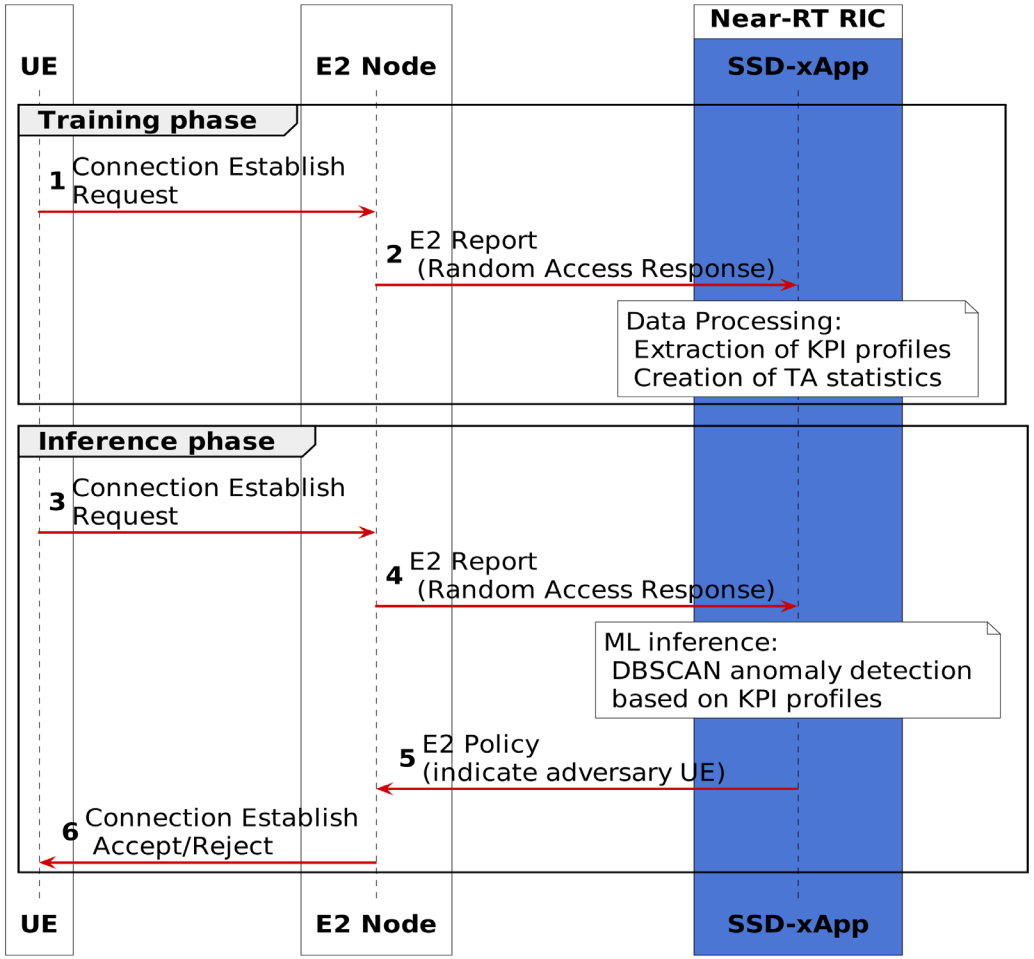


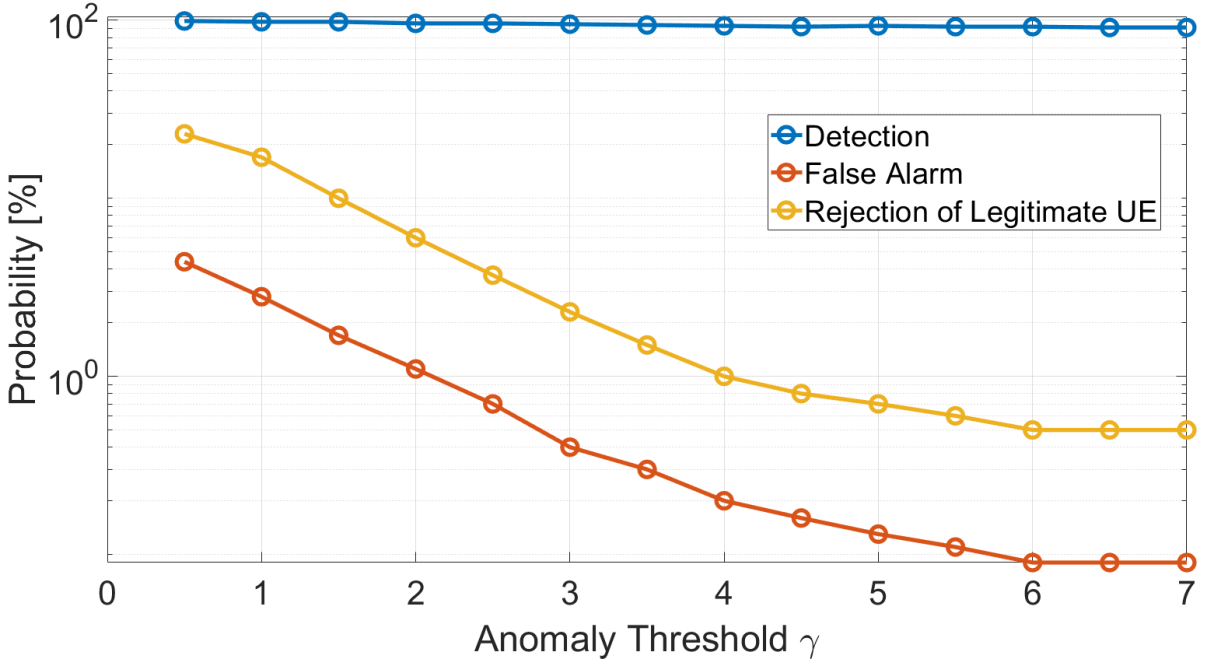
Jamming mitigation



