TIMEDO LABS

All things wireless

The O-RAN Whitepaper 2023

Security in O-RAN

Recently, security has been pointed out as one of the critical aspects moving forward within the O-RAN domain. Expanded threat surface, as well as specific security challenges and opportunities, have been identified. This whitepaper provides an overview of security topics in O-RAN, specifically in 5G/6G mobile radio networks. We also consider artificial intelligence embedded in the network edge as a great tool to support security. We present some xApps applied to detect and mitigate example attacks. Conclusions and a discussion on the directions of future developments follow this.

AUGUST 2023

Table of Contents

Executive Summary

This whitepaper provides a technical discussion of security, one of the most important topics currently related to the Open Radio Access Network (Open RAN or O-RAN). Security has been identified as crucial for further O-RAN development. Recently, operators, international organizations, and even governments have issued several declarations and recommendations to build the security and resilience of future telecommunication network infrastructure and operation. Research and development of secure architectures and algorithms used in these networks continues. Below, we overview trends in O-RAN security R&D and present Rimedo Labs' view on this critical topic.

First, an overview is provided of the most recent activities of the key players in O-RAN security. Key concepts for cybersecurity assurance in 5G and future 6G radio access networks are also reviewed.

Later, the whitepaper discusses two critical paradigms of 5G/6G networks, namely openness and intelligence. Their vulnerabilities and the potential to guarantee the security and privacy of communication are considered.

Next, the document focuses on Artificial Intelligence (AI) security applications in O-RAN. We elaborate on attack scenarios and security architectures using AI, assuming AI to be both the subject of cyberattacks and the method for counteracting them.

Finally, we present Rimedo Labs' selected xApps applied to detect and mitigate some example attacks on O-RAN: jamming and signaling storm. The UML sequence diagrams are provided together with simulation results exemplifying the efficiency of our algorithms.

The whitepaper ends with a summary and conclusions section along with a glossary of the used terms.

1.0 Introduction to O-RAN Security

For Open Radio Access Networks (O-RAN) [1][2], the year 2023 began with significant events and influential publications. A very recent report on “Open RAN MoU Progress Update on Maturity, Security and Energy Efficiency” issued in February 2023 by the five signatories (Deutsche Telekom, Orange, TIM, Telefónica, and Vodafone gathered within the Telecom Infra Project (TIP)) to the Open RAN MoU (from 2021) noted the essential progress in O-RAN. This year, the most crucial topics for further development are security and energy efficiency [3].

In this chapter, we investigate how different players of the O-RAN ecosystem look at the security topic. Those included operators, standardization, vendors, governments, and research communities.

1.1 The Voice of O-RAN ALLIANCE and Operators

Regarding security, the operators have committed (in [3]) to cooperating with national authorities, including information sharing, installation, and administration of O-RAN networks. Also, they have officially asked for O-RAN to be included in the GSMA Security Assurance Scheme (NESAS) and the European Union Agency for Cybersecurity's 5G Certification Scheme (ENISA). The consortium has pledged to improve O-RAN networks' security in several ways:

- to implement all mandatory measures outlined by the O-RAN ALLIANCE and 3GPP security specifications throughout their internal business processes and the supply chain;
- to apply a zero-trust principle to each vendor in the upcoming procurement processes;
- to include mandatory compliance with security specifications by the O-RAN suppliers (of network products and individual components);
- to engage a wide range of vendors, including European incumbent providers and SMEs (small and medium enterprises), to ensure a multivendor strategy;
- to address any unresolved security specification gaps through the O-RAN ALLIANCE.

During the O-RAN ALLIANCE Ecosystem Briefing at the Mobile World Congress (MWC) in Barcelona on February 28, O-RAN security issues and opportunities were emphasized by Claire Chauvin, the Strategy Architecture and Standardization Director, Orange. The two basic approaches were indicated:

» security through transparency;

» a risk-based (zero-trust) approach.

In March, the O-RAN ALLIANCE WG11 (earlier Security Focus Group, SFG) updated its specifications [4], which can be divided into four major sets: i) security threats models, ii) security requirements, iii) security protocol recommendations, and iv) security testing. Specifically, the updates from March 2023 include the following:

» O-RAN Security Requirements Specifications 5.0

» O-RAN Security Protocols Specification 5.0

» O-RAN Security Threat Modeling and Remediation Analysis 5.0

» O-RAN Study on Security for O-Cloud 2.0

» O-RAN Study on Security for Application Lifecycle Management 1.0

» O-RAN Study on Security Log Management 1.0

» O-RAN Study on Security for Service Management and Orchestration (SMO) 1.0

» O-RAN Study on Security for Shared O-RU (SharedORU) 1.0

» O-RAN Study on Security for Near Real-Time RIC and xApps 2.0

Other specifications issued or updated in 2022 are the following:

» O-RAN Security Test Specifications 3.0 (published in October 2022)

» O-RAN Study on Security for Non-RT-RIC 1.0 (published in July 2022)

1.2 The Voice of Vendors and Manufacturers

Early this year, in January 2023, Mavenir issued a new whitepaper on "Open architecture and supply chain diversity: securing telecoms into the future" [5]. There, Mavenir's five fundamental security principles are presented to drive the transition to open and secure systems:

- Open architecture must drive supply diversification,
- No hardware or software should result in vendor lock-in,
- No equipment or software should compromise entire units if it needs to be replaced or upgraded,
- Open, interoperable systems should provide complete visibility and control of their network's end-to-end security, and
- Open, interoperable systems should adopt a Zero Trust approach.

A fascinating discussion between John Baker, the Senior Vice President of Ecosystem Business Development at Mavenir, and Hosuk Lee-Makiyama, Director of the European Centre for International Political Economy (ECIPE) on January 13th, 2023, is available in a Euractiv "The Tech Brief" podcast [6]. The debate focuses on how security needs to be built from a zero-trust basis and the role Open RAN plays in helping secure the future of telecoms in the USA and Europe.

In 2022, some other key players in the open telecommunication networks arena addressed the O-RAN security issues and opportunities. For example, in October 2022, Rakuten Symphony issued "The Definitive Guide to Open RAN Security," which addressed the potential planes of attack and recommended strategies to mitigate risk from a total software system, configuration, and operational point of view [7]. Based on the over-decade Rakuten's experience in building secure modern software, this handbook is supposed to guide the industry toward enduring security strategies for next-generation networks being deployed worldwide.

NEC XON informed (on September 13th, 2022) on the collaboration with Fortinet to create a demonstration and test facility of best practice Open RAN security in the NEC XON Experience Centre in South Africa [8]. The Centre includes FortiGate from Fortinet, the world's most deployed next-generation firewall and highest performing hyper-scale firewall, which can cost-effectively secure Open RAN environment as reported by Anthony Laing, General Manager of Networking Business Unit at NEC XON – Sub-Saharan Africa.

Gavin Horn, the Senior Director of Engineering at Qualcomm Technologies, Inc., and Soo Bum Lee, Principal Engineer, at Qualcomm Technologies, Inc., in their article [9], notice that from a security standpoint, the disaggregated RAN architecture outlined in O-RAN offers numerous advantages. Disaggregation, for instance, enhances security resilience, adaptability, and agility. Moreover, O-RAN's openness and transparency provide the path for a more secure cellular network than private implementations of a disaggregated or conventional monolithic RAN, which in part rely on „security via obscurity."

In [10], Scott Poretsky, the Director of Security, Network Product Solutions, North America, and Joakim Jardal, the Strategic Product Manager, Security in Cloud RAN of Ericsson, consider visibility and intelligence of the service management and orchestration (SMO), such as the Ericsson Intelligent Automation Platform, play an essential role in the O-RAN security posture, providing purpose-built security functions and Artificial Intelligence (AI) and Machine Learning (ML) models. A secure, standardized R1 interface between the Non-RT RIC framework and rApps enables any rApp to work with any SMO and other rApps.

1.3 The Voice of Governmental Institutions

Regarding the security of open, interoperable networks, the past year was marked by several important policies, recommendations, and statements issued at the governmental and international levels. On April 29th, 2022, UK Government published a Policy paper on "Open RAN principles," which states, „The UK government is committed to building the security and resilience of critical network infrastructure by enhancing competition and innovation within the telecoms supply chain. Diversification of the telecoms network supply chain is essential to preserve and enhance the security, resilience, innovation, and competitiveness of telecoms networks. (...) By promoting vendor diversity, therefore, we seek to strengthen the ability of critical national networks to continue to function under threats including cyberattack and supplier exit, and for any vulnerabilities to be identified and rectified swiftly, with minimal impact."

