

# Toward Next Generation Open Radio Access Networks—What O-RAN Can and Cannot Do!

<sup>1</sup>Aly S. Abdalla, <sup>2</sup>Pratheek S. Upadhyaya, <sup>3</sup>Vijay K. Shah and <sup>1</sup>Vuk Marojevic

<sup>1</sup>Dept. of Electrical and Computer Engineering, Mississippi State University, USA

<sup>2</sup> Dept. of Electrical and Computer Engineering, Virginia Tech, USA

<sup>3</sup> Dept. of Cybersecurity Engineering, George Mason University, USA

Emails: asa298@msstate.edu, pratheek@vt.edu, vshah22@gmu.edu, vuk.marojevic@msstate.edu

**Abstract**—The open radio access network (O-RAN) describes an industry-driven open architecture and interfaces for building next generation RANs with artificial intelligence (AI) controllers. We circulated a survey among researchers, developers, and practitioners to gather their perspectives on O-RAN as a framework for 6G wireless research and development (R&D). The majority responded in favor of O-RAN and identified R&D of interest to them. Motivated by these responses, this paper identifies the limitations of the current O-RAN specifications and the technologies for overcoming them. We recognize end-to-end security, deterministic latency, physical layer real-time control, and testing of AI-based RAN control applications as the critical features to enable and discuss R&D opportunities for extending the architectural capabilities of O-RAN as a platform for 6G wireless.

**Index Terms**—6G, AI, O-RAN, real-time control, security, testing.

## I. INTRODUCTION

Next generation 5G and 6G networks are introducing architectural transformations from an inflexible and monolithic system to a flexible, agile and disaggregated architecture to support service heterogeneity, coordination among multiple technologies, and rapid on-demand deployments. Such transformations are enabled by the emerging open radio access network (O-RAN) framework which provides virtualization, intelligence, and flexibility while defining open interfaces for network innovation. The O-RAN based 5G and future 6G networks will incorporate artificial intelligence (AI) into the deployment, operation, and maintenance of the network [1]. The O-RAN architecture is expecting to offer a new dawn of services and applications for cellular networks, such as virtual network slices and dynamic spectrum sharing.

O-RAN takes advantage of Cloud RAN (C-RAN) principles and leverages the increasingly software-defined implementations of wireless communications and networking functions. Instead of legacy interfaces that are vendor-specific and controlled by major industry players, it defines open interfaces and an open architecture for innovation at all layers. It assumes that cellular network management will be increasingly data driven and establishes the generic modules and interfaces for data collection, distribution, and processing.

There have been initial studies that analyze the O-RAN technology and possible use cases for improving the performance of cellular networks. The potentials of AI applied on a data set provided by a network operator for radio resource management

are demonstrated in [2]. A green O-RAN system model is proposed in [3], which introduces the use of renewable energy sources and how to minimize the cost of deployment by applying reinforcement learning for dynamic function splitting. A data-driven closed-loop control experiment with reinforcement learning agents for optimizing the scheduler of multiple RAN slices is presented in [1]. A closed-loop control system for O-RAN is designed and validated on an outdoor testbed for maximizing the capacity of the system composed of an aerial and multiple terrestrial UEs by optimizing the drone location and transmission directionality [4].

Prior work has presented the O-RAN architecture and use cases. The contribution of this paper is to identify the limitations of the current architecture and the technologies and opportunities for research and development (R&D) for overcoming them. This is motivated by a survey that we circulated among researchers, developers, and practitioners to gather their perspectives on O-RAN as a framework for 6G wireless. Based on the responses that we received, we identify the critical components that are not addressed by the specifications—security, latency, real time control, and testing—and make recommendations.

The rest of the paper is organized as follows: Section II presents the survey results. We briefly introduce the O-RAN architecture, components, and interfaces in Section III, followed by the capabilities and use cases in Section IV. Section V identifies the main O-RAN limitations and directions for R&D. Section VI provides the concluding remarks.

## II. COMMUNITY SURVEY

In 2020/2021 we circulated a survey among wireless researchers, developers, and practitioners to explore the interest in O-RAN and to receive feedback on research priorities. About 150 experts in advanced wireless communications and networking were invited to participate in the survey. We were not seeking a popular poll and chose to distribute it via personal invitations to avoid misleading responses or misuse. Surveyors had to identify themselves and were asked for permission to use the anonymized data.

Participants from 65 institutions responded, 50 located in North America, 12 in Europe, and 3 in Asia. There were 95 total participants: 21 full professors, 13 associate professors, 14 assistant professors, 9 postdoctoral researchers, 10 experienced PhD candidates, and 28 experts from industry, government research laboratories, and research institutes.