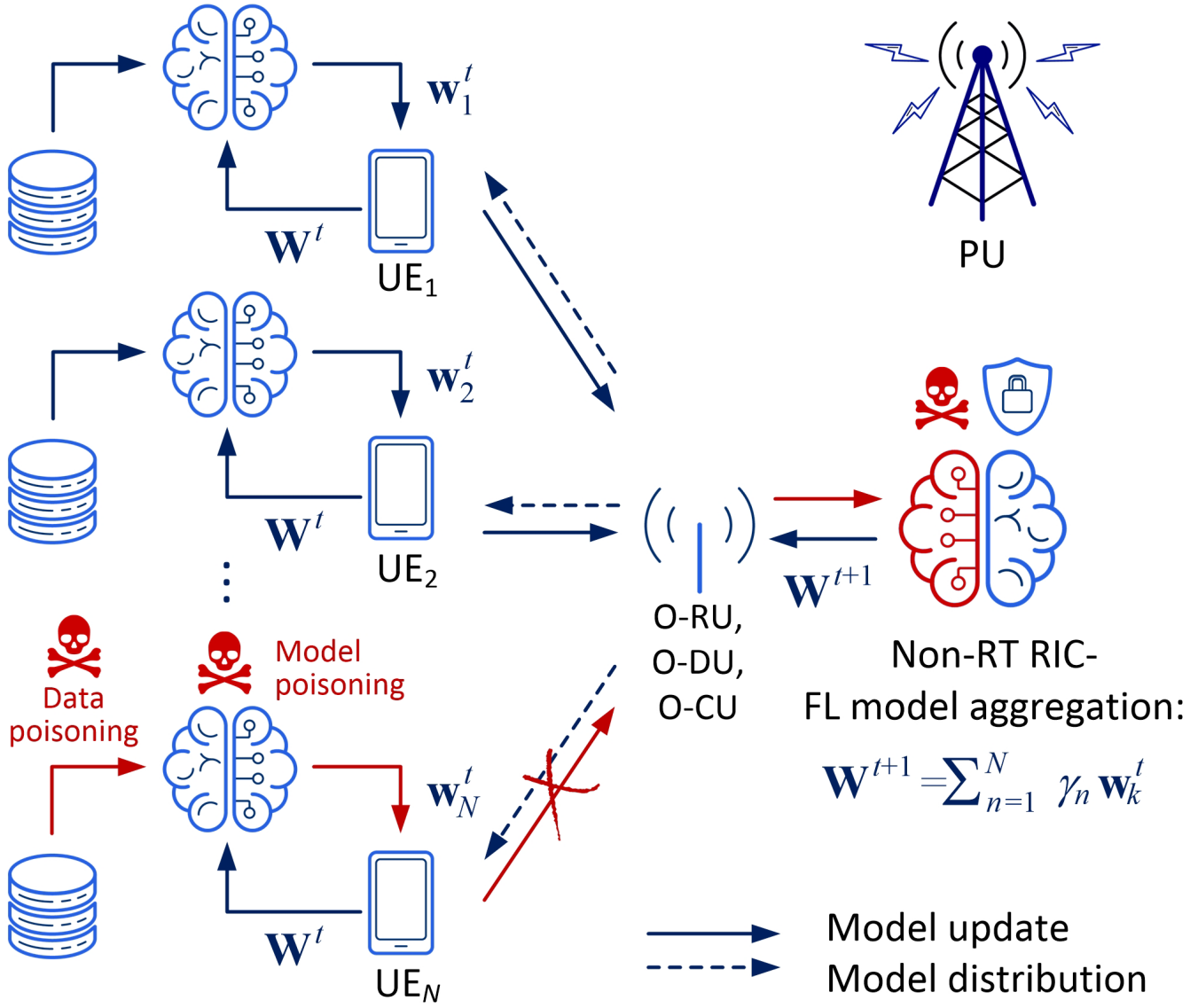
TIMEDO LABS

Signaling Storm (and DoS) detection and counteracting