On September 14th, 2022, the Australian Department of Home Affairs and the U.S. Department of Commerce, as represented by the National Telecommunications and Information Administration (NTIA), issued the "Joint Statement on 5G/Open RAN Information Sharing and Telecommunications Resilience and Security Between the United States and Australia" that is the basis for strengthening collaboration between USA and Australia on technical security of Open RAN [12]. Moreover, the next day (Sept. 15th), the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) of the USA issued the "Open Radio Access Network Security Considerations" [13]. These considerations address the threat surface area at the interfaces between technologies and components integrated via O-RAN architecture, risks emerging from the use of open-source applications, and threats related but not unique to O-RAN.

A "Joint statement between the United States of America, Australia, Canada, and the United Kingdom on Telecommunications Supplier Diversity" was released on December 08, 2022. In that statement, the signatory countries state that they "are committed to ensuring the security and resilience of their telecommunications networks, including by fostering a diverse supply chain and influencing the development of future telecommunications technologies such as 6G. Collectively, they recognize that open and interoperable architectures are one way of creating a more open, diverse, and innovative market. (...) Today they reaffirm our commitment to these principles, outlined in the (...) 2021 Prague Proposals". Moreover, they announced the endorsement of the abovementioned Open RAN Principles, published by the United Kingdom in April 2022 [11].

1.4 The Voice of IEEE

Ashutosh Dutta, Chair of IEEE SA Open RAN Industry Connections Activity, during the Future Network webinar on "Open RAN Challenges and Opportunities for Future Wireless Networks" [15], identified O-RAN security opportunities as

- programmability and virtualization that will adapt to the dynamic nature of traffic and multi-provider access,
- SoftRAN and cRAN in 5G networks will have embedded Distributed Denial of Service (DDoS) detection and mitigation functions,
- Dynamic Resource Scheduling significantly reduces the risk of jamming attacks targeting mission-critical devices,
- correlation between the control plane and the data plane traffic will enable security monitoring of traffic via correlation.

He also presented several security challenges and potential mitigation techniques for O-RAN.

1.5 The Voice of Researchers

Last but least, a recently published survey paper [16] provides insights on:

i. Classification of security-related risks,

ii. O-RAN possible security solutions based on blockchain, physical layer, and AI,

iii. general design errors of Open RAN, their consequences, and potential mitigation are presented, and importantly,

iv. a list of security benefits specific to O-RAN, and already available in V-RAN and 5G networks.

1.6 Security in O-RAN

We can infer from the summary provided in previous sections of 2022/2023 disputes, statements, and articles that the O-RAN ALLIANCE, the telecommunication business, governmental bodies, IEEE, and academic researchers speak with one voice: that the attacks surface is enlarged for O-RAN due to functional virtualization and open interfaces. Still, the same features can be used for security benefits as the threats can be monitored on these interfaces and closer to the attackers. Zero-trust principle and O-RAN disaggregated architecture offer enhanced security (see Figure 1.6-1).

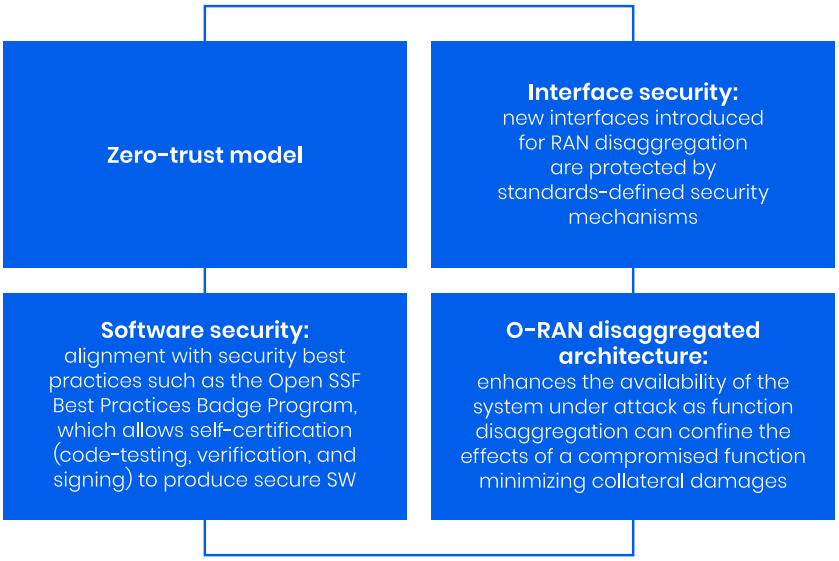


Fig. 1.6-1. The security offered by O-RAN

Indeed, it will be an exciting year for O-RAN to achieve maturity for applications in future networks. O-RAN security and security offered by O-RAN was and will be on the agenda of the events in 2023: the O-RAN Global PlugFest Spring 2023 (at four venues Across Asia, Europe, and North America), Open RAN World collocated with 6G Summit on 26-27th of April 2023 in Berlin, FYUZ organized by Telecom Infra Project on 9th-11th of October 2023 in Madrid, TelecomTV's fourth annual Open RAN Summit (virtual) organized on 21-22 June 2023.

2.0

RAN Openness and Intelligence for 5G/6G Security

The architecture of the 5G network, both at the current stage (non-standalone architecture – NSA) and ultimately implemented (stand-alone architecture – SA), will be almost entirely virtualized and based on software functionalities. As a result, it is and will be vulnerable to being used, attacked, and disrupted by hackers. Regarding the security of 5G networks, most of the attention of researchers, engineers, and practitioners is focused on software cybersecurity, although attacks on the software itself are not the only problem. This chapter discusses RAN-related aspects of 5G/6G security, including architecture-related risks, cybersecurity best practices, MEC, and O-RAN security opportunities.

2.1 Architecture-related Risks for 5G/6G Security

The 5G (and prospective 6G) architecture components and related risks are the following:

- Service-Based Architecture (SBA), decomposed, virtualized, and distributed network functions. The independence of network functions from infrastructure poses challenges for network security.
- Application Programming Interfaces (API). Poorly encrypted, inadequately secured APIs put network resources at risk of attack.
- Private and corporate 5G networks. Such networks, if not adequately protected, can be a source of attacks for the network segments to which they are connected.
- Multi-Access Edge Computing (MEC) [19]. Security management becomes difficult in decentralized information processing, such as edge computing, as significant network parts can be attacked anywhere.
- Radio Access Network (RAN) and Open-RAN. The radio segment of the mobile communication network is inherently exposed to attacks related to the omnipresent transmission medium. The open specification of the radio interface (O-RAN) introduced in the 5G network [1,2] poses a challenge to their security. Inadequately defined and poorly secured O-RAN applications, e.g., in the physical or MAC layer, may be vulnerable to these attacks.

The first three 5G security issues are similar to general software architecture and applications security problems. The last two strictly address RAN and its novel features, including its openness and intelligence. We will shortly discuss them in the following Chapter.

2.2 Best Practices

The best practices of network organizations in terms of cybersecurity include the following [20]:

- Zero trust, i.e., continuous authentication and authorization of users, nodes, connections, and interactions before granting access. Zero-trust security models assume that an attacker can be present in an internal and external environment and that an operator-owned environment is no different and not more trustworthy than any other environment. Its principle is: "Never trust, always verify" [21].
- Continuous and rigorous security practices and tests for software, hardware, and user equipment.
- Continuous monitoring of assets security logs and anomalous behavior or communication patterns to assess and reveal potential risk.
- Segmentation, i.e., creating logical groups of assets to restrict communication flows between them, e.g., through network firewalls.
- Threat protection, i.e., implementation of defensive security strategies, vulnerability management, denial-of-service defense, intrusion detection and prevention, and anti-malware systems.
- Data protection and privacy.

It is particularly interesting that mentioned openness and intelligence of future RAN create opportunities and challenges simultaneously.

2.3 MEC Security Opportunities

On the one hand, MEC and MEC-residing algorithms have to face security attacks, such as data poisoning, evasion attacks, or ML model stealing; on the other, edge intelligence allows for learning and detecting abnormal behavior of the attackers and counteracting adequately. The purpose of defense against ML attacks is to improve the resistance of ML techniques to adversary attacks by assessing their vulnerability and applying appropriate defense measures. We will discuss them in the next Chapter in greater detail.

