Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2024.052394

REVIEW

# An Investigation on Open-RAN Specifications: Use Cases, Security Threats, Requirements, Discussions

**Heejae Park[1], Tri-Hai Nguyen[2] and Laihyuk Park[1,*]**

[1]Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, 01811, Republic of Korea

[2]Faculty of Information Technology, School of Technology, Van Lang University, Ho Chi Minh City, 70000, Vietnam

*Corresponding Author: Laihyuk Park. Email: lhpark@seoultech.ac.kr

Received: 31 March 2024 Accepted: 31 May 2024 Published: 20 August 2024

**ABSTRACT**

The emergence of various technologies such as terahertz communications, Reconfigurable Intelligent Surfaces (RIS), and AI-powered communication services will burden network operators with rising infrastructure costs. Recently, the Open Radio Access Network (O-RAN) has been introduced as a solution for growing financial and operational burdens in Beyond 5G (B5G) and 6G networks. O-RAN promotes openness and intelligence to overcome the limitations of traditional RANs. By disaggregating conventional Base Band Units (BBUs) into O-RAN Distributed Units (O-DU) and O-RAN Centralized Units (O-CU), O-RAN offers greater flexibility for upgrades and network automation. However, this openness introduces new security challenges compared to traditional RANs. Many existing studies overlook these security requirements of the O-RAN networks. To gain deeper insights into the O-RAN system and security, this paper first provides an overview of the general O-RAN architecture and its diverse use cases relevant to B5G and 6G applications. We then delve into specifications of O-RAN security threats and requirements, aiming to mitigate security vulnerabilities effectively. By providing a comprehensive understanding of O-RAN architecture, use cases, and security considerations, this work serves as a valuable resource for future research in O-RAN and its security.

**KEYWORDS**

O-RAN; architecture; use cases; security issues; security requirements; security discussions

## 1 Introduction

With next-generation wireless systems built on a variety of heterogeneous technologies such as terahertz communications, Reconfigurable Intelligent Surface (RIS), and AI-based communications (e.g., Machine Learning (ML) and Deep Learning (DL)), cellular networks are becoming more complex [1–3]. This will increase operational costs and capital for the network operators since operators need to consistently perform upgrading and maintaining their infrastructure. As a result, network operators will face growing financial and operational burdens, necessitating ongoing investments in infrastructure upgrades and maintenance to stay aligned with evolving market trends, technological

advancements, and customer demands. To meet the aforementioned requirements, Open Radio Access Networks (O-RAN) has emerged as a solution [4,5].

O-RAN has been considered one of the most promising technologies for Beyond 5G (B5G) and 6G systems. Unlike conventional RAN systems, which are far from open, O-RAN advocates for openness and intelligence to address the limitations of existing RAN networks [6,7]. O-RAN deployments rely on a framework of disaggregated and software-based components, all interconnected via open interfaces. The process of disaggregation and virtualization empowers flexible deployments and enhances the network's resilience and reconfigurability [8].

Fig. 1 shows the comparison of O-RAN and traditional RAN architecture. In the O-RAN system, the traditional Based Band Unit (BBU) is split into a Distributed Unit (DU) and a Centralized Unit (CU). O-RAN architecture consists of multiple components, i.e., Radio Unit (RU), DU, CU, and RAN Intelligence Controller (RIC) [9]. RU, DU, and CU are called O-RAN Radio Unit (O-RU), O-RAN Distributed Unit (O-DU), and O-RAN Centralized Unit (O-CU) in O-RAN specifications [10]. The benefits of using O-RAN architecture are listed as follows: (1) The unification of the software-enabled architecture makes the network more suitable for future communication, (2) Splitting BBU into DUs and CUs makes the deployment flexible for updates and installation, (3) The plug-and-play feature of O-RAN, coupled with various promising techniques, is anticipated to lower maintenance costs, (4) It is possible to establish a higher level of automation within the network, (5) Open and interoperable interfaces enable operators to integrate network equipment from various vendors, thereby expanding the RAN ecosystem to include smaller vendors [8,11–13].

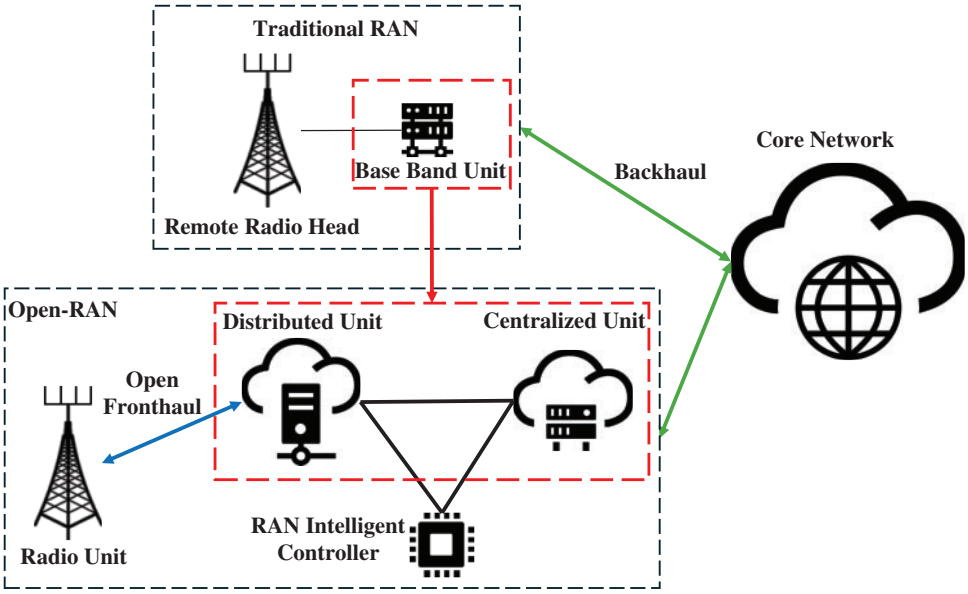


**Figure 1:** Comparison of O-RAN architecture with traditional RAN

To maximize the advantages of O-RAN, this paper investigates the diverse array of use cases specified by the O-RAN Alliance, exploring their backgrounds, goals, and entities that consist of the use case. By elucidating these use cases, we aim to provide valuable insights into the transformative potential of O-RAN technology and its role in shaping the future mobile internet.

This paper investigated several previous studies that operate the optimization process in the O-RAN system. A summary of recent studies related to O-RAN is shown in Table 1. Authors in [14]

proposed an O-RANFed framework for implementing and optimizing federated learning on O-RAN devices to facilitate 5G network slicing. They handle the non-convex formulated problem by successive convex approximation (SCA). Authors in [15] introduced a hierarchical RAN slicing framework that utilizes Deep Reinforcement Learning (DRL) for resource allocation. This framework operates on two slices: communication and computation slices. The first slice focuses on assigning network resources to the user, while the second slice manages allocating computational resources for those devices. Authors in [16] designed a federated DRL framework to manage the interplay between multiple Extended Applications (xApps) within the O-RAN architecture for network slicing. This framework focuses on two key xAPPs: power and resource allocation for network slices. By employing a model generated by federated learning to accommodate these xApps, the approach aims to improve training efficiency and achieve better system performance. Authors in [17] formulated the problem of jointly optimizing wireless link scheduling, service-to-slice mapping, and physical data center resource allocation for network slices. The goal is to solve a mixed-integer optimization problem, prioritizing maximizing energy efficiency while minimizing both power consumption and physical resource costs. The authors decomposed the optimization problem, solving each subproblem with heuristic algorithms.

**Table 1:** Summary of prior research on O-RAN applications

| Application | Reference | Description |
|---|---|---|
| Network slicing | [14] | Proposed an O-RANFed, for implementing federated learning model on devices within O-RAN to facilitate 5G network slicing |
| | [15] | Introduced a hierarchical RAN slicing framework that utilizes DRL for resource allocation |
| | [16] | Designed a federated DRL framework to manage the interplay between multiple xAPPs within the O-RAN architecture for network slicing |
| | [17] | formulated the problem of jointly optimizing wireless link scheduling, service-to-slice mapping, and physical data center resource allocation for network slices |
| Resource allocation | [18] | Proposed a RL-based resource management method that optimizes service latency |
| | [19] | Designed a two-stage resource management algorithm |
| | [20] | Formulated CNF deployment and resource management problem |
| | [21] | Proposed a DRL approach that utilizes a self-play mechanism to handle the problem of assigning resources between RUs and DUs |
| | [22] | Introduced SAS method which is aimed at providing user services |
| Scheduling | [23] | Modeled connection scheduling as a graph optimization problem and proposed a DRL-based solution that leverages GNN |
| | [24] | Proposed a team learning algorithm to facilitate improved coordination between xApps within the network |

(Continued)

**Table 1 (continued)**

| Application | Reference | Description |
|---|---|---|
| | [25] | Proposed a SA2C-EADDUS which integrates two actor-critic agents |
| Traffic steering | [26] | Proposed a novel traffic steering xApp that leverages DRL for optimal user-level mobility control |
| | [27] | Designed a JIFDR framework to address scenarios with unknown and dynamic traffic demands |
| | [28] | Proposed the method for radio access technology (RAT) allocation that leverages federated meta-learning |
| | [29] | Leveraged SCA method to optimize throughput and latency |

Authors in [18] formulated the resource management problem considering communication, computation, and cache model. To address service latency arising from Near-RT RIC and non-RT RIC interactions, the authors recast the optimization problem as a Markov decision process (MDP) and proposed a reinforcement learning (RL)-based resource allocation scheme that minimizes this latency. Authors in [19] designed a two-stage resource allocation scheme. The formulated problem is simplified and reformulated in the first step. It aims to establish both lower/upper limits of the number of activated Virtual Network Functions (VNFs). They leveraged the Karush-Kuhn-Tucker (KKT) conditions and Lagrangian function to determine the optimal allocation of transmit power and Physical Resource Blocks (PRBs). In the second stage, the O-RU association problem is transformed into a knapsack problem, efficiently solved using a greedy algorithm. Authors in [20] formulated a Cloud Network Function (CNF) deployment and resource management problem within an O-RAN enabled LTE/5G network through a mathematical model. This model prioritizes minimizing end-to-end data plane delays. To achieve an efficient solution, the authors propose a gradient-based approach. Authors in [21] modeled the problem of assigning resources between O-RUs and O-DUs as a bin-packing problem. They proposed a DRL approach that utilizes a self-play mechanism to achieve efficient resource management. Authors in [22] introduced the Service Allocation Scheduling (SAS) method aimed at providing user services. The authors formulated several objectives with multiple constraint problems to enhance service level guarantees for users. A graph-based approach is proposed to achieve optimal service allocation, maximizing the network capacity.