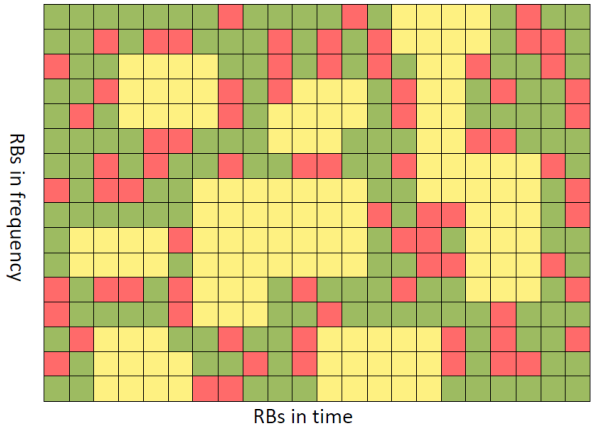




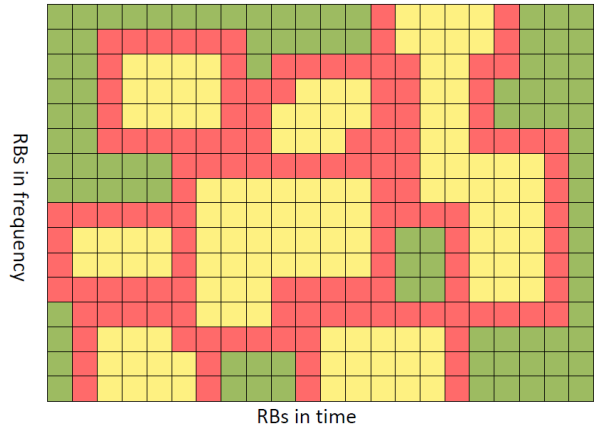
Poisoning-resistant federated-learning example