2.4 O-RAN Security Opportunities

As indicated in the White Paper by O-RAN Alliance Security Focus Group (SFG) [21]: "O-RAN Alliance recognizes that the attack surface of RAN systems is expanded due to open and cloud-based architectures, but the transparency of new open interfaces will increase scrutiny and monitoring of vulnerabilities and failures. Openness also brings more competition to the telecommunication industry because the implementation of security solutions will not be bound to products of just one vendor but will be usable with equipment from any O-RAN compliant vendor". O-RAN Alliance's SFG uses a risk-based approach compliant with the ISO 27005 [22] methodology using a Zero Trust Architecture, defined by the National Institute of Standards and Technology [23]. The authors of [21] claim that "...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."

Moreover, O-RAN architecture allows for running the specialized programming modules/applications (xApps) in Near-Real-Time RAN Intelligent Controller (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. It makes it possible to detect threats much faster before they affect the operation of the entire network. Importantly, xApps can be developed for 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.

3.0
AI for O-RAN Security

When talking about future Radio Access Networks (RANs) security threats, one has to consider typical (or "traditional") threats related to the radio segment of a network, as well as the expanded attack surface, due to the open architecture and interfaces in O-RAN. A discussion should expand these considerations on AI algorithms security issues since AI is envisioned to be embedded in multiple network tiers starting from User Equipment (UE), the gNodeB (as specialized programming modules/applications – xApps and Radio Intelligent Controllers – RICs in O-RAN), at the edge of the network in the Multi-access Edge Computing (MEC) module and in a cloud. This vision is reflected in the term Intelligent Internet of Intelligent Things (IIoIT), which is getting increasingly popular.

In this chapter, we extend our considerations on threats and opportunities that O-RAN specifications create for network security (presented in Chapter 2.0) to deliberations on how AI at the network edge can, on the one hand, be a target of attacks and, on the other, increase the network security.

3.1 Radio Segment Threats

The radio segment of the contemporary and future mobile communication networks is inherently exposed to attacks related to the omnipresent transmission medium. RAN and open specification of RAN (O-RAN) introduced in the 5G network [1,2] pose a challenge to their security. The typical and identified security threats for RAN are:

- Jamming – normal, delusive (including Primary User Emulation – PUE), random, responsive, go-next, control-channel jamming, that injects unwanted signals in either the communication or control channels,
- Denial of Service (DoS), Distributed DoS (DDoS) exhausting network resources and making it impossible to serve users, creating traffic congestion or wasting network resources,
- Signaling Storm – seizing the resources for the transmission of signaling information in the control plane,
- Eavesdropping and traffic analysis,
- Man in the Middle (MITM) where an adversary intercepts users' messages, analyzes them, or changes their content, e.g., by creating a fake base station, and
- Free-riding (spoofing) attacks to conserve local computing resources, to make up for lack of necessary data, or to avoid violating data privacy laws.

These threats are well described in the literature, and more and more efficient countermeasures are also developed (e.g., see [24]).

3.2 O-RAN-related Threats

We should also note that interfaces for O-RAN, including the front-haul interface, O1, O2, A1, and E2, that are being introduced can also potentially be targets of attacks. Attackers can utilize these new open interfaces to attack the system, which could lead to a denial of service, data tampering, or data leaking, all of which indirectly impact the system's security. Each O-RAN interface and function may be subject to different threats, and each threat will have a particular impact; thus, for each threat, specific security measures and solutions must be used for all aspects and assets [25].

3.3 AI/ML-related Threats

AI, especially edge intelligence, is envisioned as one of the fundamental paradigms for 5G and future 6G systems. On the one hand, AI and ML algorithms can help manage the network, e.g., by improving resource allocation, improving energy efficiency, or optimizing multi-antenna transmission or beamforming. Importantly, they can also be developed to improve security, e.g., by detecting anomalies in radio traffic. On the other hand, the use of AI/ML algorithms exposes the access network to a new type of attack – attacks on machine learning algorithms. They can be classified as (i) poisoning attacks, (ii) evasion attacks, and (iii) inference attacks [26].

Poisoning attacks aim to impact the learning outcomes by manipulating the data or the learning algorithm in the model training phase. Based on the previously learned model, the evasion attack is aimed at the inference stage (test phase). Here, the attacker tries to bypass the model by introducing small perturbations in the input values. Inference attacks (reverse engineering) aim to recover the training data and/or their labels, discover the model architecture and parameters (model stealing), or determine whether a sample was used to train a target ML model. This is supposed to be done by observing and using the results of the ML algorithm and model under attack.

In Figure 3.3-1, these mentioned attacks on RAN with embedded intelligence are graphically presented. As the computational capacity of centralized units (in gNodeB or MEC) is typically higher than that of the UE, all these algorithms can be designed to work together, e.g., as federated learning (FL).

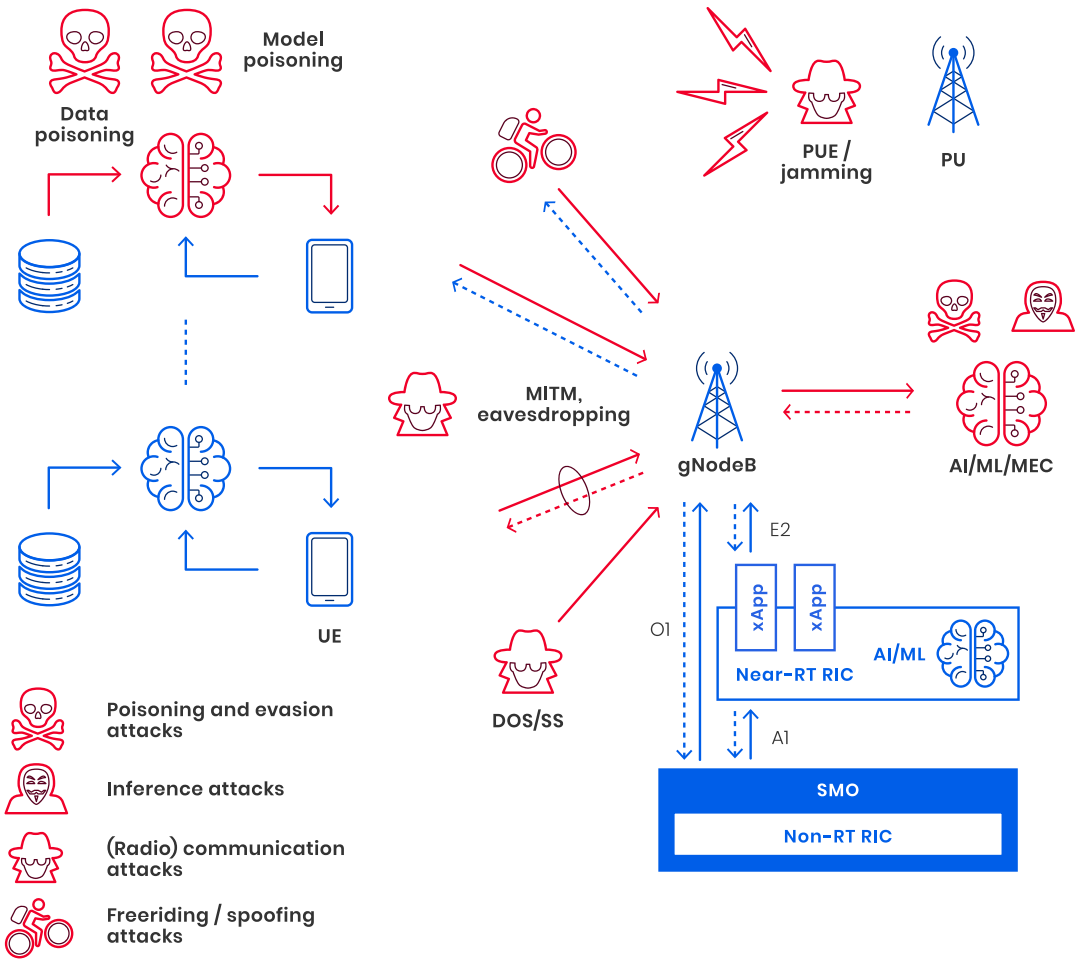


Fig. 3.3-1. Attacks on intelligent RAN and O-RAN-embedded intelligent countermeasures

3.4 AI for O-RAN Security

Let us consider how O-RAN architecture can increase security in radio access networks and connected MEC. O-RAN architecture allows for running 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. It makes it possible to detect threats much faster before they affect the operation of the entire network. xApps can be developed for specific types of threats in a given network that can be detected closer to the place of their occurrence. As discussed above, AI/ML algorithms, including those developed for O-RAN, can be the target of cyberattacks, and specific defense strategies have to be in place and onboard O-RAN platforms. Again, it is possible to develop xApps for specifying threats like this. xApps developed for RAN and O-RAN security should apply best practices for network cybersecurity, which include a zero-trust approach, continuous monitoring, and security tests, data protection and privacy, and defensive mechanisms [24].