Authors in [23] modeled connection scheduling as a graph optimization problem. To achieve optimal user-cell association, they proposed a DRL-based solution that leverages the graph structure to train Graph Neural Network (GNN). This approach considers three key objectives: maximizing throughput, ensuring network coverage, and balancing the network load/traffic. Authors in [24] addressed the challenge of managing conflicts between different xApps. They presented a team learning-based method to facilitate improved coordination between xApps within the network, ultimately enhancing overall performance. Authors in [25] proposed a SA2C-EADDUS (Soft Actor-Critic Energy-Aware Dynamic DU Selection) method. The proposed algorithm utilizes two A2C agents. The first prioritizes radio RB allocation to the user based on packet type and priority. The second agent focuses on network Energy Consumption (EC) by optimizing power, resource capacity, and propagation delay across the O-DUs.

Authors in [26] proposed a novel traffic steering xApp that leverages DRL for optimal user-level mobility control. Proposed techniques enable the xApp to choose the optimal cell for each user. Authors in [27] designed a JIFDR framework (Joint Intelligent Traffic Prediction, Flow-Split Distribution, Dynamic User Association, and Radio Resource Management) to address scenarios with unknown and dynamic traffic demands. This framework tackles the complex optimization problem by decomposing it into long-term subproblems and short-term subproblems. The solution to the short-term problem relies on the solution for the long-term subproblem. To address this dependency, the authors leverage LSTM (Long Short-Term Memory) to efficiently handle the long-term problem, informing the short-term solution. Authors in [28] proposed a radio access technology (RAT) allocation method that leverages federated meta-learning. This approach empowers RICs to adapt more swiftly to dynamic environmental changes. Authors in [29] formulated the problem that achieves two key objectives: maximizing the weighted sum of enhanced Mobile Broadband (eMBB) throughput and minimizing the worst-user Ultra-Reliable Low-Latency Communication (URLLC) latency. This problem considers Quality-of-Service (QoS) requirements, orthogonality constraints, power limitations, and limited fronthaul capacity. The authors leveraged the SCA method to solve the formulated mixed integer nonlinear problem.

However, the above works do not consider the security requirements of the O-RAN system. Moreover, since O-RAN architecture differs significantly from traditional RAN setups, it inherently introduces new security challenges. Therefore, this paper investigates the specifications of O-RAN security threats and security requirements and discusses O-RAN security, aiming to address and mitigate the challenges effectively. Through these insights, we aim to establish a comprehensive guideline that not only addresses current security concerns but also anticipates and prepares for the evolving landscape of future mobile internet technologies. The main contributions are summarized as follows:

- This paper provides an overview of general O-RAN architecture and use case specifications that can be applied or extended in future B5G and 6G.
- This paper aims to create a comprehensive guideline for future work by providing O-RAN security threats, requirements, and discussions.

The rest of this paper is organized as follows. Section 2 provides brief overview on O-RAN architecture. Section 3 provides use cases of O-RAN. Then, Section 4 presents O-RAN security threats against O-RAN components. Security requirements of O-RAN components are described in Section 5, and Section 6 provides discussions on O-RAN security. The conclusion is shown in Section 7.

## 2 Architecture of O-RAN

Fig. 2 shows the high-level architecture of O-RAN. The main components of the O-RAN system include O-Cloud, RIC, O-CU, O-DU, and O-RU, R1, A1, O1, O2, E2, and O-RAN Fronthaul (O-FH), and Service Management and Orchestration (SMO).

### *2.1 O-Cloud*

O-Cloud is a cloud computing platform comprising O-RAN functions and physical infrastructure. It focuses on creating an open and standardized cloud-native infrastructure for deploying and managing VNFs and CNFs. O-Cloud enables greater flexibility, scalability, and efficiency in deploying and managing network services by leveraging cloud computing principles.

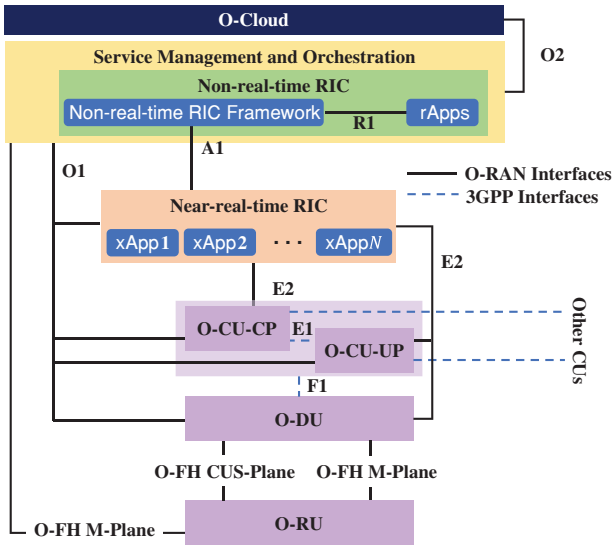


**Figure 2:** High-level architecture of O-RAN

### *2.2 RIC*

RIC is a key element that executes resource allocation by leveraging data gathered from both the network and end users. RIC is split into Non-Real-Time RIC (Non-RT RIC) and Near-Real-Time (Near-RT RIC).

- **Non-RT RIC:** Non-RT RIC is integrated within SMO. It is specifically designed to optimize and manage RAN resources and AI/ML workflows that do not necessitate immediate, real-time responsiveness. Non-RT RIC also supports the execution of the Non-RT RIC Applications (rApps) [8].
- **Near-RT RIC:** Residing at the network edge or regional clouds, the Near-RT RIC leverages the E2 interface for data collection. This data is used for optimization and control of RAN resources. Near-RT RIC also supports xApps.

### *2.3 O-CU*

O-RAN splits O-CU into two parts, i.e., O-CU Control Plane (CP) and O-CU User Plane (UP). While O-CU-CP hosts the Radio Resource Control (RRC) layer and the CP part of the Packet Data Convergence Protocol (PDCP) protocol, O-CU-UP hosts the UP part of the PDCP protocol and the Service Data Adaptation Protocol (SDAP) protocol [8,30].

### *2.4 O-DU*

O-DU is typically physically positioned in proximity to the RU and hosts Radio Link Control (RLC) layer, Medium Access Control (MAC) layer, and high physical layers.

### *2.5 O-RU*

O-RU, which has a physical layer, is equipped with antennas and is responsible for processing signals such as transmitting, receiving, digitizing, and amplifying [9]. O-RU is connected to the SMO through the O-FH M-plane and users through radio interfaces.

### *2.6 R1*

rApps utilize the R1 interface to access Non-RT RIC framework [31]. It provides policy-based guidance, data analysis results, AI/ML-based models, and data for optimization.

### *2.7 A1*

A1 interface acts as a bridge for communication between the Non-RT RIC and Near-RT RIC, facilitating AI/ML workflow and the data transmission from both internal and external O-RAN sources to the SMO framework.

### *2.8 O1*

O1 interface connects the SMO to all O-RAN components, facilitating management for Fault, Configuration, Accounting, Performance, Security (FCAPS), software, and files.

### *2.9 O2*

O2 connects SMO and O-Cloud to support additional computation. The goal of the O2 interface is to guarantee reliable communication between the SMO and the O-Cloud.

### *2.10 E2*

E2 connects Near-RT RIC and the E2 Nodes, i.e., O-DUs, O-CU-CPs, O-CU-UPs [32]. The objective of the E2 interface is to enhance the performance of E2 nodes and their resource consumption.

### *2.11 O-FH*

O-FH includes the O-FH Management plane (O-FH M-Plane) and O-FH UP, CP, Synchronization Plane (O-FH CUS-Plane) [33].

- **O-FH M-Plane:** O-FH M-Plane enables the management of O-RU resources, encompassing tasks such as signal maintenance and monitoring. This interface serves two key functions: performance reporting and initialization/configuration of operating parameters [31].
- **O-FH CUS-Plane:** O-FH CUS-Plane transmits control signals and user data and achieves synchronization between multiple equipment.

### *2.12 SMO*

SMO, which manages the RAN domain and oversees the network function's lifecycle management, is a main component of the O-RAN architecture. SMO consists of Non-RT RIC and manages Near-RT RIC, O-CU-CP, O-CU-UP, and O-DU through the O1, O-RU through the O-FH M-Plane [34].

## 3 O-RAN Use Cases

In this section, we investigate O-RAN use cases specified in O-RAN Alliance specifications: dynamic handover management for Vehicle-to-Everything (V2X) communication, flight path-based dynamic Unmanned Aerial Vehicles (UAV) radio resource allocation, traffic steering, massive Multiple Input, Multiple Output (MIMO) Grid of Beam (GoB) beamforming optimization, dynamic spectrum sharing, and energy saving [35,36]. These use cases can be applied and extended in B5G and 6G networks.

### *3.1 Dynamic Handover Management for V2X Communication*

#### *3.1.1 Background and Goal of Use Case*

V2X communication offers various potentials such as enhanced road safety, emissions reduction, and time savings [37,38]. However, due to vehicles' high speed and the diverse natural environment, frequent handovers of V2X users can occur, leading to suboptimal handover optimization and anomalies. These inefficient handover operations can significantly degrade the performance of V2X applications. Since the xNBs control handover through the Neighbour Relation Tables (NRTs), there is limited opportunity for user-level customization [35]. This use case enables customizing handover operations based on past navigation and radio data to address problematic handovers for V2X applications. Fig. 3 shows the role of O-RAN components.

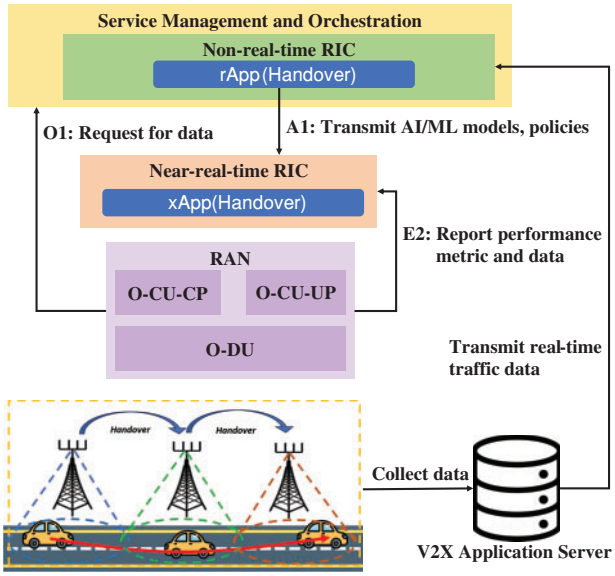


**Figure 3:** Handover management by O-RAN components

#### *3.1.2 Entities Involved in Use Case*

- **Non-RT RIC:** Non-RT RIC collects essential performance, configuration, and other data to train AI/ML models used in the Near-RT RIC. These models are used to identify traffic scenarios and radio conditions. Moreover, Non-RT RIC transmits intents, policies, and non-RAN data to the Near-RT RIC to enhance the performance of decision-making capabilities.
- **Near-RT RIC:** Near-RT RIC updates AI/ML models, interprets intents, and executes policies received from the Non-RT RIC. Additionally, it transmits configuration parameters to RAN.
- **RAN:** RAN collects data gathered by the SMO data collector through the O1 interface and supports near-real-time optimization of handover parameters through the E2 interface. To optimize V2X handovers in real time, the RAN reports essential performance metrics, configuration details, and other relevant data to the Near-RT RIC over the E2 interface.
- **V2X Application Server:** The V2X application server collects data from V2X users and supports the transmission of real-time traffic data to non-RT RIC.