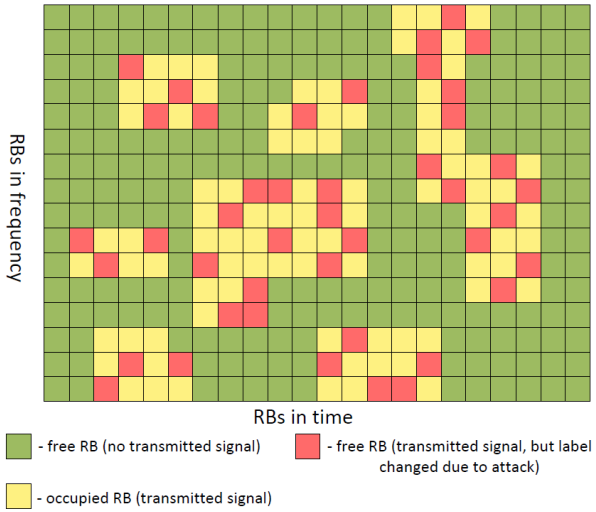
Attacks on FL-based RBs sensing



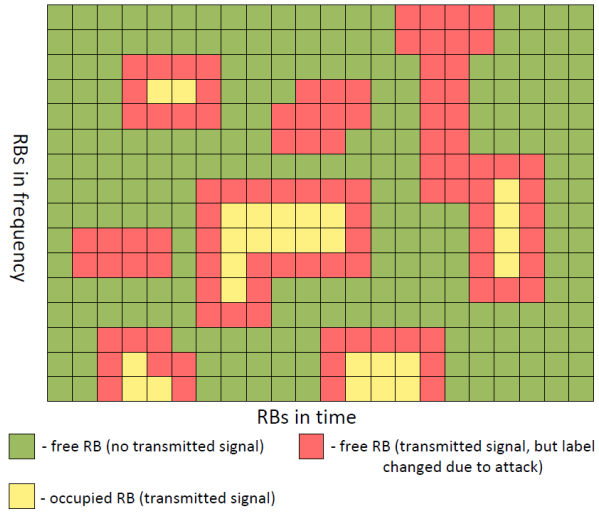
(a) Random attack aimed at the false increase in RBs occupancy



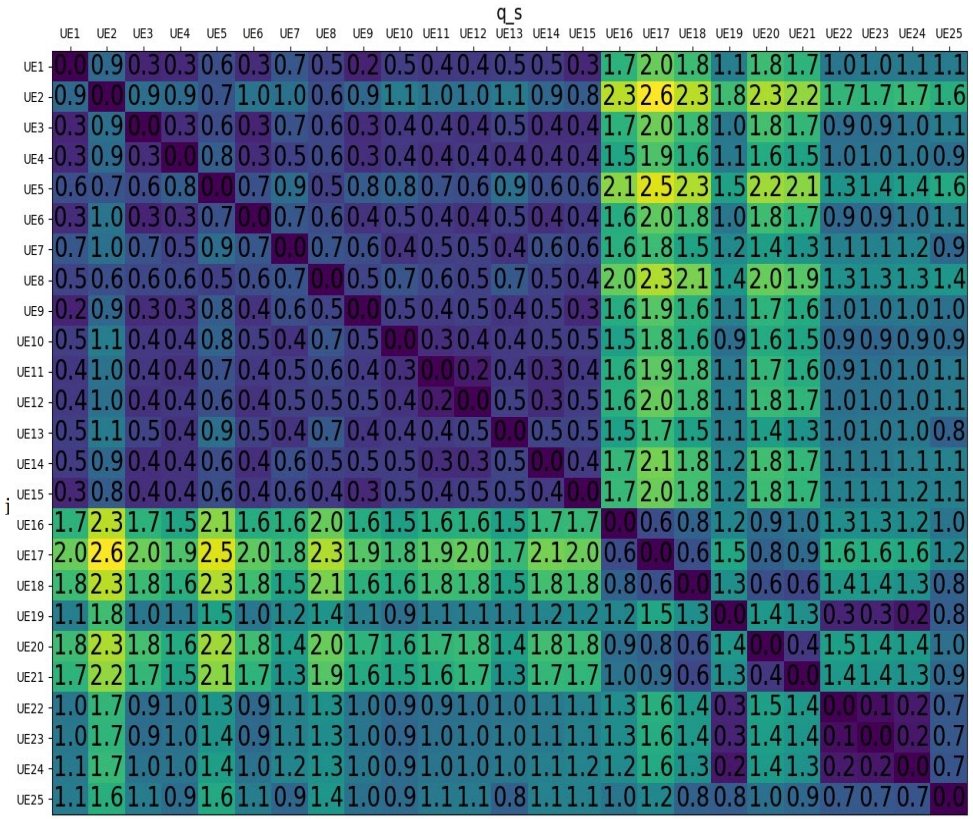
(a) Coordinated attack (encapsulation) aimed at the false increase in RBs occupancy