Examples of a defensive strategy against various kinds of attacks is to detect anomalies in the radio traffic using ML methods, such as the k-nearest neighbors (k-NN) [27], DBSCAN clustering algorithm [28], decision trees, and neural networks (NN) [29], as well as deep learning NN [30]. Convolutional Neural Networks (CNN) can be used for detecting and eliminating poisoned data and models in FL. (A specific use case of the FL application to spectrum sensing is described in [31]).

4.0 Anomaly Detection in O-RAN

The operating patterns of adversaries attacking the open radio interface are complicated and not obvious, e.g., an adversary may change the attacked band or periodically interrupt an attack. The number of attackers can change, impacting the attack severity. The prospective defense algorithms should be able to not only detect anomalies but also adapt to a variety of attack mechanisms. This can be done, as we emphasized above, by AI/ML methods, which have been researched over the last years (e.g., see [27]-[29]). Below, we present two representative AI/ML-based attack detection and analysis mechanisms under development for Near-RT RIC.

4.1 Jamming Detection, Analysis, and Mitigation

The 5G system, due to broadband and adaptive transmission and advanced channel coding, is quite resistant to interference in the long run. On the other hand, the response to an anomaly disturbance may take several milliseconds. This delay may be unacceptable for Ultra-Reliable, Low Latency Communication (URLLC) traffic. As such, the detection should be carried out without additional delay, requiring Near-RT RIC to be used. In addition, this type of attack can be easy and inexpensive to carry out, increasing its occurrence probability.

Multiple ML approaches can be used to address jamming detection. Supervised learning can be used to detect jamming as an anomaly based on signal quality parameters reported by UEs (e.g., Channel Quality Indicator - CQI and Reference Signals Received Power – RSRP). However, this requires building a database of reports with labels for both jamming and non-jamming situations. This problem does not exist if unsupervised methods are used. We propose to analyze the two-dimensional distribution of CQI and RSRP values to find the anomaly caused by jamming. In this method, CQI and RSRP reports are collected for a given cell assuming some prespecified memory size reflecting the valid time horizon, e.g., to account for rejecting older reports that might have been collected under different propagation conditions or inter-site interference levels. If the report is not classified as collected under jamming, it is added to the current CQI-RSRP distribution estimate. A new report is compared with the current distribution, assuming its local Gaussian approximation with prespecified false alarm probability. If a given report is more distanced from the distribution than the constant false alarm threshold, it is assumed that jamming occurs. The sequence UML diagram of this method is presented in Figure 4.1-1. It shows what messages over what interfaces must be exchanged to enable jamming detection in the xApp.

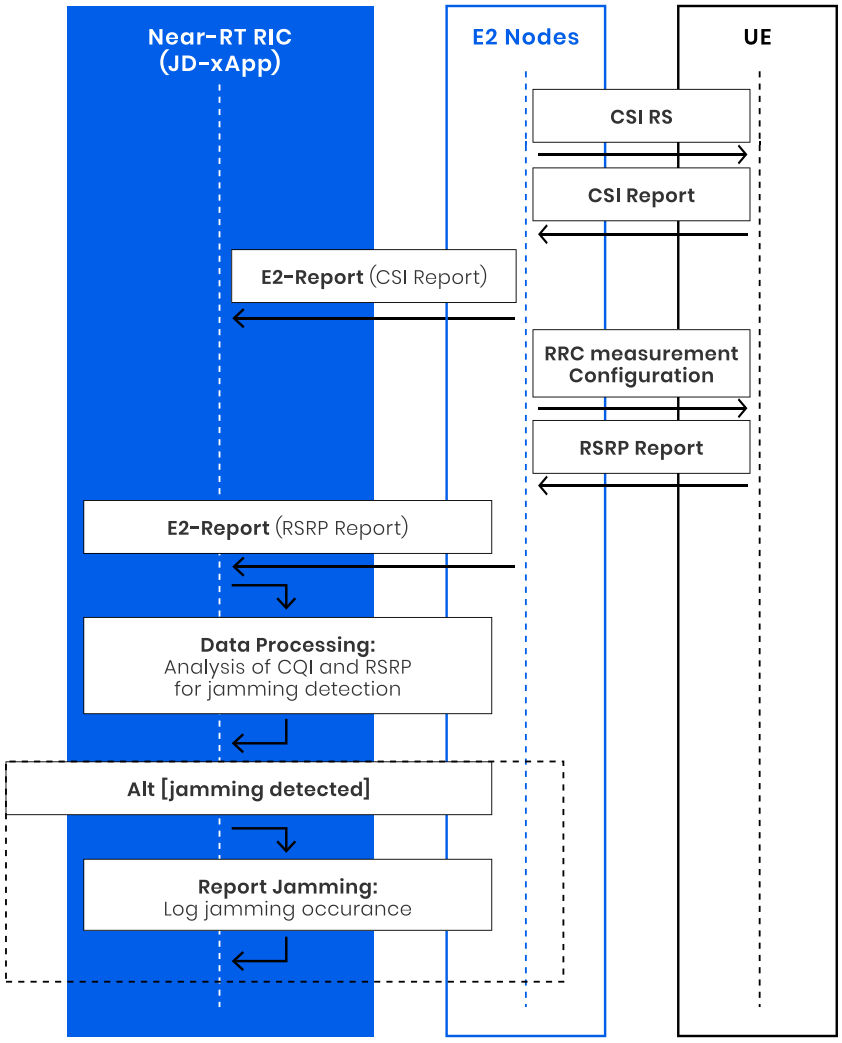


Fig. 4.1-1. UML sequence diagram for jamming detection (Jamming Detection xApp, JD-xApp).

Although the probability of jamming detection of unsupervised learning may be naturally lower than the supervised learning (training-based) based method, tests show that it is highly effective in the presence of highly damaging broadband jamming. Example results are shown in Fig. 4.1-2 (for the exact scenario definition, refer to [32]). Moreover, the probability of false jamming detection is relatively low. This requires a rather large base of reference measurements to create a reliable RSRP-CQI distribution estimate.