### *3.2 Flight Path-Based Dynamic UAV Radio Resource Allocation*

#### *3.2.1 Background and Goal of Use Case*

The field trial findings indicate that UAVs can offer reliable services to terrestrial users through larger coverage [39]. However, as UAVs fly above, they often fall outside the main lobe of ground station antennas, resulting in scattered cell associations [40,41]. This causes a fragmented cell association pattern, especially at heights exceeding 300 m, posing challenges like signal strength drops and uplink interference. To address these issues and enhance drone mobility and user experience, there is a need for dynamic UAV resource allocation based on the UAV flight paths. Fig. 4 shows the role of O-RAN components in handling dynamic UAV radio resource allocation.

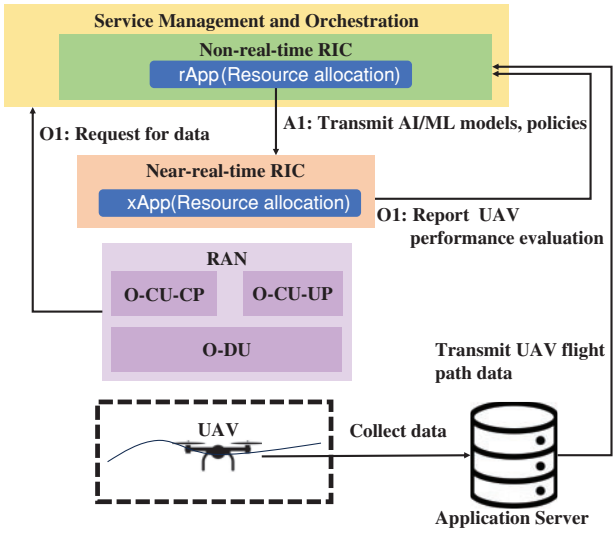


**Figure 4:** Dynamic UAV radio resource allocation by O-RAN components

#### *3.2.2 Entities Involved in Use Case*

- **Non-RT RIC:** Non-RT RIC trains AI/ML models to support UAVs. These models are used to autonomously manage uplink/downlink interference from/to UAVs and predict available radio resources for UAVs. In addition, policies and intents are sent to the Near-RT RIC to support the O-RAN.
- **Near-RT RIC:** Near-RT RIC manages AI/ML models, interprets intents, and executes policies received from the Non-RT RIC to support UAVs. Near-RT RIC leverages AI/ML models to perform on-demand radio resource allocation for UAVs, considering wireless channel conditions, UAV flight paths, and other application-specific information. It also reports UAV performance evaluation to Non-RT RIC.
- **RAN:** RAN collects data about user performance via the O1 interface and optimizes radio resources in non-real-time.
- **Application Server:** The application server provides information about UAVs' past flight path.

### *3.3 Traffic Steering*

#### *3.3.1 Background and Goal of Use Case*

Commercial networks face challenges in managing traffic due to huge traffic and the use of multiple frequency bands. Additionally, multi-access systems require traffic switching based on radio conditions, application needs, and performance demands. Splitting traffic across different frequency bands and access technologies at the same time can be difficult [42,43]. Current Radio Resource Management (RRM) solutions are limited, relying primarily on cell reselection and handover adjustments. They are also cell-centric, making them less adaptable to diverse scenarios. To address these limitations, this use case aims to empower operators with flexible policy configuration and AI/ML models for intelligent and proactive traffic steering. Fig. 5 shows the role of O-RAN components in handling traffic steering optimization.

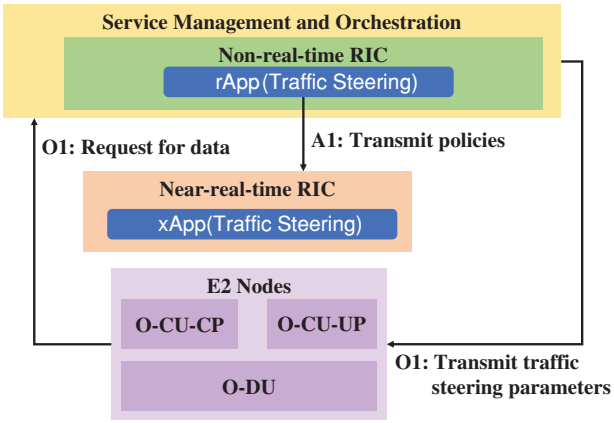


**Figure 5:** Traffic steering optimization by O-RAN components

#### *3.3.2 Entities Involved in Use Case*

- **Non-RT RIC:** Non-RT RIC transmits policies to the Near-RT RIC and parameters for traffic steering to the RAN.
- **Near-RT RIC:** Near-RT RIC interprets the policies from Non-RT RIC.
- **E2 Nodes:** E2 Nodes collect data via the O1 interface.

### *3.4 Massive MIMO GoB Beamforming Optimization*

#### *3.4.1 Background and Goal of Use Case*

Massive MIMO is one of the key technologies for 5G, which leverages its multi-antenna capabilities to provide diversity and improve capacity by directing high-gain beams toward users [44]. It can also improve the received signal power and spatially filter interference. Massive MIMO systems utilize a Grid of Beams (GoB) to facilitate beamforming for control channels during initial access [45]. In order to obtain optimal beamforming and resource allocation, the algorithm has to consider a multi-cell environment instead of a single cell. Additionally, the vast number of adjustable parameters, such as the number of beams, beam widths, azimuth, and elevation range, make it difficult for manual configuration to achieve optimal performance [46,47]. Current solutions struggle with issues such as high interference, unbalanced traffic, and poor performance at cell edges.

This use case proposes a solution that allows operators to configure mMIMO systems more flexibly. This will be achieved through policies and machine learning techniques, enabling operators to define specific objectives and optimize performance accordingly. Fig. 6 shows the role of O-RAN components in optimizing beamforming configuration.

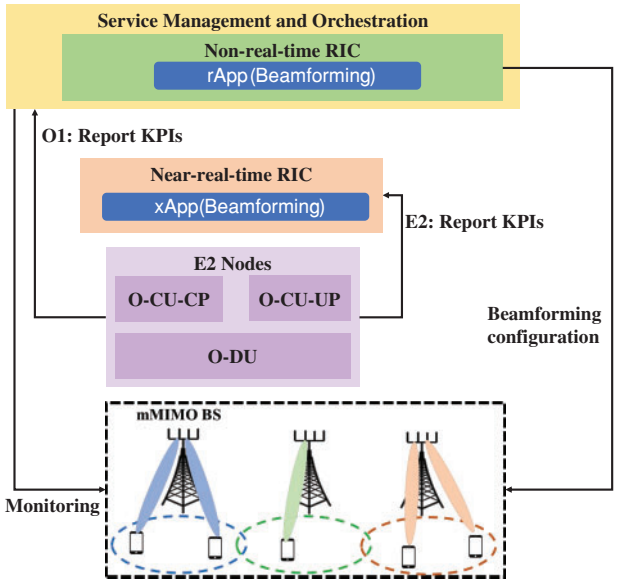


**Figure 6:** Beamforming configuration by O-RAN components

### *3.4.2 Entities Involved in Use Case*

- **Non-RT RIC:** Non-RT RIC gathers data such as user mobility information to train AI/ML models that optimize massive MIMO parameters. Leveraging the trained AI/ML model, the Non-RT RIC infers user and traffic distribution across multiple cells. This information predicts the optimal configuration of massive MIMO parameters, aligning with the operator's global optimization goals.
- **SMO:** SMO continuously monitors cell performance, and if the optimization constraints are not met, a fallback procedure can be initiated. Additionally, the SMO triggers the Non-RT RIC to retrain its AI/ML model, incorporating new data analytics for further optimization.
- **E2 Nodes:** E2 Nodes collect and report key performance indicators (KPIs) to both the SMO and the Near-RT RIC. These KPIs encompass user activity, traffic load, coverage, QoS per beam/area, handover statistics, and beam/resource utilization. Additionally, E2 Nodes apply beam management strategies based on configurations received from the SMO and the Near-RT RIC.

## *3.5 Dynamic Spectrum Sharing*

### *3.5.1 Background and Goal of Use Case*

Spectrum allocation is a crucial aspect of 5G deployment, with operators facing diverse situations [48]. While new C-band (3–6 GHz) and mmWave bands offer high capacity, their coverage suffers due to propagation and penetration limitations. A cost-effective solution is to deploy 5G on existing lower bands (below 2 GHz) also used by 4G LTE. Dynamic Spectrum Sharing (DSS) enables operators

to dynamically share these existing resources between LTE and NR devices, ensuring continued Quality of Experience (QoE) for 4G subscribers while providing necessary coverage and QoS for 5G users [49,50]. This use case aims to suggest DSS within the O-RAN architecture, particularly as an application within the RIC framework. Fig. 7 shows the role of O-RAN components to handle DSS.