(b) Random attack aimed at the false decrease in RBs occupancy

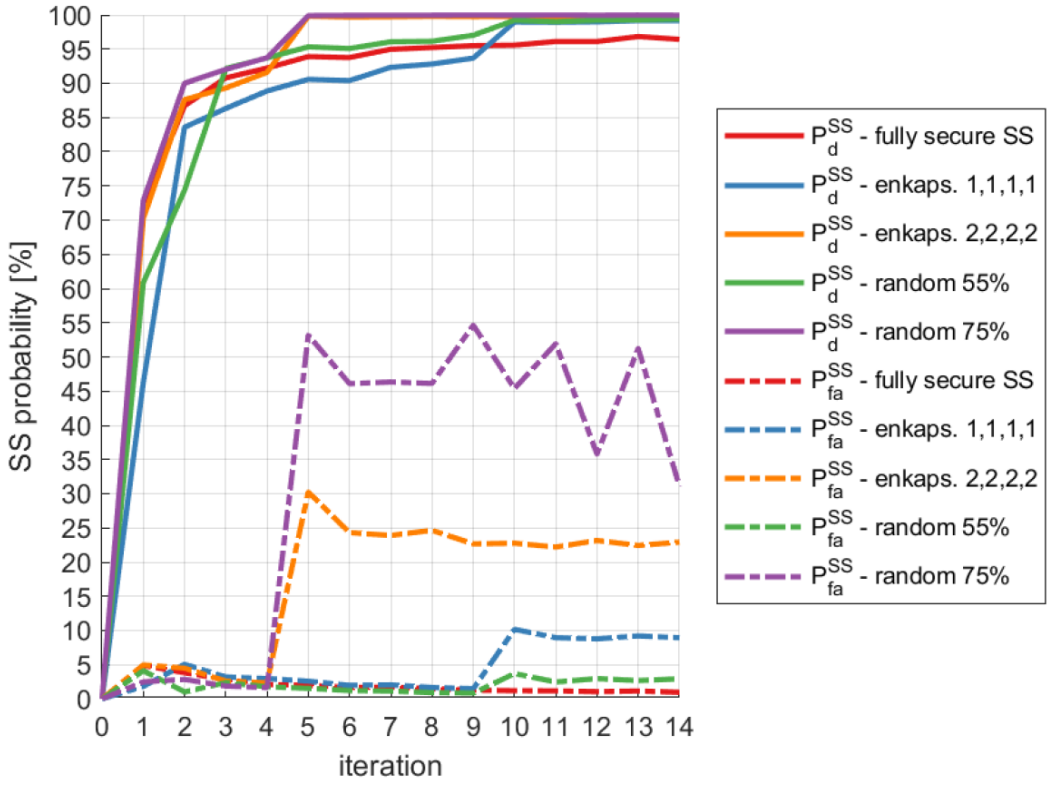


(b) Coordinated attack (encapsulation) aimed at the false decrease in RBs occupancy