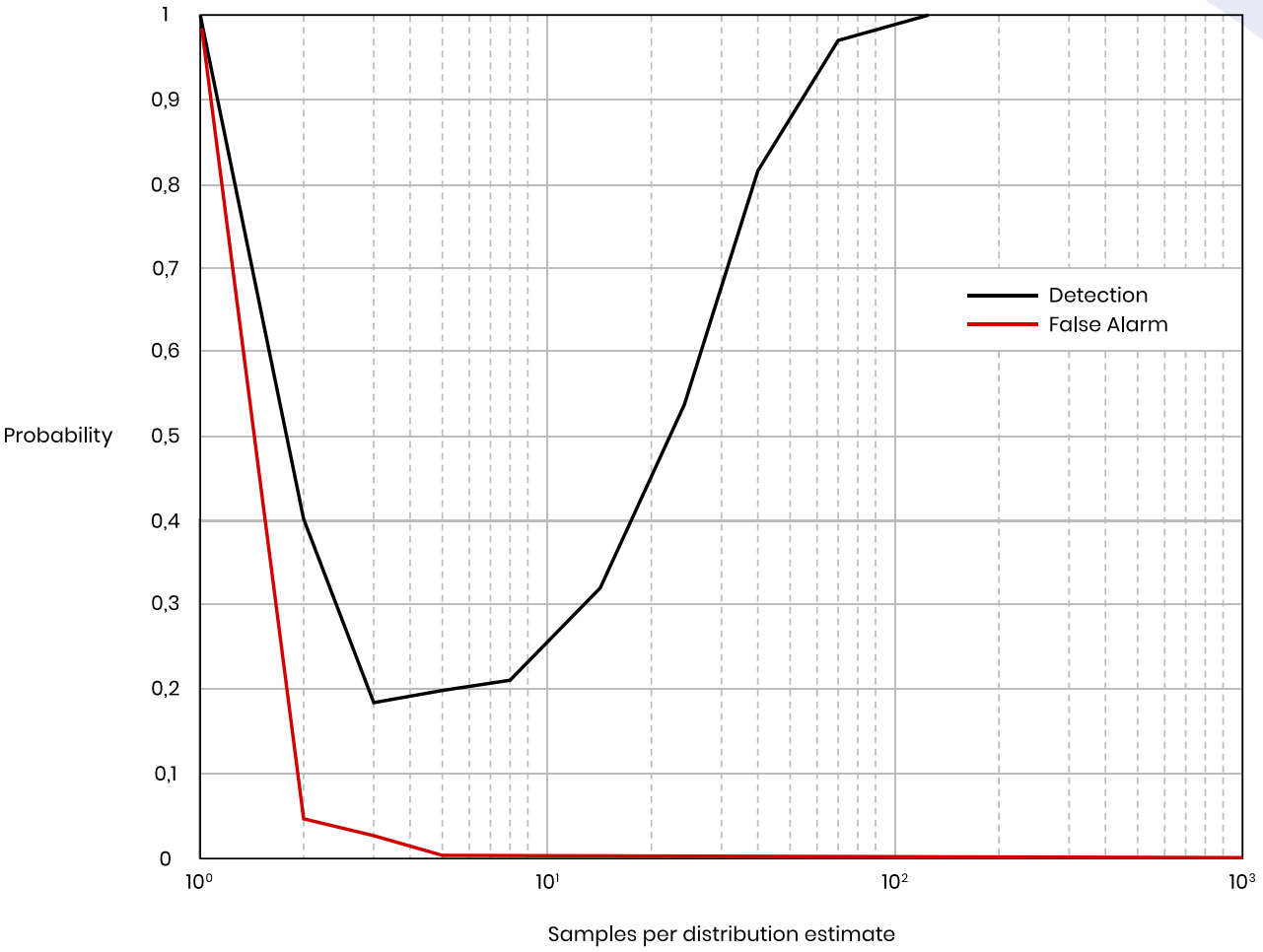


Fig. 4.1-2. The probability of jamming detection and false alarm as a function of the number of samples used for distribution estimate in an example scenario.

The other issue is the mitigation of the detected jamming effects. Multiple solutions are possible here, from major base station reconfigurations, e.g., carrier frequency change, to Modulation and Coding Schemes (MCS) adaptations. Jammers should be automatically reported to the security monitoring entity and responsible authorities.

4.2 Signalling Storm Detection, Analysis, and Mitigation

Signaling Storm is a specific case of DoS or DDoS attack identified by the O-RAN ALLIANCE to be addressed by xApps. When firing this kind of attack, devices authorized (or not) to access the network make repeated attempts to connect to the network, "clogging up" the Random Access Channel (RACH). In addition, due to the multi-stage nature of the hand-shaking procedure, a whole range of redundant control information is generated in the access and core network. It is, therefore, essential to quickly locate the source of this threat and decide to reject the connection request at an early stage of registration.

To detect signaling storms or DDoS attacks at the early stage of RAN (before reaching the core network), the O-RAN interfaces can be used to create so-called KPI profiles [28] that are created in Near-RT RIC and updated dynamically. Based on the monitoring of Random Access Responses, the KPI profile can capture statistics of the network access requests and Timing Advance (TA) parameters of each UE. In particular, IoT devices have this kind of profile and statistics constant. Based on the KPI profile and the currently observed number of access requests, the so-called anomaly values (or metrics) are calculated and then input to a weighted version of the DBSCAN grouping algorithm. The algorithm decides on the presence or absence of a Signaling Storm attack. In this case, the threat analysis determines the adversary's approximate distance from gNodeB (E2 Node). In the case of adversary UEs, an increased number of Msg2: Random Access Response messages containing the same TA parameter measured by gNodeB (E2 Node) will be observed. This way, by detecting the adversary's activity, we can automatically identify to which group of IoT devices it belongs. (Usually, several devices located at a similar distance from the base station have the same TA.) After the detection of a signaling storm, connection requests associated with a given TA may be rejected at the stage of RAN to protect core network resources.

The KPI profile-based signaling storm detection can be deployed as xApp [33]. The sequence UML diagram of the signaling storm/DDoS attack detection algorithm, deployed as xApp in Near-RT RIC, is shown in Fig. 4.2-1. The sequence can be divided into two phases: the training phase and the inference phase. The training phase aims to build KPI profiles based on the Random Access responses forwarded to the Near-RT RIC from E2 Node (gNodeB) via the E2 interface. Within this phase, tuning the detection algorithm's parameters is also done, e.g., adjusting the threshold for the anomaly metric above which the attack will be detected. In the inference phase, detection of the adversary's presence takes place already at the level of the access network. It only requires the collection of Msg2 messages for a period corresponding to the KPI profile validity. If the adversary activity is detected, the xApp utilizes the E2 interface to notify the gNodeB (E2 Node) to reject connection requests from a given UE, i.e., to send an RRC Connection Reject message to stop UE authentication within the core network.

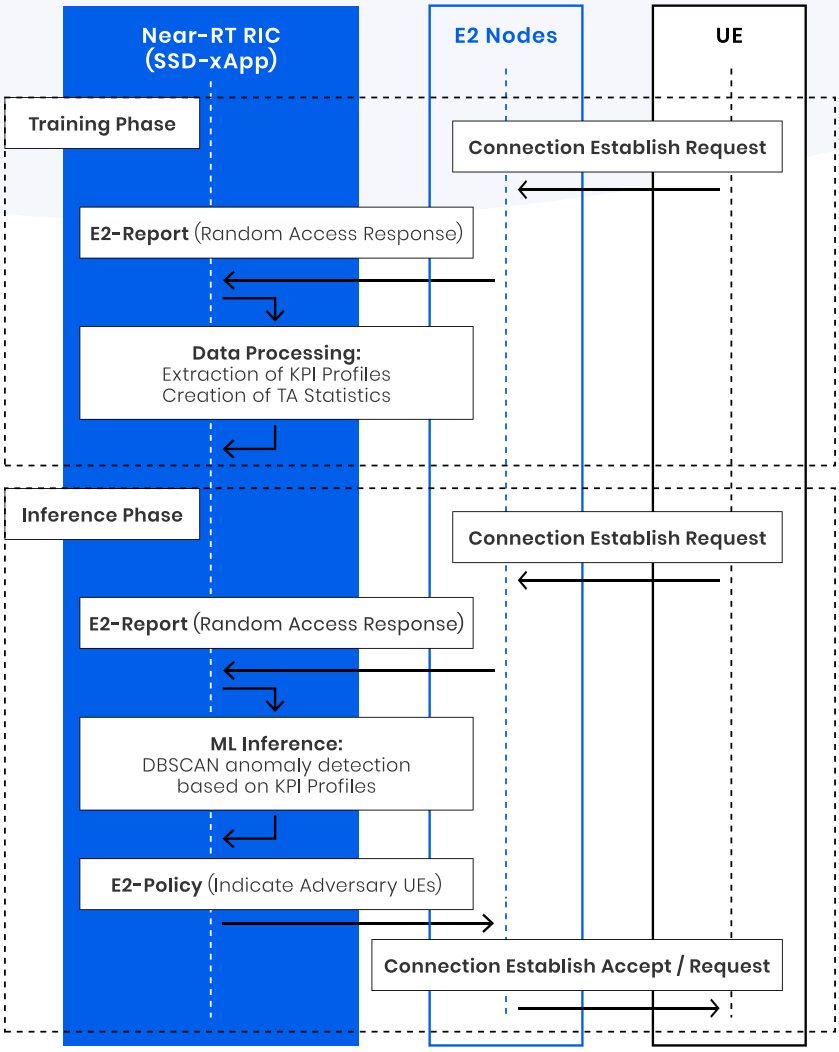


Fig. 4.2-1. UML sequence diagram for signaling storm detection and mitigation (Signaling Storm Detection xApp, SSD-xApp).

In our work [33], we tested the xApp through the computer simulations within the use case that exploits a single cell of a 2 Km radius, 100 legitimate IIoT devices, and three adversaries. Results presented in Fig. 4.2-2 show that our algorithm achieves the probability of attackers' detection above 80% for all anomaly thresholds. However, one should notice that the probability of false alarms strongly depends on the selected threshold. From the perspective of MNO, it is often acceptable to sacrifice detection probability to avoid unnecessary alarms. Thus, the threshold of about 6.5 seems to be a reasonable choice that provides the probability of detection at the level of about 92% and a low probability of false alarm, i.e., 1.5%.