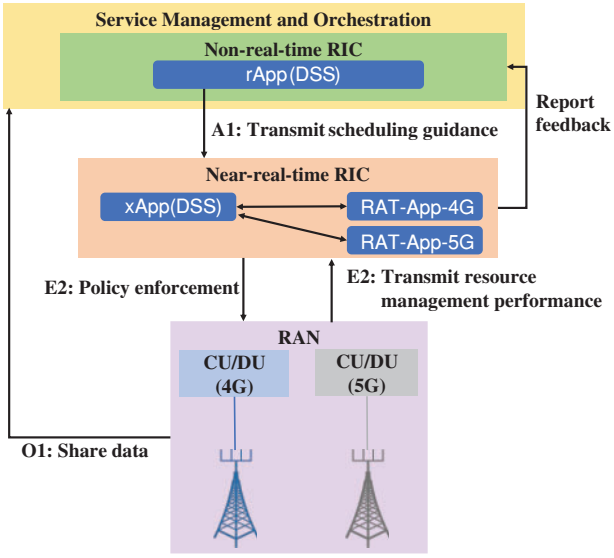


**Figure 7:** Dynamic spectrum sharing by O-RAN components

### *3.5.2 Entities Involved in Use Case*

- **Non-RT RIC:** Non-RT RIC translates SMO's DSS service requirement into resource-sharing policies and provides long-term scheduling guidance for the RAN via A1 to Near-RT RIC. It also trains AI/ML models to predict short-term 4G/5G traffic using near-real-time RAN data. Non-RT RIC uses feedback to update policies and retrain models for continuous optimization.
- **Near-RT RIC:** Near-RT RIC supports deployment, execution, and updates of AI/ML models received from the non-RT RIC. Additionally, the Near-RT RIC interprets operator policies related to resource allocation for specific Radio Access Technologies (RATs) involved in DSS (e.g., LTE and NR). It also shares resource allocation performance and policy feedback reports with the non-RT RIC via the O1/A1 interface.
- **RAN:** RAN shares the data collection via the O1 interface. It also supports the collection of resource management metrics related to DSS and policy enforcement from the Near-RT RIC, both of which utilize the E2 interface.

## *3.6 Local Indoor Positioning in RAN*

### *3.6.1 Background and Goal of Use Case*

The emergence of 5G vertical industries has heightened interest in real-time indoor positioning using cellular networks [51,52]. However, the current approach with a centralized Location Management Function (LMF) can suffer from network delays due to the long message path between the NG-RAN node and LMF. This can lead to inaccurate, non-real-time location results. This use case

proposes enabling local positioning within the O-RAN architecture by leveraging its open interfaces. Fig. 8 shows the role of O-RAN components in handling indoor positioning.

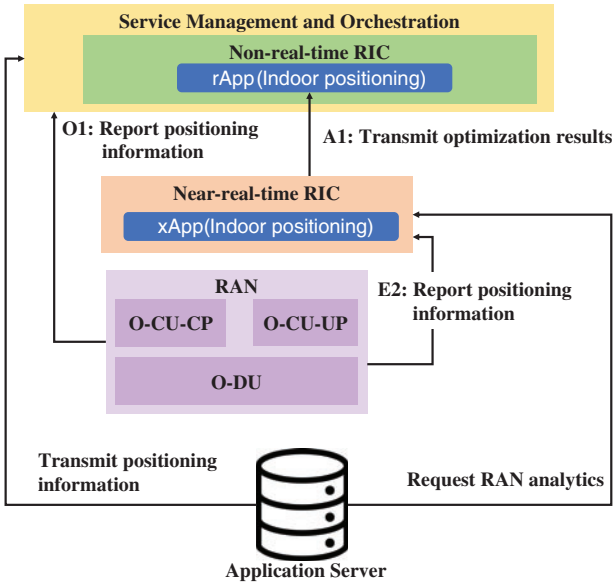


**Figure 8:** Indoor positioning by O-RAN components

### *3.6.2 Entities Involved in Use Case*

- **Non-RT RIC:** Non-RT RIC retrieves RAN data from SMO to train the AI/ML model deployed in Near-RT RIC.
- **Near-RT RIC:** Near-RT RIC computes user location based on RAN measurements and transmits the results to the non-RT RIC for evaluation and optimization.
- **RAN:** RAN reports positioning information over the E2 and O1 interface.
- **Application Server:** The application server requests RAN analytics information from Near-RT RIC and transmits positioning information to SMO.

## *3.7 Energy Saving*

### *3.7.1 Background and Goal of Use Case*

Mobile networks face challenges in managing EC within the RAN [53,54]. Optimizing RAN EC is complex due to varying traffic and user mobility. Reducing network EC can be achieved through improved Energy Efficiency (EE) and the implementation of various Energy Saving (ES) mechanisms [55]. However, existing solutions include sleep modes for base stations, carrier/channel switching, and Advanced Sleep Modes (ASM) for very short time scales. This use case proposes leveraging O-RAN's AI/ML and open interfaces to optimize ES and EE through switching on/off network components at different time scales. Fig. 9 shows the role of O-RAN components in handling indoor positioning.

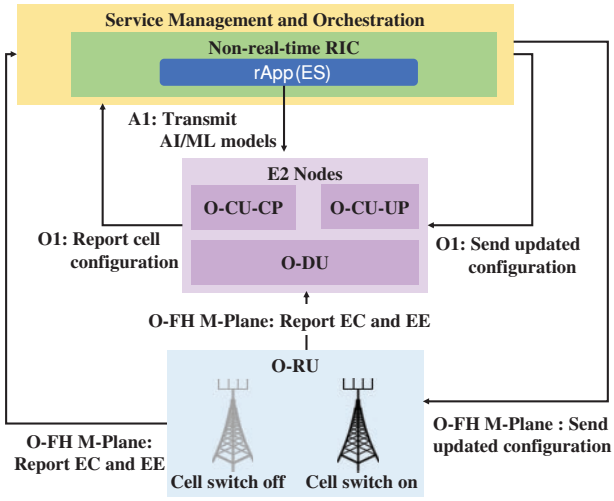


**Figure 9:** Energy saving by O-RAN components

### *3.7.2 Entities Involved in Use Case*

- **Non-RT RIC:** Non-RT RIC collects cell traffic information from E2 Nodes and O-RUs and configures carrier, cell switch off/on, and traffic steering. It also determines EE/ES optimization using AI/ML models and sends updated configuration to E2 Nodes via O1 and O-RU via Open FH M-Plane.
- **E2 Node:** E2 Node reports carrier (i.e., operating frequencies) cell configuration to SMO via the O1 interface.
- **O-RU Node:** O-RU nodes report information about EC and EE via the Open FH M-Plane interface to O-DU or SMO.

## 4 Security Threats against O-RAN Components

O-RAN has many advantages, but it also has several security threats. In this section, we investigate existing threats that can be applied in the O-RAN system and security threats against O-RAN components [56–60].

### *4.1 Conventional RAN Security Threats*

- **RAN Spoofing:** Spoofing attacks are a major threat to wireless networks. In such attacks, malicious actors impersonate legitimate users by manipulating their identifying signals. This can be achieved by transmitting fake signals that mimic authentic ones [61,62]. If a receiver mistakes the spoofed information for a genuine navigation message, it could lead to inaccurate positioning or timing data. Additionally, spoofing attacks can be used to launch Denial-of-Service (DoS) attacks [63].
- **RAN Sniffing:** RANs, including O-RAN, are vulnerable to eavesdropping attacks, where unauthorized individuals can intercept data transmissions. This technique, known as RAN sniffing, allows attackers to capture network information, potentially including sensitive details [9]. Unauthorized network monitoring raises significant privacy and security concerns [64]. For instance, attackers might exploit RAN sniffing to steal login credentials or intercept messages.

- **Jamming Attacks:** RANs are vulnerable to a general attack called jamming. In a jamming attack, malicious actors deliberately disrupt communication by transmitting interfering signals on the same frequency as the targeted network. This essentially drowns out the legitimate signal, hindering communication for authorized devices [65]. Jamming can specifically impact critical RAN elements, including reference signals, synchronization signals, and control channels [66]. In the O-RAN system, O-RAN interfaces are susceptible to jamming attacks.
- **User Data Traffic Vulnerability:** While 3GPP RAN employs integrity protection for CP messages, user data traffic remains susceptible. This vulnerability arises from the segregation between the CP and UP functionalities within the network architecture [9]. The disaggregation of O-CU into O-CU-CP and O-CU-UP in the O-RAN architecture introduces potential attack vectors for user data traffic.
- **Man-in-the-Middle Attacks:** In a Man-in-the-Middle (MITM) attack, a malicious actor secretly positions themself between two parties engaged in communication, deceiving each party into believing they are directly communicating with the other [67]. An attacker leveraging MITM attacks on the O-FH interface can disrupt critical timing synchronization. For example, the attacker intercepts UP data, specifically messages associated with the Precision Timing Protocol (PTP). By manipulating these messages, such as introducing delays in PTP sync messages or delay requests/responses, the attacker throws off PTP offset calculations. This can lead to clock inconsistencies across the network, potentially impacting network performance and reliability.
- **Physical Threats:** The additional hardware installed in the O-RAN can be compromised by attackers with physical access to the O-RAN system [8]. These attacks may encompass disrupting power availability, reconfiguring cabling, adding hardware backdoors, or compromising sensitive data.
- **Backdoors:** Given that O-RAN is anticipated to rely on open-source code, it becomes particularly susceptible to this form of attack. A malicious actor with trusted developer access could deliberately insert harmful code into the O-RAN codebase [68].

### *4.2 Threats against SMO*

- **Internal Attack:** Internal attackers can exploit authorized access to manipulate AI/ML training data or models stored in the SMO system, potentially influencing generated insights [56]. Even authorized internal actors could misuse their access to view, modify, or delete stored logs, posing similar risks to system integrity and security.
- **External Attack:** External attackers may gain access to external entities, allowing them to view or modify sensitive AI/ML data or models transferred between the external function and SMO via A1 and O1 interfaces. These attacks threaten the integrity and confidentiality of AI/ML processes and data within the system. In addition, external attackers may gain unauthorized access to stored logs, allowing them to view, modify, or delete log entries [56,69].

### *4.3 Threats against O-Cloud*

- **Credential Compromise in O-Cloud Services:** Access to O-Cloud services requires valid credentials, which adversaries may obtain through credential pharming or network breaches. Such compromised credentials enable attackers to bypass access controls, gain escalated privileges, persist within the system, or evade detection, potentially leading to unauthorized access to sensitive O-Cloud services and areas [56,70].

- **Threats Caused by CNF Deployments:** O-Cloud deploys CNF applications as containers across physical nodes, possibly spanning different geographical locations. This architecture, especially in multi-tenant or public cloud environments, makes it challenging to differentiate between externally and internally exposed services. One significant concern is the lack of proper authentication in CNF service endpoints, which can lead to various security threats [69].

### *4.4 Threats against O-RU*

- **False Base Station Attack:** An attacker can disrupt an O-RU's connection to the O-FH by connecting a malicious base station to the O-RU's fronthaul interface. O-RU then unwittingly serves as the air interface for the attack [71].