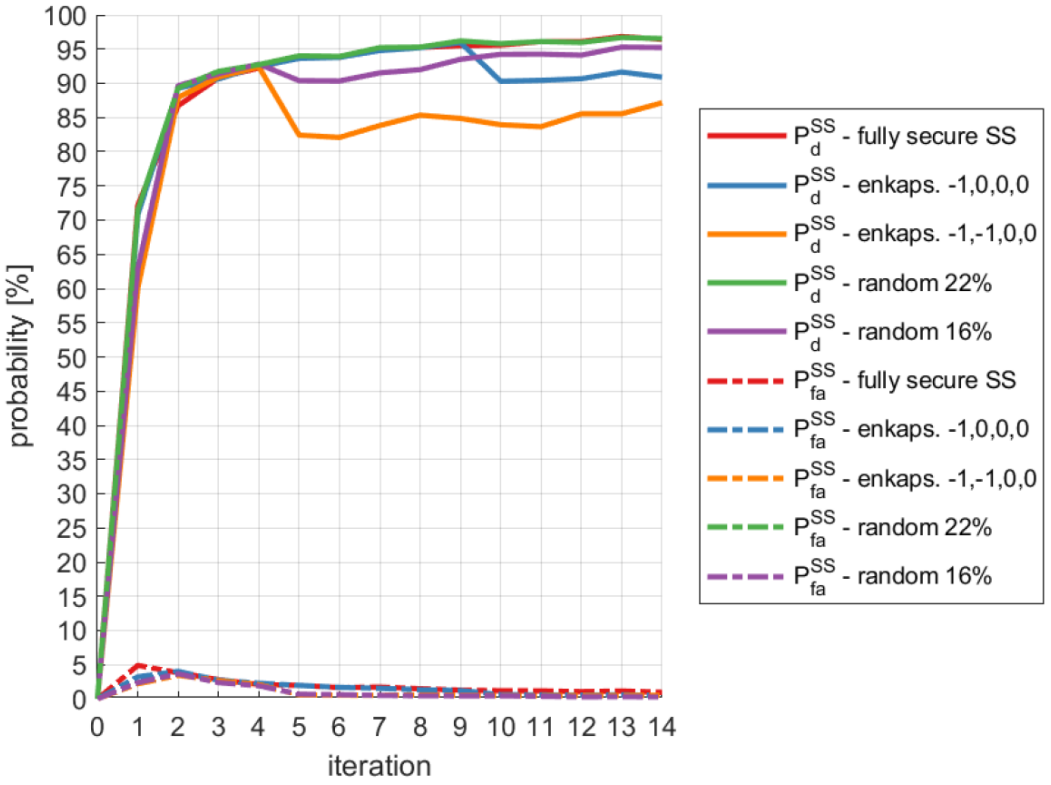


Kolmogorov-Smirnov similarity test on models to be aggregated

FL-based sensing – attack impact



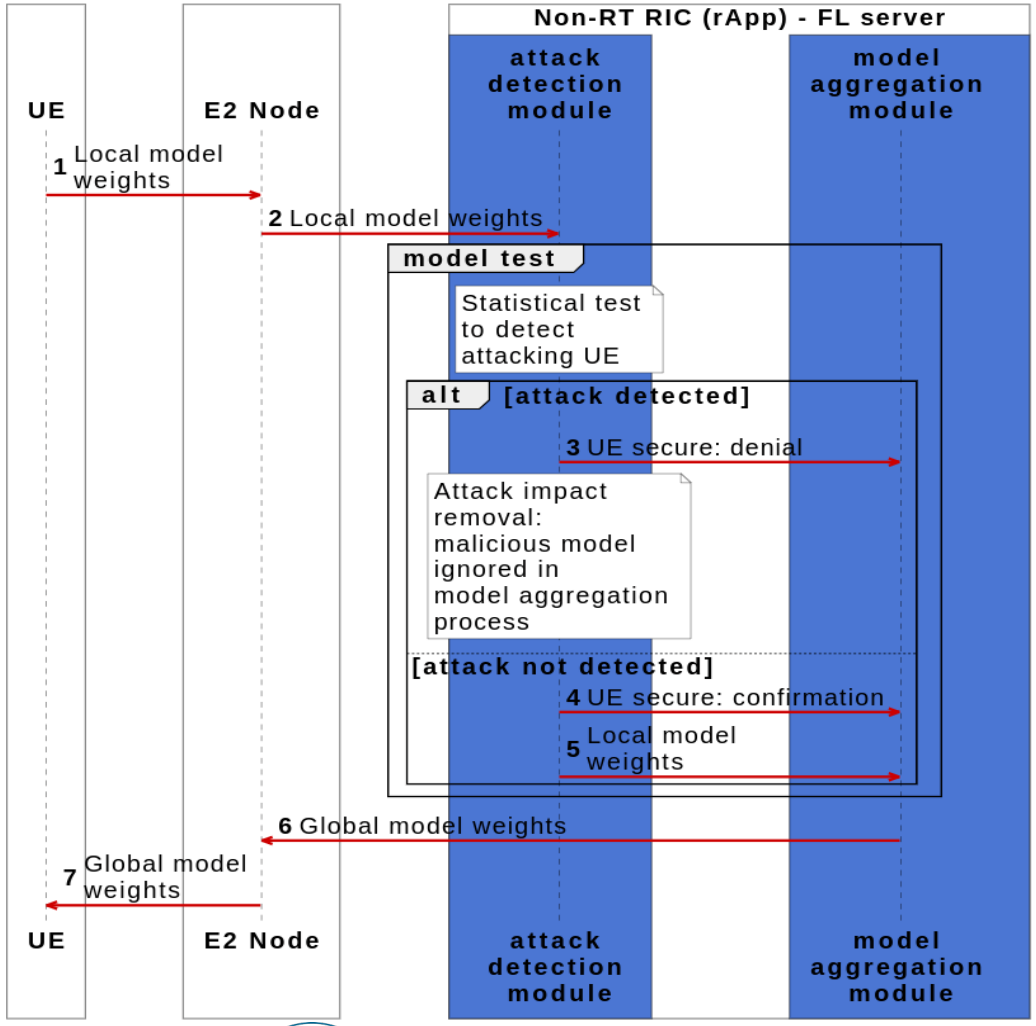
Estimated $P_{\mathrm{d}}^{\mathrm{SS}}$ and $P_{\mathrm{fa}}^{\mathrm{SS}}$ for FL-based SS under attacks for SNR = 20 dB vs. the iteration number; Attacks aimed at the false increase in RBs occupancy.