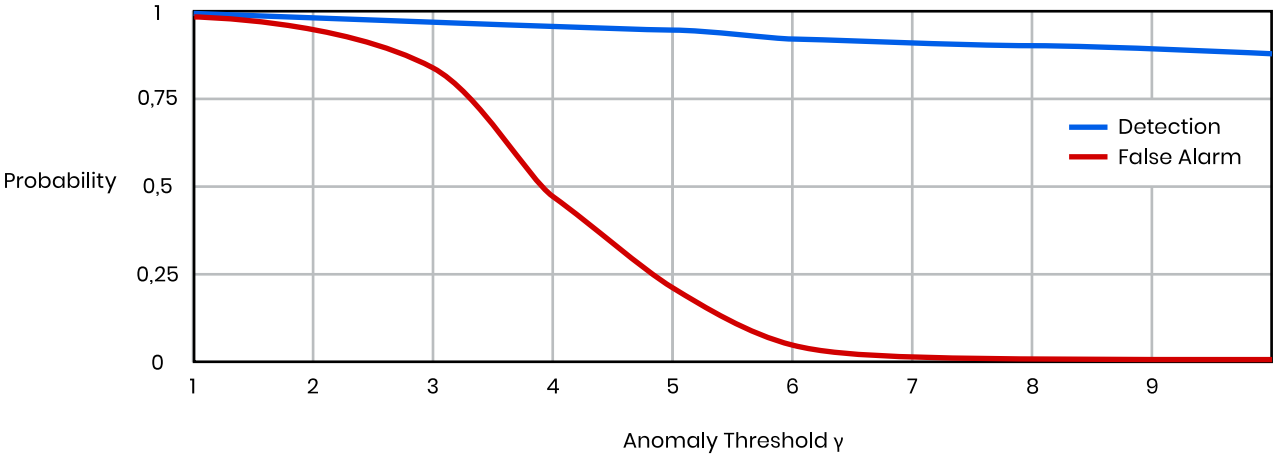


Fig. 4.2-2. Probabilities of signaling storm attack detection and false alarm for the proposed xApp as a function of threshold parameter γ

Summary & Conclusions

Security is one of the key aspects within Open RAN currently in the industry's and research activities' agenda. The Open RAN MoU Progress Update on Maturity, Security, and Energy Efficiency issued in February 2023 indicated the importance of solving the critical issues for further O-RAN development: security and energy efficiency.

As discussed in Chapter 1.0, the O-RAN ALLIANCE WG11 is continuously updating its specifications, while key organizations (like IEEE) and players in the telecommunication business are looking at solutions to address O-RAN security issues and exploit opportunities provided by O-RAN to increase security in future networks. Governments are issuing policies, recommendations, and statements regarding the security of open, interoperable telecom networks.

The discussion in Chapter 2.0 regarding openness and intelligence as key paradigms of future 5G/6G networks presents them as the source of cybersecurity challenges and opportunities to enhance security. Open and software-based architectures expand the O-RAN attack surface while enabling increased control and monitoring of vulnerabilities. Openness increases competition in the telecommunication industry, allowing security solutions to be implemented with any vendor's equipment. O-RAN embedded AI allows for running xApps in Near-RT RIC, enabling continuous monitoring and analysis of security threats, and detecting them faster.

Chapter 3.0 complements this topic with the application of AI in O-RAN. Apart from "traditional" radio attacks against RANs and against software or service-based architecture, cyberattacks against AI/ML algorithms (e.g., applied for 5G/6G network automation) are also envisioned. Thus, specific defense strategies must be in place and onboard O-RAN platforms and the application of AI/ML for this purpose is promising. Thus, AI appears as both the subject of and the defense against security threats.

Dedicated xApps are under development in Rimedo Labs to protect the network against jamming, DoS attacks, and signaling storms and against poisoning attacks on the applied FL algorithms. Selected xApp examples are discussed in Chapter 4.0, together with their UML sequence diagrams and selected results.

The overall conclusions from this whitepaper are as follows:

- O-RAN security and security offered by O-RAN are crucial topics for further O-RAN development. Best practices for O-RAN security are currently being formalized.
- Openness and intelligence of O-RAN create both challenges and opportunities for network cybersecurity.
- AI-exploiting xApps and rApps are promising solutions to detect and mitigate specific types of threats close to their occurrence.
- Dedicated xApps are under development in Rimedo Labs. Examples are anomaly-detecting and attack-mitigating xApps for jamming, signaling storm, DDoS, and data poisoning.

References

[1] M. Dryjański, Ł. Kułacz, A. Kliks, "Toward Modular and Flexible Open RAN Implementations in 6G Networks: Traffic Steering Use Case and O-RAN xApps". Sensors. 2021; 21(24):8173. https://doi.org/10.3390/s21248173

[2] M. Dryjanski, R. Lundberg, "The O-RAN Whitepaper; Overview, Architecture and Traffic Steering Use Case", 2021, https://www.rimedolabs.com/blog/the-o-ran-whitepaper/

[3] "Open RAN MoU Progress Update on Maturity, Security and Energy Efficiency", February 2023, online: https://www.orange.com/sites/orangecom/files/documents/2023-02/Joint%20MoU% 20White%20Paper%20for%20MWC%202023%20FINAL%20%5Bdigital%5D.pdf

[4] O-RAN ALLIANCE Security Work Group WG11 Specifications, online: https://orandownloadsweb.azurewebsites.net/specifications

[5] Mavenir whitepaper on "Open architecture and supply chain diversity: securing telecoms into the future", January 2023, https://www.mavenir.com/resources/open-architecture-supply-chain-diversity-securing-telecoms-into-the-future/

[6] Euractive podcast, The Tech Brief, Episode 121, "Open RAN: European and American views" https://www.euractiv.com/section/digital/podcast/open-ran-european-and-american-views/

[7] Rakuten Symphony, "The Definitive Guide to Open RAN Security." October 2022 https://assets.website-files.com/6317e170a9eabbe0fbbf4519/63582c8cec69a24b2bcde588_221025-Security-Handbook.pdf

[8] https://www.nec.xon.co.za/open-ran-best-practice-security-tests-are-now-available/

[9] G. Horn, Soo Bum Lee, "Toward enabling secure 5G networks with O-RAN", https://www.qualcomm.com/news/onq/2022/04/toward-enabling-secure-5g-networks-o-ran

[10] S. Poretsky, J. Jardal, "Why SMO provides an ideal platform for intelligent Open RAN security", online: https://www.ericsson.com/en/blog/2022/6/why-smo-provides-an-ideal-platform-for-intelligent-open-ran-security

[11] UK Government, Policy paper, "Open RAN principles", 29th of April, 2022, https://www.gov.uk/government/publications/uk-open-ran-principles/open-ran-principles

[12] https://www.ntia.doc.gov/files/ntia/publications/us-australia_joint_statement_9-14-22.pdf

[13] National Security Agency and Cybersecurity and Infrastructure Security Agency (USA) "Open Radio Access Network Security Considerations", September 15th, 2022, https://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf

[14] Joint statement between the United States of America, Australia, Canada and the United Kingdom on Telecommunications Supplier Diversity, December 8th, 2022, https://www.ntia.gov/press-release/2022/joint-statement-between-united-states-america-australia-canada-and-united

[15] https://futurenetworks.ieee.org/images/files//pdf/Webinars/FNI-Webinar-Combined-slides-20220316_v02.pdf

[16] M. Liyanagea, A. Braekenb, S. Shahabuddinc, P. Ranaweerad, "Open RAN Security: Challenges and Opportunities", arXiv:2212.01510v1 [cs.CR] 3 Dec 2022

[17] https://rimedolabs.com/blog/ai-for-oran-security/

[18] M. Wasilewska, H. Bogucka, H. V. Poor, "Secure Federated Learning for Cognitive Radio Sensing", IEEE Communications Magazine, Vol. 61, no. 3, March 2023, pp. 68 – 73

[19] ETSI, „GS MEC 003 V2.2.1: Multi-access Edge Computing (MEC): Framework and Reference Architecture," Group Specification, ETSI, 12.2020.