### *4.5 Threats against Near-RT RIC*

- **xApp Misuse and Privacy Concerns:** xApps can potentially manipulate cell behavior, affecting specific users or groups. A malfunctioning root of trust could lead to significant issues, including privacy breaches, tracking of subscribers, and targeted service disruptions [57]. Specifically, malicious xApps could exploit A1 and E2 interfaces to prioritize or deprioritize users, enabling unauthorized tracking and service manipulation and potentially targeting Very Important People (VIP) or specific subscriber groups [69].
- **User Identifier Exposure:** The E2 interface, facilitating near-real-time communication between xApps and RAN, can expose user identifiers. This exposure risks creating correlations between anonymized user identities across RAN nodes, turning xApps into potential sniffing tools for user identification [9].
- **Authorization Weaknesses:** The absence of mutual authentication between xApps and Near-RT RIC APIs can enable several attacks, including service theft, data leakage, and MITM attacks. In addition, weak or improperly implemented authentication mechanisms (e.g., basic user/password combos) also significantly elevate the risk of compromise, extending attack surfaces and potentially leading to unauthorized access and exploitation of network resources [6,56].

### *4.6 Threats against Non-RT RIC*

- **DoS Attack:** An attacker penetrates the Non-RT RIC through the SMO and attempts to trigger a DoS or degrade the performance of the Non-RT RIC, hindering its ability to monitor the network, update A1 policies, and securely deliver A1 enrichment information [72,73]. This could disrupt network operations and compromise the Non-RT RIC's ability to ensure effective management of the RAN environment.
- **Unauthorized Tracking and Data Corruption/Modification:** An attacker gaining access to the Non-RT RIC through the SMO poses risks of unauthorized tracking of users and potential data corruption or modification within the network [69,74]. This intrusion could compromise user privacy, undermine network integrity, and lead to unauthorized access to sensitive information or services.
- **Exploitation of Non-Unique rApp IDs:** Non-unique rApp IDs present vulnerabilities that could be exploited by malicious actors [56,57]. This poses risks of data leakage and unauthorized access to network resources, undermining the security and integrity of the Non-RT RIC framework.

### *4.7 Threats against R1 Interface*

- **Service Heartbeat Exploitation:** By manipulating or inserting heartbeat messages on the R1, an attacker can cause DoS, disrupting the regular monitoring and maintenance communications between services [56].
- **Unauthorized Access and Data Compromise:** An attacker exploits vulnerabilities in the system's service production authorization mechanism to impersonate a legitimate service producer, thereby gaining unauthorized access to R1 services [56]. Additionally, through spoofing attacks on the data request and subscription service, the attacker can illegitimately access data, posing substantial risks to data integrity and confidentiality.

### *4.8 Threats against A1 Interface*

- **Malicious Peering:** Due to insufficient mutual authentication mechanisms, a malicious Non-RT RIC can establish a peer connection with a Near-RT RIC over the A1 interface or vice versa [57]. This vulnerability facilitates unauthorized access and manipulation of RIC operations.
- **MiTM Attack:** An internal threat actor exploits weak security controls to conduct a MiTM attack on the A1 interface, enabling them to intercept and read policy-related messages [75].
- **Policy Modification or Injection:** By gaining access to the A1 interface, an internal threat actor can modify or inject malicious policy directives [56]. This manipulation can lead to the Near-RT RIC executing harmful or unintended policies, impacting network operations and security.

### *4.9 Threats against E2 Interface*

- **Weak Mutual Authentication:** Due to weak mutual authentication, a malicious E2 Node or Near-RT-RIC can communicate with each other over the E2 interface. This vulnerability opens the door to unauthorized access and potential attacks [76].

### *4.10 Threats against O1*

- **Identity Verification Failure:** The absence of robust identity verification mechanisms and logging capabilities prevents the SMO from validating the authenticity of the parties involved, directly threatening the security of data transmissions and policy enforcement between the SMO and Near-RT RIC [76].

### *4.11 Threats against O2*

- **Unauthorized Access and Disruption:** Insufficient protection of the O2 interface can enable attackers to disrupt, modify, or gain unauthorized access to communications between the O-Cloud and SMO [8]. This vulnerability threatens the normal operation of the O-Cloud and may lead to DoS attacks and data leakage.
- **Resource Mismanagement:** Attackers altering or intercepting virtualized resource management communications can cause resource misallocation and operational errors, expose sensitive configuration details, and enable further targeted attacks [56].

### *4.12 Threats against the O-FH Interface*

- **Unauthorized Access and Disruption:** Unauthorized access to the O-FH interface through coaxial cables, twisted pairs, or optical fibers can lead to attacks on the system's availability, integrity, and confidentiality [56,69]. An unauthorized device connected to this interface can

flood it with traffic, causing disruption or degradation of service, or send messages that disrupt the communication between legitimate network elements.

- **Heterogeneous Security Levels:** The use of O-RAN components from different vendors may result in varying security levels. This discrepancy complicates network security management and increases the potential for vulnerabilities to be exploited, posing additional risks to the network's overall security posture [9,56].

## 5 Security Requirements of O-RAN

Since O-RAN differs from traditional communication systems, various requirements must be investigated. This section describes the security requirements of each O-RAN component and interfaces [30,77,78].

- **SMO:** SMO shall authenticate internal requests, external systems, resource owners, servers, and clients and authorize service requests obtained from external systems [30]. Also, SMOs shall be able to recover from Distributed Denial of Service (DDoS) attacks without experiencing a catastrophic failure.
- **O-Cloud:** Users who access the O-Cloud platform need to be authenticated, authorized, and recommended to use Multi-Factor Authentication (MFA). The implementation of isolation measures for controlling and segregating resources among users is essential.
- The O-Cloud platform monitors App/VNF/CNF packages downloaded from the O-Cloud images repository [69]. To update the O-Cloud platform, all software images need to be verified by O-Cloud to ensure authenticity and integrity, and SMO needs to validate them further. Sensitive data, including Cryptographic keys, need to be safeguarded for integrity and confidentiality, both at rest and during transit and securely deleted using approved methods from active and backup storage media [30,78]. Additionally, the O-Cloud platform needs to support a root-of-trust mechanism to verify the integrity of all relevant components.
- **Non-RT RIC:** Non-RT RIC system needs to support authorization both as a resource owner/server and as a client, providing authorization to requests from rApps [78]. It should also demonstrate resilience by recovering from volumetric DDoS attacks across the A1 and R1 interfaces without experiencing catastrophic failure.
- **Near-RT RIC:** The Near-RT RIC system is mandated to authenticate xApp access to its databases during SDL registration and provide authorized access to these databases. Mutual authentication is required for secure communication between xApps and Near-RT RIC platform APIs [79]. Near-RT RIC architecture should incorporate an authorization framework that considers operator policies for xApps' consumption of services exposed in platform APIs. Near-RT RIC is required to support authorization as a resource owner, server, and client. Furthermore, it needs to be capable of recovering from volumetric DDoS attacks across the A1 interface without experiencing catastrophic failure [78].
- **O-CU-CP/UP:** O-CU-CP and O-CU-UP shall meet the security requirements for gNB-CU-CP and gNB-CU-UP, respectively, as specified in [10].
- **O-DU:** O-DU shall meet the security requirements for gNB-DU as specified in [10].
- **R1 Interface:** R1 interface needs to support mutual authentication and authorization, confidentiality, integrity, and replay protection [77].

- **A1 Interface:** A1 interface shall meet confidentiality, integrity, replay protection, and mutual authentication and authorization. It shall support mutual Transport Layer Security (mTLS) for Non-RT RICs and Near-RT RICs and Open Authorization (OAuth) 2.0 authentication [78].
- **O1 Interface:** O1 needs to use Transport Layer Security (TLS) 1.2 or higher to enforce confidentiality, integrity, and authenticity. Additionally, it shall enforce the least privileged access through Network Configuration Access Control Mode (NACM) [78].
- **E2/O2 Interface:** E2 and O2 interface need to meet confidentiality, integrity, replay protection, and data origin authentication [77].
- **O-FH M-Plane:** O-FH M-Plane needs to utilize strong authentication and authorization detection mechanisms to secure point-to-point Local Area Network (LAN) segments [69,77]. It also shall offer functionalities to block unauthorized access to unused ethernet ports on network elements.
- **O-FH CUS-Plane:** O-FH CUS-Plane needs to maintain secure access for O-DUs through authentication and authorization mechanisms [77,78]. The CUS-Plane also needs to support the authentication and authorization of PTP nodes and execute algorithms that prevent master clock spoofing.

Table 2 shows the mapping of previous studies' responses to security threats and requirements. Authors in [6] proposed a security strategy that uses public key infrastructure architecture. The proposed architecture is used for secure communication between an SMO and a Near-RT RIC. It involves registration, identity verification, digital certificate issuance, and two-way verification before they can communicate. Authors in [61] introduced a novel channel feature called channel virtual representation to address spoofing attacks. They leveraged channel virtual representation, a feature more sensitive to transmitter location than traditional methods. This enhanced sensitivity makes it well-suited for spoofing attack detection in mmWave 5G networks. They proposed two distinct detection algorithms to address spoofing attacks in both static and dynamic radio environments. Authors in [64] proposed a measurement-based sniffing detection method that utilizes traffic probes to identify suspicious activity and incorporates machine learning for enhanced analysis. They use not only Internet Control Message Protocol (ICMP), but also an Hypertext Transfer Protocol (HTTP) for traffic probing. They also showed how to detect sniffing on Linux. Authors in [65] proposed BeamArmor, a real-time application designed to safeguard cellular networks against jamming attacks. It leverages beam-nulling techniques with MIMO antennas, effectively canceling out jamming signals. BeamArmor achieves this real-time operation by optimizing computational resource allocation within the RAN stack. This ensures the system adheres to the stringent timing and security requirements of the cellular network's physical layer. Authors in [69] suggested using IEEE 802.1x and Internet Protocol Security (IPsec) to handle heterogeneous security levels due to different vendors/clients. while IEEE 802.1x supports various authentication methods, including certificate-based one-time passwords, IPsec secures communication by providing authentication for data origin and content (using authentication header), optional encryption (using encapsulating security payload), and secure key exchange (using Internet key exchange). In addition, the authors suggest using X.509 to handle a DoS attack against a master clock. X.509 is a hierarchical Public Key Infrastructure (PKI) where trust in certificate authorities (CAs) flows one-way from top to bottom. Authors in [72] proposed a DDoS detection method for IoT networks utilizing ML and neural networks. Authors in [73] generated the CICDDoS2019 dataset and built ML models using ID3, random forest, Naive Bayes, and logistic regression. Authors in [74] formulated a weighted-proportional-fairness-based resource allocation problem. They solved the problem by using the Lagrangian dual method, the brute force

method, and reinforcement learning. Authors in [75] proposed a 5G SPECTOR framework for O-RAN to detect cellular attacks against layer-3, with a telemetry stream and xApp. To handle malicious xApps, authors in [76] adopted an authentication mechanism such as API Key or OAuth 2.0 to ensure the system's security. Moreover, to strengthen the E2 signaling confirmation process, the authors suggest verification of its compliance and implementation of integrity protection for the E2 signaling content. Authors in [80] proposed a novel decentralized RAN architecture called Blockchain-enabled Radio Access Networks (BE-RAN) to enhance security and privacy in identification and authentication processes. Authors in [81] proposed a novel Blockchain Radio Access Network (B-RAN) architecture featuring secure and efficient decentralized mechanisms for managing network access and authentication, addressing the inherent trust challenges.