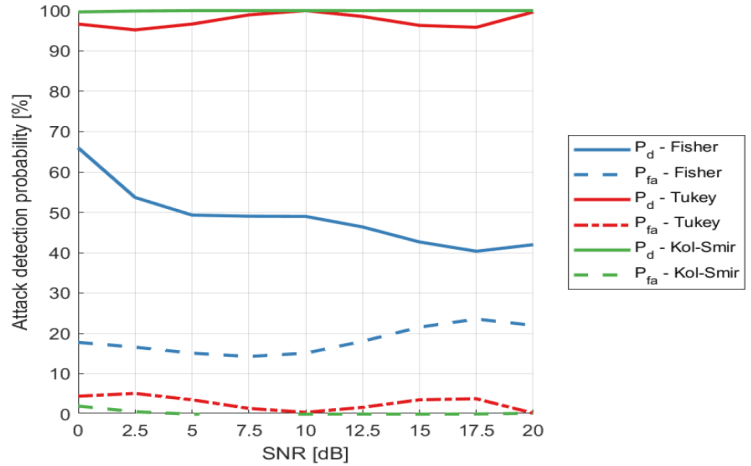


Estimated $P_{\mathrm{d}}^{\mathrm{SS}}$ and $P_{\mathrm{fa}}^{\mathrm{SS}}$ for FL-based SS under attacks for SNR = 20 dB vs. the iteration number; Attacks aimed at the false decrease in RBs occupancy.