[20] https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

[21] "Open RAN Security White Paper, Under the Open RAN MoU", by Deutsche Telekom, Orange, Telefónica, TIM, and Vodafone, https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/623adef-88d4ea05aae841f40/1648025338041/Open+RAN+MoU+Security+White+Paper+–+FV.pdf

[22] ISO 27005: https://www.iso.org/standard/75281.html

[23] Rose, S., Borchert, O., Mitchell, S., and Connelly, S., NIST SP 800-207: "Zero-Trust Architecture", U.S. NIST, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

[24] J. Cao et al., „A Survey on Security Aspects for 3GPP 5G Networks," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 170-195, Firstquarter 2020

[25] C. Benzaïd, T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?." IEEE Network, vol. 34, no. 6, Nov./Dec. 2020, pp. 140-147

[26] C.T. Shen et.al., "Security Threat Analysis and Treatment Strategy for ORAN", International Conference on Advanced Communications Technology, ICACT2022 Feb. 13-16, 2022, pp.417-422

[27] V. Marojevic, R. M. Rao, S. Ha, and J. H. Reed, „Performance Analysis of a Mission-Critical Portable LTE System in Targeted RF Interference," 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), 2017, pp. 1-6

[28] L. Bodrog, M. Kajo, S. Kocsis and B. Schultz, „A robust algorithm for anomaly detection in mobile networks," 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, 2016, pp. 1-6

[29] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," IEEE Secur. Privacy Workshops, May 2018, pp. 29– 35

[30] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 1, pp. 2–14, 2018.

[31] M. Wasilewska, H. Bogucka, A. Kliks, "Federated Learning for 5G Radio Spectrum Sensing", Sensors, 2022, 22(1), 198, pp. 1-15

[32] P. Kryszkiewicz, M. Hoffmann, "Open RAN for detection of a jamming attack in a 5G network", IEEE 97th Vehicular Technology Conference (VTC2022-Spring).

[33] M. Hoffmann, and P. Kryszkiewicz. "Signaling Storm Detection in IIoT Network based on the Open RAN Architecture.", IEEE International Conference on Computer Communications INFOCOM 2023, 17–20 May 2023, New York, USA 2023, arXiv e-prints: arXiv-2302

Glossary

5G	The 5th Generation of Mobile Networks
6G	The 6th Generation of Mobile Networks
AI	Artificial Intelligence
API	Application Programming Interface
CISA	Cybersecurity and Infrastructure Security Agency
CNN	Convolutional Neural Networks
CQI	Channel Quality Indicator
DBSCAN	Density-Based Spatial Clustering of Applications with Noise
DDoS	Distributed DoS
DoS	Denial of Service
FL	Federated Learning
gNB	gNodeB
GSMA	Groupe Speciale Mobile Association
IEEE	Institute of Electrical and Electronic Engineers
IoT	Internet of Things
k-NN	k-nearest neighbors
KPI	Key Performance Indicator
MCS	Modulation and Coding Scheme
MEC	Multi-Access Edge Computing
MITM	Man in the Middle
ML	Machine Learning
MNO	Mobile Network Operator
MoU	Memorandum of Understanding
Near-RT RIC	Near-Real Time RIC
NN	Neural Networks
Non-RT RIC	Non-Real Time RIC

NSA	National Security Agency
NSA	Non Standalone
NTIA	National Telecommunications and Information Administration
O-RAN	Open RAN (by O-RAN ALLIANCE)
O-RU	O-RAN Radio Unit
PUE	Primary User Emulation
QoS	Quality of Service
RACH	Random Access Channel
RAN	Radio Access Network
rApp	Application to run on Non-RT RIC
RIC	RAN Intelligent Controller
RL	Reinforcement Learning
RSRP	Reference Signal Receive Power
SA	Standalone
SBA	Service Based Architecture
SFG	Security Focus Group
SMO	Service Management and Orchestration
SS	Signaling Storm
TA	Timing Advance
TIP	Telecom Infra Project
UE	User Equipment
UML	Unified Modeling Language
URLLC	Ultra Reliable and Low Latency Communications
V-RAN	Virtualized RAN
xApp	Application to run on Near-RT RIC

About the Authors

Prof. Hanna Bogucka, Ph.D.

Head of Cooperation / Board Member

Prof. Hanna Bogucka received her Ph.D. with honors in 1995 and Doctor Habilitus Telecommunications in 2006 from Poznan University of Technology (PUT). Currently, she is a full professor and the Director of the Institute of Radiocommunications at PUT. Moreover, prof. Bogucka is the co-founder, Board Member, and the Head of Cooperation of Rimedo Labs, a spin-off from PUT. Prof. Bogucka is involved in research in the area of wireless communications: radio resource management, cognitive radio, and green communication. She has been involved in multiple European 5th – 7th Framework Programme and Horizon 2020 projects, European COST actions, National Science Centre projects, and industry cooperation. Prof. Bogucka is the author of 200 research papers, 3 handbooks on radio communications and digital signal processing, and 3 scientific monographs on flexible and cognitive radio. Prof. Bogucka has been appointed IEEE Communications Society Director of the EAME Region and elected IEEE Radio Communications Committee Chair for the term of 2015-2016. Currently, she is the IEEE ComSoc Fog/Edge Industry Community Regional Chair in Europe, elected Member at Large of the IEEE ComSoc Board of Governors representing the EMEA region (2023-2025), and a member of the Polish Academy of Sciences.

Pawel Kryszkiewicz, Ph.D.

Technical Director

Pawel Kryszkiewicz received his Ph.D. (with distinction) and and Doctor Habilitus in the field of technical sciences, the telecommunications discipline at the Poznan University of Technology in 2015 and 2022, respectivelly. Since October 2010 he has been working at the Poznan University of Technology, currently at the Institute of Radiocommunications as an associate professor. He was involved in a number of national and international research projects. His main research interests include multicarrier system design, green communications, dynamic spectrum access, O-RAN security and massive MIMO systems.

Marcin Hoffmann

Senior R&D Engineer

Marcin Hoffmann is a Senior R&D engineer at Rimedo Labs working on O-RAN software development solutions and spectrum sharing-related projects. Marcin is a Graduate Student Member, at IEEE and received the M.Sc. degree (Hons.) in electronics and telecommunication from Poznań University of Technology, in 2019, where he is currently pursuing a Ph.D. degree with the Institute of Radiocommunications. He is gaining scientific experience by being involved in both national and international research projects. His research interests include the utilization of machine learning and location-dependent information for the purpose of network management. In addition to that Marcin works on massive MIMO and advanced beamforming techniques. His scientific articles are published in top journals like IEEE Transactions on Intelligent Transportation Systems or IEEE Access.

Małgorzata Wasilewska

R&D Engineer

Małgorzata Wasilewska is an R&D engineer at Rimedo Labs working on O-RAN security, and AI-security related projects. Małgorzata received the M.Sc. degree in electronics and telecommunication from Poznań University of Technology, where she is currently pursuing a Ph.D. degree with the Institute of Radiocommunications. Her main fields of interest are spectrum sensing, security in wireless networks, artificial intelligence algorithms design, and distributed learning. She is the author of 10 papers. His scientific articles are published in top journals like IEEE Communications Magazine, IEEE Access or IEEE Wireless Communications Letters.

About Rimedo Labs

Rimedo Labs specializes in providing high-quality consulting, implementation, and R&D services in the field of modern wireless systems currently focusing on Open RAN, 5G, and beyond. Rimedo Labs is an O-RAN software provider delivering customized xApps and rApps for RAN Intelligent Controllers.

To read more about us, see:
www.rimedolabs.com/about/

To learn more about our O-RAN services, see:
www.rimedolabs.com/o-ran/

Rimedo Labs successfully took part in the **O-RAN Global Plugfest Fall 2022** and **Spring 2023** hosted by **i14y Lab and EANTC in Berlin.**

Rimedo Labs is a proud member of **ONF**, **O-RAN ALLIANCE**, and **VMware TAP**.