**Table 2:** Summary of security threats, requirements, and responses in O-RAN research

| Reference | Threat | Requirement | Response |
|---|---|---|---|
| [6] | Invalid authentication | Mutual authentication and authorization | Authors proposed public key infrastructure architecture |
| [61] | RAN spoofing | Authentication and authorization detection mechanisms | Authors proposed channel-based spoofing attack detection scheme based on channel virtual representation |
| [64] | RAN sniffing | Cryptographic keys and sensitive data safeguard algorithm | Authors proposed traffic probing and ML-based sniffing detection method |
| [65] | Jamming | Confidentiality, integrity, replay protection, and data origin authentication | Authors proposed BeamArmor, a practical real-time application to monitor and mitigate jamming attacks |
| [69] | Heterogeneous security levels | Harmonious authentication and authorization scheme | IEEE 802.1x access control mechanism and IPsec can be employed |
| | DoS attack against a master clock | Authentication and authorization of PTP nodes | X.509 certificates can be employed |
| [72,73] | DDoS | Ability to recover from DDoS attacks without experiencing a catastrophic failure | Authors proposed ML-based DDoS attack detection algorithm |
| [74] | Data compromise | Confidentiality, integrity, replay protection, and data origin authentication | Authors used Lagrangian dual method, the brute force method, and reinforcement learning to handle data falsification attacks |
| [75] | MiTM | Mutual authentication and authorization, confidentiality, integrity, and replay protection | Authors implemented 5G SPECTOR framework |

(Continued)

**Table 2 (continued)**

| Reference | Threat | Requirement | Response |
|---|---|---|---|
| [76] | Malicious xApps | mTLS and OAuth 2.0 authentication | Authors adopted an authentication mechanism such as API Key or OAuth 2.0 to ensure the system's security |
| | Lack of integrity protection | Confidentiality, integrity, and data origin authentication | Authors recommended verification of its compliance and implementation of integrity protection for the E2 signaling content. |
| [80] | Privacy attack | Cryptographic keys and sensitive data safeguard algorithm | Authors proposed Blockchain-Enabled Radio Access Networks (BE-RAN) |
| [81] | False base station | Mutual authentication and authorization | Authors proposed a Blockchain Radio Access Network (B-RAN) architecture and develop decentralized, secure, and efficient mechanisms |

## 6 Open Issues for O-RAN Security

The O-RAN security will encounter various issues in response to advancements in AI and Quantum Computing (QC) technology. This section explores these challenges, providing valuable insights into potential research directions to solve them.

### *6.1 Overhead and Cost of AI-Based Security*

#### *6.1.1 Challenges*

Since AI-based methods are low in complexity, AI-based security solutions will be integral to future O-RAN architecture. For example, to enhance security within O-RAN, integrating ML/DL-driven firewalls and Intrusion Detection Systems (IDS) is essential for safeguarding its subdomains [82]. However, it needs to consider the overhead caused by seamless data collection and communication between O-RAN components while meeting the security requirements [83].

#### *6.1.2 Future Research Directions*

To mitigate the data collection and communication overhead, generative AI-based rApps can be employed. Integrating these techniques can facilitate robust model training by generating and augmenting data, minimizing the need for additional data collection [84,85]. When installing generative AI-based rApps within non-RT RIC, the process excludes data collection executed by SMO or RAN nodes, and only a few communication occurs via the R1 or A1 interface, allowing us to reduce the amount of information shared through the network.

While generative AI-based rApps can reduce the overhead of O-RAN, the cost for maintaining and (re-)training these AI-based models within SMO or RIC needs to be considered. To reduce maintenance cost, rApps and xApps can leverage lightweight security models tailored to the various requirements of O-RAN environments. This can be achieved through model compression techniques such as quantization, pruning, weight factorization, knowledge distillation, and weight sharing [86,87].

To reduce (re-)training cost, transfer learning, and online learning techniques can be leveraged [88]. These techniques allow models to adapt and learn from new data without extensive retraining. By considering these strategies in practice, O-RAN networks can effectively harness the power of AI-based security solutions while mitigating associated overhead and costs.

### *6.2 Weak Generalizability Due to Diverse Security Requirements*

#### *6.2.1 Challenges*

In dynamic O-RAN environments, adaptable and resilient security solutions are paramount. The array of factors, including heterogeneous communication nodes, varied data types, high-mobility users, and diverse O-RAN vendor equipment, makes the O-RAN security requirements diverse and complex [89–91]. This complexity inevitably leads to vulnerabilities in AI models, rendering them susceptible to weak generalizability. Retraining models with new data is a straightforward solution to address any deficiencies or changes in networks. However, it is time-consuming and can compromise real-time responsiveness, posing a significant challenge in the face of evolving threats.

#### *6.2.2 Future Research Directions*

Here, GNNs can be used to enhance model generalizability. Unlike traditional fully connected neural networks, which struggle to adapt to changing network sizes, GNNs excel in dynamic environments [92]. While a fully connected scheduler would require retraining for each user pool size, GNNs can inherently handle variations in user numbers or requirements. This flexibility stems from their ability to add or remove components during feature extraction and information exchange stages, allowing them to seamlessly adapt to the evolving network landscape [93]. Considering O-RAN components and each component's security requirements in GNN (e.g., node feature, edge) can enhance the generalizability of AI-based security models.

Moreover, the integration of Automated Reinforcement Learning (AutoRL) into GNN-based O-RAN security solutions can also be discussed. AutoRL automates the process of identifying the best hyperparameter configurations for an RL agent, ultimately maximizing its performance [94,95]. Given that AutoRL operates within the realm of RL, known for its resilience in dynamic network scenarios, its usage can significantly bolster the adaptability of models to dynamic O-RAN environments [96]. Thus, the synergy between AutoRL and GNN may further enhance the model's generalizability and adaptability.

### *6.3 Computation Overhead of Secured Federated Learning*

#### *6.3.1 Challenges*

To address the privacy and poisoning attacks against AI models within RIC and user data, federated learning emerges as a promising solution [97]. Federated learning enables collaborative training of AI models across mobile devices in the O-RAN network without compromising local privacy. Devices train local models on their private data and then contribute updates to a central server, aggregating them to build a robust global model [98]. However, federated learning introduces

a trade-off. While it can prevent model poisoning and privacy attacks, the communication overhead of aggregating numerous local model updates can create a bottleneck.

#### *6.3.2 Future Research Directions*

Recently, Over-the-Air Computation (AirComp) has been introduced to handle the bottleneck problem of federated learning [99]. AirComp offers significant advantages in communication efficiency compared to the traditional separation of communication and computation. By leveraging the superposition property of a wireless multiple-access channel, AirComp enables concurrent transmission of locally computed updates, effectively reducing the required bandwidth and network traffic [100,101]. Integrating federated learning with AirComp can reduce communication overhead.

### *6.4 Quantum Computing Threats*

#### *6.4.1 Challenges*

QC has the potential to pose security threats to O-RAN networks. QC represents an unprecedented level of computing power, surpassing the capabilities of a state-of-the-art supercomputer [9,102]. Thus, with its computing capabilities, QC can assist O-RAN by processing the RIC computation tasks in real-time. However, from the security perspective, QC poses a threat to the security of communication networks since it challenges the complexity of cryptographic algorithms.

#### *6.4.2 Future Research Directions*

Quantum Resistance (QR) cryptography-based security strategies can be discussed to ensure the security of the O-RAN system while mitigating QC threats. O-RAN can utilize the functionalities provided by Quantum Cryptography (QC) through various algorithms based on lattices, multivariate problems, or elliptic curves [103]. This enables O-RAN to achieve the necessary service level requirements with enhanced security guarantees.

## 7 Conclusion

This paper provides an overview of general O-RAN architecture and use case specifications that can be applied or extended in future B5G and 6G. Moreover, this paper aims to create a comprehensive guideline for future research by providing O-RAN security threats, requirements, and discussions. In future work, more use cases can be investigated and extended. Also, solution strategies for each threat can be analyzed.

**Acknowledgement:** This paper is an extended version of the paper presented at the 7th International Symposium on Mobile Internet Security (MobiSec'23) Conference.

**Funding Statement:** This study was supported by the Research Program funded by the SeoulTech (Seoul National University of Science and Technology).

**Author Contributions:** The authors confirm contribution to the paper as follows: study conception and design: Heejae Park, Laihyuk Park; data collection: Tri-Hai Nguyen; analysis and interpretation of results: Heejae Park, Tri-Hai Nguyen; draft manuscript preparation: Laihyuk Park. All authors reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** As this paper is an investigation, it does not contain any original datasets generated. Investigated specifications can be downloaded on the official website: https://orandownloadsweb.azurewebsites.net/specifications (accessed on 31 April 2024).

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References


1. Park H, Nguyen TH, Park L. Federated deep learning for RIS-assisted UAV-enabled wireless communications. In: 2022 13th International Conference on Information and Communication Technology Convergence (ICTC); 2022; Jeju Island, Republic of Korea: IEEE. p. 831–3.
2. Du H, Zhang J, Guan K, Niyato D, Jiao H, Wang Z, et al. Performance and optimization of reconfigurable intelligent surface aided THz communications. IEEE Trans Commun. 2022;70(5):3575–93. doi:10.1109/TCOMM.2022.3162645.
3. Park H, Nguyen TH, Park L. Reconfigurable intelligent surface-assisted system models for uplink communications. In: 2022 13th International Conference on Information and Communication Technology Convergence (ICTC); 2022; Jeju Island, Republic of Korea: IEEE. p. 828–30.
4. Gavrilovska L, Rakovic V, Denkovski D. From cloud RAN to open RAN. Wirel Pers Commun. 2020;113:1523–39. doi:10.1007/s11277-020-07231-3.
5. D'Oro S, Bonati L, Polese M, Melodia T. OrchestRAN: network automation through orchestrated intelligence in the open ran. In: IEEE INFOCOM 2022-IEEE Conference on Computer Communications; 2022; London, UK: IEEE. p. 270–9.
6. Shen C, Xiao Y, Ma Y, Chen J, Chiang CM, Chen S, et al. Security threat analysis and treatment strategy for ORAN. In: 2022 24th International Conference on Advanced Communication Technology (ICACT); 2022; PyeongChang KwangwoonDo, Republic of Korea: IEEE. p. 417–22.
7. Kang MS. Potential security concerns at the physical layer of 6G cellular systems. In: 2022 13th International Conference on Information and Communication Technology Convergence (ICTC); 2022; Jeju Island, Republic of Korea: IEEE. p. 981–4.
8. Polese M, Bonati L, Doro S, Basagni S, Melodia T. Understanding O-RAN: architecture, interfaces, algorithms, security, and research challenges. IEEE Commun Surv Tutor. 2023;25(2):1376–411. doi:10.1109/COMST.2023.3239220.
9. Liyanage M, Braeken A, Shahabuddin S, Ranaweera P. Open RAN security: challenges and opportunities. J Netw Comput Appl. 2023;214:103621. doi:10.1016/j.jnca.2023.103621.
10. 3rd Generation Partnership Project (3GPP). Security architecture and procedures for 5G system: TS 33.501 V17.7.0; 2020. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
11. Singh SK, Singh R, Kumbhani B. The evolution of radio access network towards open-ran: challenges and opportunities. In: 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW); 2020; Seoul, Republic of Korea: IEEE. p. 1–6.
12. Abdalla AS, Upadhyaya PS, Shah VK, Marojevic V. Toward next generation open radio access networks: what O-RAN can and cannot do! IEEE Netw. 2022;36(6):206–13. doi:10.1109/MNET.108.2100659.
13. Mimran D, Bitton R, Kfir Y, Klevansky E, Brodt O, Lehmann H, et al. Security of open radio access networks. Comput Secur. 2022;122:102890. doi:10.1016/j.cose.2022.102890.
14. Singh AK, Nguyen KK. Joint selection of local trainers and resource allocation for federated learning in open RAN intelligent controllers. In: 2022 IEEE Wireless Communications and Networking Conference (WCNC); 2022; Austin, TX, USA: IEEE. p. 1874–9.