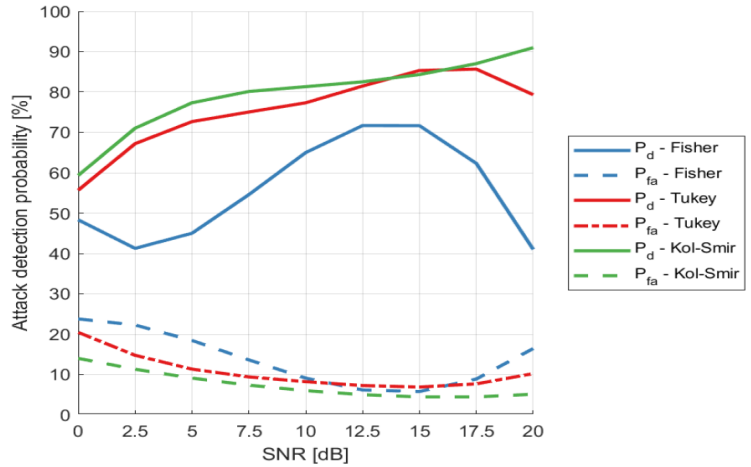
TIMEDO LABS

FL-based sensing – attack detection and defense



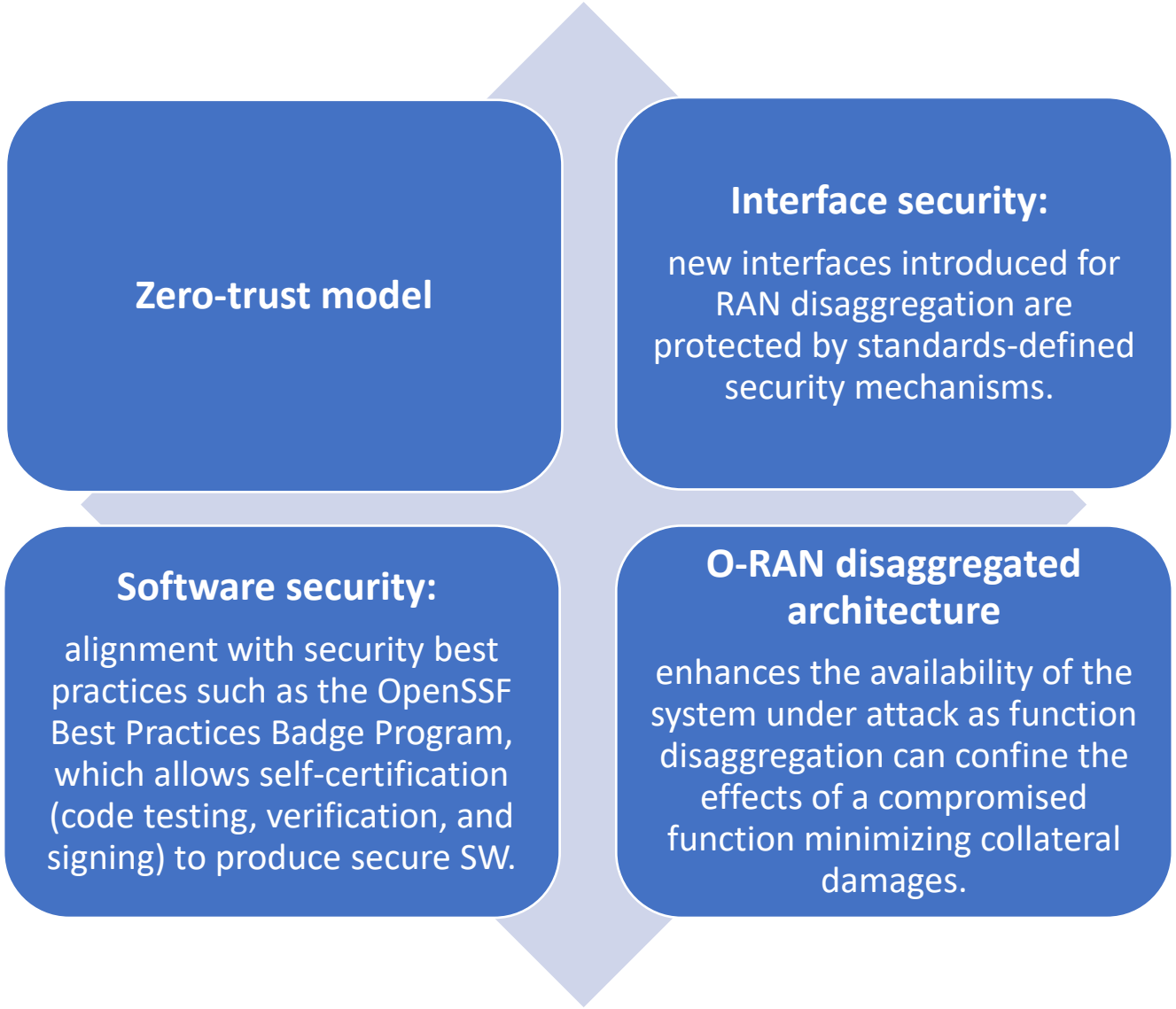


Estimated P_{d} and P_{fa} vs. SNR; Random attacks aimed at the false increase in RBs occupancy to 55%.



Estimated P_{d} and P_{fa} vs. SNR; En- capsulation (1,1,1,1) attacks aimed at the false increase in RBs occupancy.

Best practices for O-RAN security



Conclusions

O-RAN expanded threat surface: Open fronthaul interface, Near-RT RIC and its 3rd party xApps, Nnon-RT RIC and its 3rd party rApps, OCloud

An increased attack surface does not mean the system is less secure. Rather, open interfaces are more transparent than black-box implementations.

Openness and intelligence of future RANs create both opportunities and challenges.

Transparency and openness of O-RAN paves the way to more secure networks than those with proprietary implementations of a disaggregated or conventional monolithic RAN.

AI/ML enables ***visibility and intelligence*** for greater security.

TIMEDO LABS

20

Thank you!

Read my blog on O-RAN security:

https://rimedolabs.com/blog/o-ran-security-updates/

RIMEDO LABS