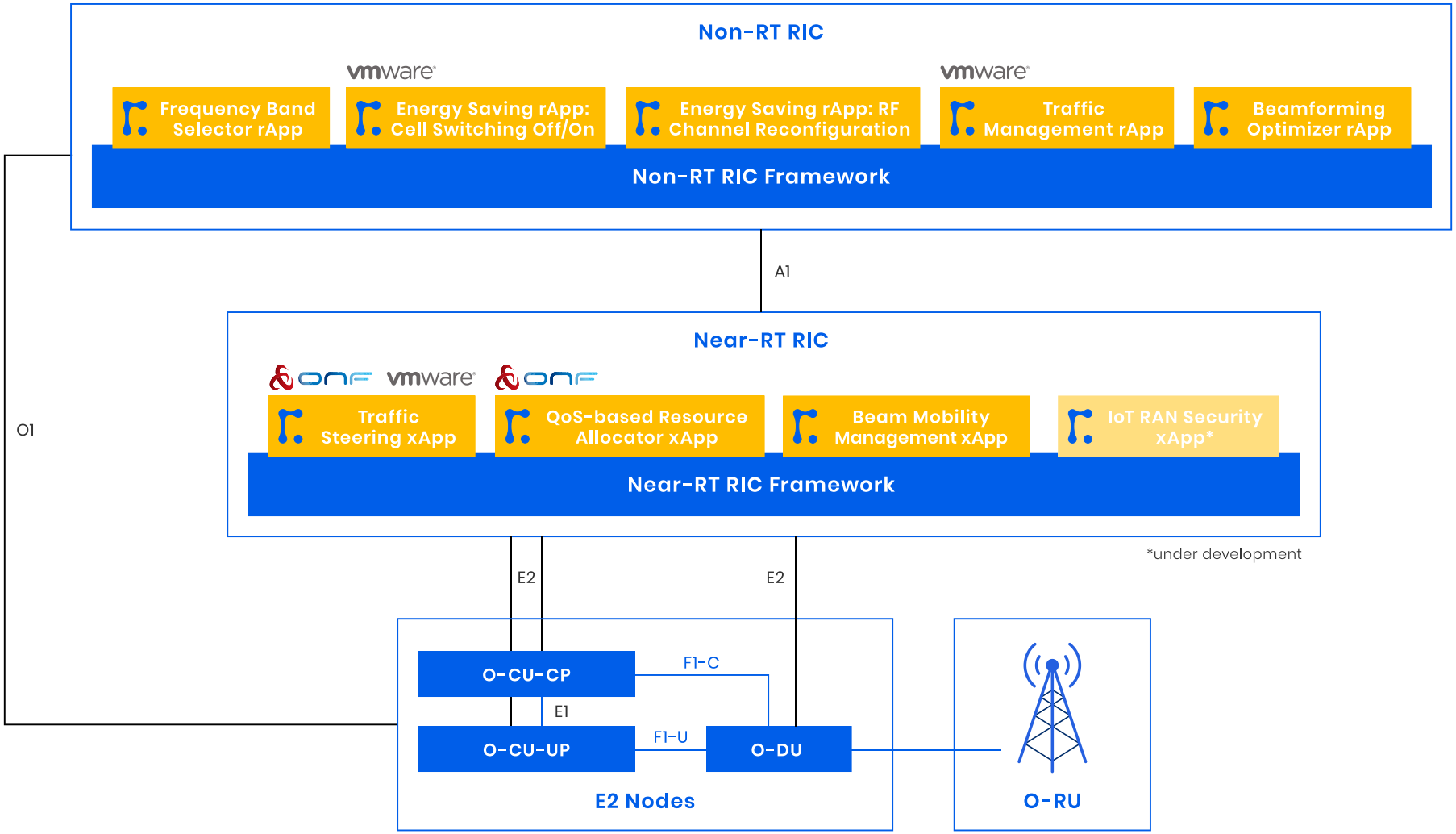
Rimedo Labs & 5G Security

Rimedo Labs participates in the 5gSTAR project on *"Advanced methods and techniques for identification and counteracting cyber-attacks on 5G access network and applications"*. The project is funded within the 4th CyberSecIdent program – Cybersecurity and e-Identity by the Polish National Centre for Research and Development (NCBIR) from 2021 to 2024. We believe that the openness and intelligence of RAN create opportunities for the secure operation of future networks.

You can find more about the 5gSTAR project on this website:
5gstar.pl

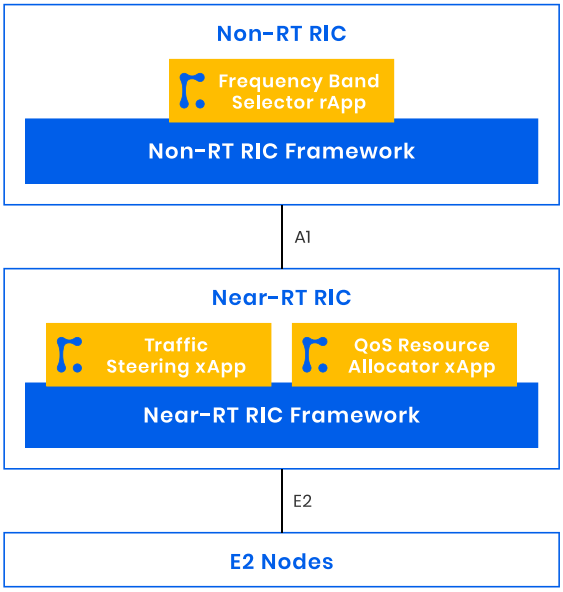
You can find more details about the 5gSTAR project and our work in the 5G/6G security area in this **blog post**

Rimedo Labs xApp/rApp Portfolio



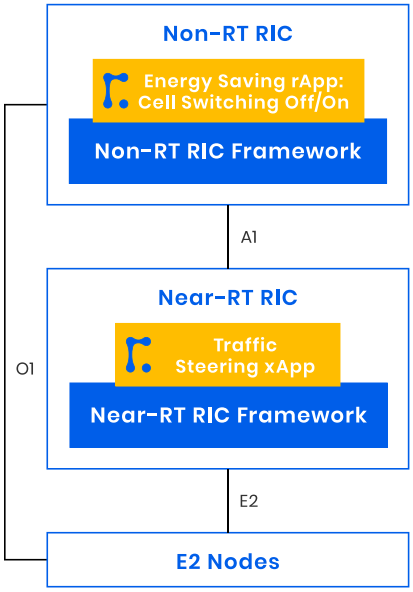
Example use cases addressed by Rimedo Labs RIC applications

Joint optimization of the radio resources



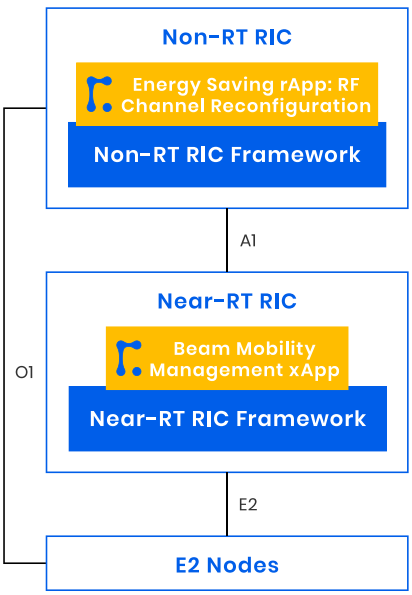
Advanced Traffic Steering operation, with joint optimization of the radio resource utilization. The combined operation of FBS-rApp, TS-xApp, and QRA-xApp.

Energy saving for HetNet



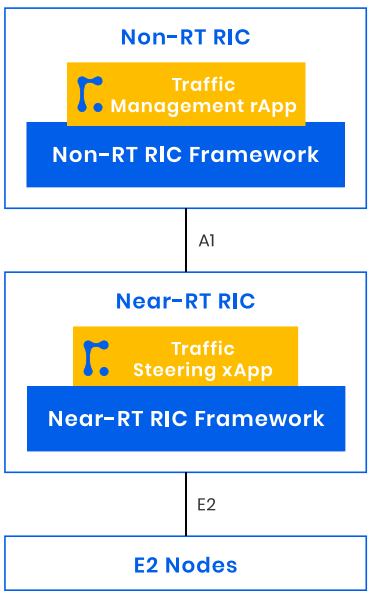
ES-rApp working in cooperation with TS-xApp through adjustment of TS policies. ES-rApp decides on cell on/off for the capacity-small-cell layer.

Energy saving for Massive MIMO



ES-rApp decides on the antenna panel configuration and updates the BMM-xApp with the configuration and REM.

Traffic Management for V2X scenarios



TM-rApp utilizes the enrichment information to derive policies for TS-xApp for advanced V2X scenarios (e.g. emergency, car platoon).

RIMEDO LABS

Let's keep in touch!

info@rimedolabs.com
+48 (61) 665 38 17

RIMEDO sp. z o.o.
ul. Polanka 3
61-131 Poznan
Poland, EU

www.rimedolabs.com