15. Filali A, Nour B, Cherkaoui S, Kobbane A. Communication and computation O-RAN resource slicing for URLLC services using deep reinforcement learning. IEEE Commun Stand Mag. 2023;7(1):66–73. doi:10.1109/MCOMSTD.0002.2100078.
16. Zhang H, Zhou H, Erol-Kantarci M. Federated deep reinforcement learning for resource allocation in O-RAN slicing. In: GLOBECOM 2022-2022 IEEE Global Communications Conference; 2022; Rio de Janeiro, Brazil: IEEE. p. 958–63.
17. Motalleb MK, Shah-Mansouri V, Naghadeh SN. Joint power allocation and network slicing in an open RAN system. arXiv preprint arXiv:191101904. 2019.
18. Wang Q, Liu Y, Wang Y, Xiong X, Zong J, Wang J, et al. Resource allocation based on radio intelligence controller for open RAN towards 6G. IEEE Access. 2023;11:97909–19. doi:10.1109/ACCESS.2023.3311888.
19. Motalleb MK, Shah-Mansouri V, Parsaeefard S, López OLA. Resource allocation in an open RAN system using network slicing. IEEE Trans Netw Serv Manag. 2022;20(1):471–85.
20. Kazemifard N, Shah-Mansouri V. Minimum delay function placement and resource allocation for Open RAN (O-RAN) 5G networks. Comput Netw. 2021;188:107809. doi:10.1016/j.comnet.2021.107809.
21. Wang X, Thomas JD, Piechocki RJ, Kapoor S, Santos-Rodríguez R, Parekh A. Self-play learning strategies for resource assignment in Open-RAN networks. Comput Netw. 2022;206:108682. doi:10.1016/j.comnet.2021.108682.
22. Ravindran S, Chaudhuri S, Bapat J, Das D. Efficient service allocation scheduling algorithms for 5G user equipments in slice-in-slice networks. In: 2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS); 2021; Hyderabad, India: IEEE. p. 36–41.
23. Orhan O, Swamy VN, Tetzlaff T, Nassar M, Nikopour H, Talwar S. Connection management xAPP for O-RAN RIC: A graph neural network and reinforcement learning approach. In: 2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA); 2021; Pasadena, CA, USA: IEEE. p. 936–41.
24. Zhang H, Zhou H, Erol-Kantarci M. Team learning-based resource allocation for open radio access network (O-RAN). In: ICC 2022-IEEE International Conference on Communications; 2022; Seoul, Republic of Korea: IEEE. p. 4938–43.
25. Mollahasani S, Pamuklu T, Wilson R, Erol-Kantarci M. Energy-aware dynamic DU selection and NF relocation in O-RAN using actor-critic learning. Sensors. 2022;22(13):5029. doi:10.3390/s22135029.
26. Lacava A, Polese M, Sivaraj R, Soundrarajan R, Bhati BS, Singh T, et al. Programmable and customized intelligence for traffic steering in 5G networks using open ran architectures. IEEE Trans Mob Comput. 2023;23(4):2882–97.
27. Kavehmadavani F, Nguyen VD, Vu TX, Chatzinotas S. Intelligent traffic steering in beyond 5g open ran based on lstm traffic prediction. IEEE Trans Wirel Commun. 2023;22(11):7727–42. doi:10.1109/TWC.2023.3254903.
28. Erdol H, Wang X, Li P, Thomas JD, Piechocki R, Oikonomou G, et al. Federated meta-learning for traffic steering in o-ran. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall); 2022; London, UK: IEEE. p. 1–7.
29. Kavehmadavani F, Nguyen VD, Vu TX, Chatzinotas S. Traffic steering for eMBB and uRLLC coexistence in open radio access networks. In: 2022 IEEE International Conference on Communications Workshops (ICC Workshops); 2022; Seoul, Republic of Korea: IEEE. p. 242–7.
30. O-RAN Alliance. O-RAN security requirements specification 6.0. 2023. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
31. Klement F, Katzenbeisser S, Ulitzsch V, Krämer J, Stanczak S, Utkovski Z, et al. Open or not open: are conventional radio access networks more secure and trustworthy than open-RAN? arXiv preprint arXiv:220412227. 2022

32. Marinova S, Leon-Garcia A. Intelligent O-RAN beyond 5G: architecture, use cases, challenges, and opportunities. IEEE Access. 2024;12:27088–114. doi:10.1109/ACCESS.2024.3367289.
33. Groen J, DOro S, Demir U, Bonati L, Polese M, Melodia T, et al. Implementing and evaluating security in O-RAN: interfaces, intelligence, and platforms. arXiv preprint arXiv:230411125. 2023.
34. Wang TH, Chen YC, Huang SJ, Hsu KS, Hu CH. Design of a network management system for 5g open ran. In: 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS); 2021; Tainan, Taiwan: IEEE. p. 138–41.
35. O-RAN Alliance. O-RAN use cases analysis report 13.0. 2024. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
36. O-RAN Alliance. O-RAN use cases detailed specification 13.0. 2024. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
37. Yoshizawa T, Singelée D, Muehlberg JT, Delbruel S, Taherkordi A, Hughes D, et al. A survey of security and privacy issues in V2X communication systems. ACM Comput Surv. 2023;55(9):1–36.
38. Garcia MHC, Molina-Galan A, Boban M, Gozalvez J, Coll-Perales B, Şahin T, et al. A tutorial on 5G NR V2X communications. IEEE Commun Surv Tutorials. 2021;23(3):1972–2026. doi:10.1109/COMST.2021.3057017.
39. He Y, Gan Y, Cui H, Guizani M. Fairness-based 3D multi-UAV trajectory optimization in multi-UAV-assisted MEC system. IEEE Internet Things J. 2023;10(13):11383–95. doi:10.1109/JIOT.2023.3241087.
40. Diao J. Unmanned aerial vehicles swarm-based distributed phased arrays for grating lobe mitigation and collision avoidance. IEEE Open J Antennas Propag. 2022;3:1264–72. doi:10.1109/OJAP.2022.3220277.
41. Ruan L, Wang J, Chen J, Xu Y, Yang Y, Jiang H, et al. Energy-efficient multi-UAV coverage deployment in UAV networks: a game-theoretic framework. China Commun. 2018;15(10):194–209. doi:10.1109/CC.2018.8485481.
42. Anwar MR, Wang S, Akram MF, Raza S, Mahmood S. 5G-enabled MEC: a distributed traffic steering for seamless service migration of internet of vehicles. IEEE Internet Things J. 2021;9(1):648–61.
43. Wu H, Ferlin S, Caso G, Alay Ö, Brunstrom A. A survey on multipath transport protocols towards 5G access traffic steering, switching and splitting. IEEE Access. 2021;9:164417–39. doi:10.1109/ACCESS.2021.3134261.
44. Chopra R, Murthy CR, Papazafeiropoulos AK. Uplink performance analysis of cell-free mMIMO systems under channel aging. IEEE Commun Lett. 2021;25(7):2206–10. doi:10.1109/LCOMM.2021.3073778.
45. Barb G, Otesteanu M. Digital GoB-based beamforming for 5G communication systems. In: 2020 International Symposium on Antennas and Propagation (ISAP); 2021; Osaka, Japan: IEEE. p. 469–70.
46. Zheng B, You C, Mei W, Zhang R. A survey on channel estimation and practical passive beamforming design for intelligent reflecting surface aided wireless communications. IEEE Commun Surv Tutorials. 2022;24(2):1035–71. doi:10.1109/COMST.2022.3155305.
47. Avitabile G, Florio A, Coviello G. Angle of arrival estimation through a full-hardware approach for adaptive beamforming. IEEE Trans Circuits Syst II: Express Briefs. 2020;67(12):3033–7.
48. Wang X, Wang J, Xu Y, Chen J, Jia L, Liu X, et al. Dynamic spectrum anti-jamming communications: challenges and opportunities. IEEE Commun Mag. 2020;58(2):79–85. doi:10.1109/MCOM.35.
49. Ahmad WSHMW, Radzi NAM, Samidi FS, Ismail A, Abdullah F, Jamaludin MZ, et al. 5G technology: towards dynamic spectrum sharing using cognitive radio networks. IEEE Access. 2020;8:14460–88. doi:10.1109/Access.6287639.
50. Xin J, Xu S, Zhang L. Dynamic spectrum sharing for NR-LTE networks. In: 2021 2nd Information Communication Technologies Conference (ICTC); 2021; Nanjing, China. p. 161–4.
51. Gao K, Wang H, Lv H, Liu W. Toward 5G NR high-precision indoor positioning via channel frequency response: a new paradigm and dataset generation method. IEEE J Sel Areas Commun. 2022;40(7):2233–47. doi:10.1109/JSAC.2022.3157397.

52. Bai L, Sun C, Dempster AG, Zhao H, Cheong JW, Feng W. GNSS-5G hybrid positioning based on multi-rate measurements fusion and proactive measurement uncertainty prediction. IEEE Trans Instrum Meas. 2022;71:1–15.
53. Chang KC, Chu KC, Wang HC, Lin YC, Pan JS. Energy saving technology of 5G base station based on internet of things collaborative control. IEEE Access. 2020;8:32935–46. doi:10.1109/Access.6287639.
54. Xu D, Zhou A, Zhang X, Wang G, Liu X, An C, et al. Understanding operational 5G: a first measurement study on its coverage, performance and energy consumption. In: Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication; 2020; USA. p. 479–94.
55. Li YNR, Chen M, Xu J, Tian L, Huang K. Power saving techniques for 5G and beyond. IEEE Access. 2020;8:108675–90. doi:10.1109/Access.6287639.
56. O-RAN Alliance. O-RAN security threat modeling and risk assessment 2.0; 2024. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
57. O-RAN Alliance. O-RAN security threat modeling and remediation analysis 6.0; 2023. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
58. O-RAN Alliance. O-RAN study on security for service management and orchestration (SMO) 3.0; 2024. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
59. O-RAN Alliance. O-RAN study on security for O-cloud 5.0; 2024. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
60. O-RAN Alliance. O-RAN study on security for near real time RIC and xApps 5.0; 2024. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
61. Li W, Wang N, Jiao L, Zeng K. Physical layer spoofing attack detection in MmWave massive MIMO 5G networks. IEEE Access. 2021;9:60419–32. doi:10.1109/ACCESS.2021.3073115.
62. Wu Z, Zhang Y, Yang Y, Liang C, Liu R. Spoofing and anti-spoofing technologies of global navigation satellite system: a survey. IEEE Access. 2020;8:165444–96. doi:10.1109/Access.6287639.
63. Lichtman M, Rao R, Marojevic V, Reed J, Jover RP. 5G NR jamming, spoofing, and sniffing: threat assessment and mitigation. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops); 2018; Kansas City, MO, USA: IEEE. p. 1–6.
64. Gregorczyk M, żórawski P, Nowakowski P, Cabaj K, Mazurczyk W. Sniffing detection based on network traffic probing and machine learning. IEEE Access. 2020;8:149255–69. doi:10.1109/Access.6287639.
65. Zumegen FJ, Jain IK, Bharadia D. BeamArmor: seamless anti-jamming in 5G cellular networks with MIMO null-steering. In: Proceedings of the 25th International Workshop on Mobile Computing Systems and Applications; 2024; San Diego, CA, USA. p. 121–6.
66. Chi Z, Li Y, Liu X, Wang W, Yao Y, Zhu T, et al. Countering cross-technology jamming attack. In: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks; 2020; Linz, Austria. p. 99–110.
67. Mallik A. Man-in-the-middle-attack: understanding in simple words. Cyberspace: Jurnal Pendidikan Teknol Informasi. 2019;2(2):109–34.
68. Balding C. Revisiting the United States telecommunications network policy in a post-huawei world: improving economic competitiveness, addressing security weakness, and building alliances. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3861826. [Accessed 2021].
69. Abdalla AS, Marojevic V. End-to-end O-RAN security architecture, threat surface, coverage, and the case of the open fronthaul. IEEE Commun Standards Mag. 2024;8(1):36–43. doi:10.1109/MCOMSTD.0001.2200047.
70. Klement F, Liu W, Katzenbeisser S. Toward securing the 6G transition: a comprehensive empirical method to analyze threats in O-RAN environments. IEEE J Sel Areas Commun. 2024;42(2):420–31. doi:10.1109/JSAC.2023.3339172.

71. Tabiban A, Alameddine HA, Salahuddin MA, Boutaba R. Signaling storm in O-RAN: challenges and research opportunities. IEEE Commun Mag. 2023;62(6):58–64.
72. Doshi R, Apthorpe N, Feamster N. Machine learning ddos detection for consumer internet of things devices. In: 2018 IEEE Security and Privacy Workshops (SPW); 2018; San Francisco, CA, USA: IEEE. p. 29–35.
73. Sharafaldin I, Lashkari AH, Hakak S, Ghorbani AA. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In: 2019 International Carnahan Conference on Security Technology (ICCST); 2019; Chennai, India: IEEE. p. 1–8.
74. Chen H, Zhou M, Xie L, Wang K, Li J. Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack. IEEE Trans Vehicular Technol. 2016;65(11):9181–91. doi:10.1109/TVT.2016.2520983.
75. Wen H, Porras P, Yegneswaran V, Gehani A, Lin Z. 5G-SPECTOR: an O-RAN compliant Layer-3 cellular attack detection service. In: Network and Distributed System Security (NDSS) Symposium; 2024; San Diego, CA, USA.
76. Hung CF, Chen YR, Tseng CH, Cheng SM. Security threats to xApps access control and E2 interface in O-RAN. IEEE Open J Commun Soc. 2024;5:1197–203. doi:10.1109/OJCOMS.2024.3364840.
77. O-RAN Alliance. O-RAN security requirements and controls specification 7.0; 2023. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
78. O-RAN Alliance. O-RAN security requirements and controls specification 8.0; 2024. Available from: https://www.o-ran.org/specifications. [Accessed 2024].
79. Wypiór D, Klinkowski M, Michalski I. Open ran-radio access network evolution, benefits and market trends. Appl Sci. 2022;12(1):408. doi:10.3390/app12010408.
80. Xu H, Zhang L, Sun Y, Chih-Lin I. BE-RAN: blockchain-enabled open RAN with decentralized identity management and privacy-preserving communication. arXiv preprint arXiv:210110856. 2021.
81. Ling X, Wang J, Bouchoucha T, Levy BC, Ding Z. Blockchain radio access network (B-RAN): towards decentralized secure radio access paradigm. IEEE Access. 2019;7:9714–23. doi:10.1109/Access.6287639.
82. Brik B, Chergui H, Zanzi L, Devoti F, Ksentini A, Siddiqui MS, et al. A survey on explainable AI for 6G O-RAN: architecture, use cases, challenges and research directions. arXiv preprint arXiv:230700319. 2023.
83. Chen PY, Das P. AI maintenance: a robustness perspective. Computer. 2023;56(2):48–56. doi:10.1109/MC.2022.3218005.
84. Van Huynh N, Wang J, Du H, Hoang DT, Niyato D, Nguyen DN, et al. Generative AI for physical layer communications: a survey. IEEE Trans Cogn Commun Netw; 2024;10(3):706–28. doi:10.1109/TCCN.2024.3384500.
85. Bariah L, Zhao Q, Zou H, Tian Y, Bader F, Debbah M. Large generative AI models for telecom: the next big thing? IEEE Commun Mag. 2024;1–7. doi:10.1109/MCOM.001.2300364.
86. Choudhary T, Mishra V, Goswami A, Sarangapani J. A comprehensive survey on model compression and acceleration. Artif Intell Rev. 2020;53:5113–55. doi:10.1007/s10462-020-09816-7.
87. Cheng Y, Wang D, Zhou P, Zhang T. Model compression and acceleration for deep neural networks: the principles, progress, and challenges. IEEE Signal Process Mag. 2018;35(1):126–36. doi:10.1109/MSP.2017.2765695.
88. Zhu Z, Lin K, Jain AK, Zhou J. Transfer learning in deep reinforcement learning: a survey. IEEE Trans Pattern Anal Mach Intell; 2023;45(11):13344–62. doi:10.1109/TPAMI.2023.3292075.
89. Alhashimi HF, Hindia MN, Dimyati K, Hanafi EB, Safie N, Qamar F, et al. A survey on resource management for 6G heterogeneous networks: current research, future trends, and challenges. Electronics. 2023;12(3):647. doi:10.3390/electronics12030647.

90. Xiong K, Fan P, Zhang Y, Letaief KB. Towards 5G high mobility: a fairness-adjustable time-domain power allocation approach. IEEE Access. 2017;5:11817–31. doi:10.1109/ACCESS.2017.2712710.
91. Dryjański M, Kułacz Ł., Kliks A. Toward modular and flexible open ran implementations in 6G networks: traffic steering use case and o-ran xapps. Sensors. 2021;21(24):8173. doi:10.3390/s21248173.
92. Tan Y, Liu J, Wang J. 5G end-to-end slice embedding based on heterogeneous graph neural network and reinforcement learning. IEEE Trans Cogn Commun Netw. 2024;10(3):1119–31. doi:10.1109/TCCN.2024.3349452.
93. Jiang T, Cheng HV, Yu W. Learning to reflect and to beamform for intelligent reflecting surface with implicit channel estimation. IEEE J Sel Areas Commun. 2021;39(7):1931–45. doi:10.1109/JSAC.2021.3078502.
94. Parker-Holder J, Rajan R, Song X, Biedenkapp A, Miao Y, Eimer T, et al. Automated reinforcement learning (AutoRL): a survey and open problems. J Artif Intell Res. 2022;74:517–68. doi:10.1613/jair.1.13596.
95. Truong TP, Tuong VD, Dao NN, Cho S. FlyReflect: joint flying IRS trajectory and phase shift design using deep reinforcement learning. IEEE Internet Things J. 2022;10(5):4605–20.
96. Portelas R, Colas C, Weng L, Hofmann K, Oudeyer PY. Automatic curriculum learning for deep RL: a short survey. arXiv preprint arXiv:200304664. 2020.
97. Khan LU, Saad W, Han Z, Hossain E, Hong CS. Federated learning for internet of things: recent advances, taxonomy, and open challenges. IEEE Commun Surv Tutorials. 2021;23(3):1759–99. doi:10.1109/COMST.2021.3090430.
98. Li L, Fan Y, Tse M, Lin KY. A review of applications in federated learning. Comput Ind Eng. 2020;149:106854. doi:10.1016/j.cie.2020.106854.
99. Xu C, Liu S, Yang Z, Huang Y, Wong KK. Learning rate optimization for federated learning exploiting over-the-air computation. IEEE J Sel Areas Commun. 2021;39(12):3742–56. doi:10.1109/JSAC.2021.3118402.
100. Yang K, Jiang T, Shi Y, Ding Z. Federated learning via over-the-air computation. IEEE Trans Wirel Commun. 2020;19(3):2022–35. doi:10.1109/TWC.7693.
101. Liu W, Zang X, Li Y, Vucetic B. Over-the-air computation systems: optimization, analysis and scaling laws. IEEE Trans Wirel Commun. 2020;19(8):5488–502. doi:10.1109/TWC.7693.
102. Herman D, Googin C, Liu X, Galda A, Safro I, Sun Y, et al. A survey of quantum computing for finance. arXiv preprint arXiv:220102773. 2022.
103. Ranaweera P, De Alwis C, Jurcut AD, Liyanage M. Realizing contact-less applications with multi-access edge computing. ICT Express. 2022;8(4):575–87. doi:10.1016/j.icte.2022.03.001.