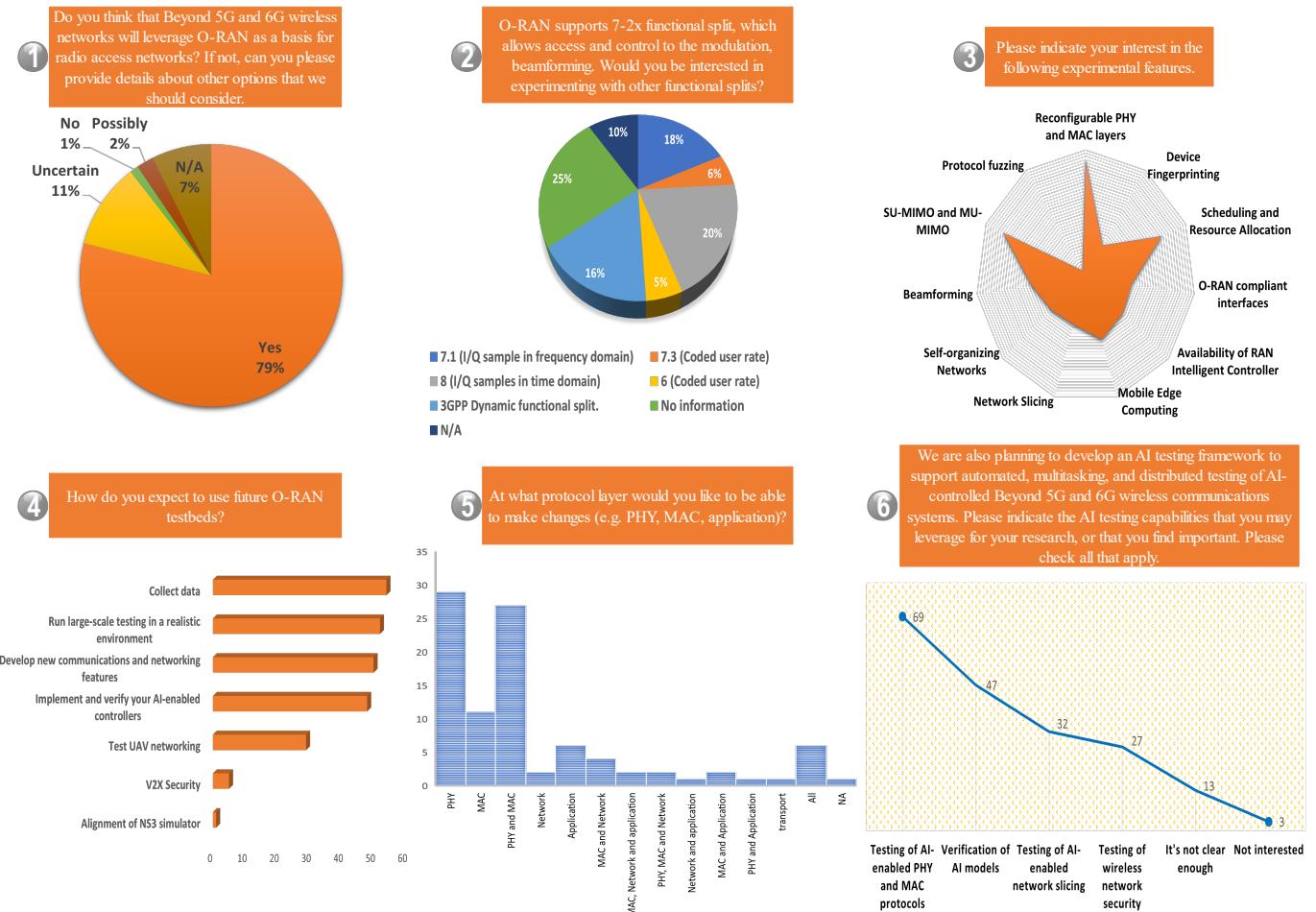


Fig. 1: Community survey outcome.

The purpose of this survey was to initiate the dialog with the advanced wireless and networking R&D community about O-RAN, understand if O-RAN is the framework of interest for 6G wireless R&D, and what features are of most interest. We asked questions about what O-RAN capabilities they are most interested exploring and what new capabilities they would be interested in developing or using. For each question we provided a list of sample choices, allowed introducing alternative answers, and selecting multiple choices.

Figure 1(1) shows that the majority agrees that O-RAN will be the foundation of future cellular networks. The answers to Question 2 indicate that around 38% are interested in having the ability to access the in-phase and quadrature (I/Q) data in the time and frequency domains leveraging different functional split (FS) options. Sixteen percent (16%) of the participants would like to see support for a dynamic FS in O-RAN. The O-RAN features of highest interest are the programmable physical (PHY) and medium access control (MAC) layers, single and multi-user multiple-input, multiple-output (MIMO), scheduling and resource allocation (Fig. 1(3)). Figure 1(4) presents the expectations of the survey takers about their intended use of future O-RAN research testbeds. At the top of the list is data collection, large-scale experimentation under realistic constraints, development of novel communications and

networking features, and the implementation and verification of AI-enabled wireless network controllers. Such use cases require access to the PHY and MAC layers, as highlighted in Fig. 1(5). The majority of survey takers find it important to facilitate testing of AI controlled RANs, from the PHY to higher layers (Fig. 1(6)).

The obtained data motivates studying the capabilities and limitations of O-RAN, and what R&D can do to extend the capabilities of the architecture and introduce complementary elements and processes.

### III. THE O-RAN ARCHITECTURE, COMPONENTS, AND INTERFACES

The O-RAN Alliance was formed by merging the C-RAN Alliance and the xRAN Forum. Its mission is to extend the current RAN standards and facilitate open, intelligent, virtualized, and fully interoperable next generation RANs [5]. Many of its members are also members of the Third Generation Partnership Project (3GPP). They meet regularly to update specifications that are made accessible to the community. The O-RAN Alliance defines study items that are currently organized into ten technical work groups (WGs) and four focus groups (FGs). Figure 2 shows the high-level O-RAN architecture and the roles of the WGs and FGs.

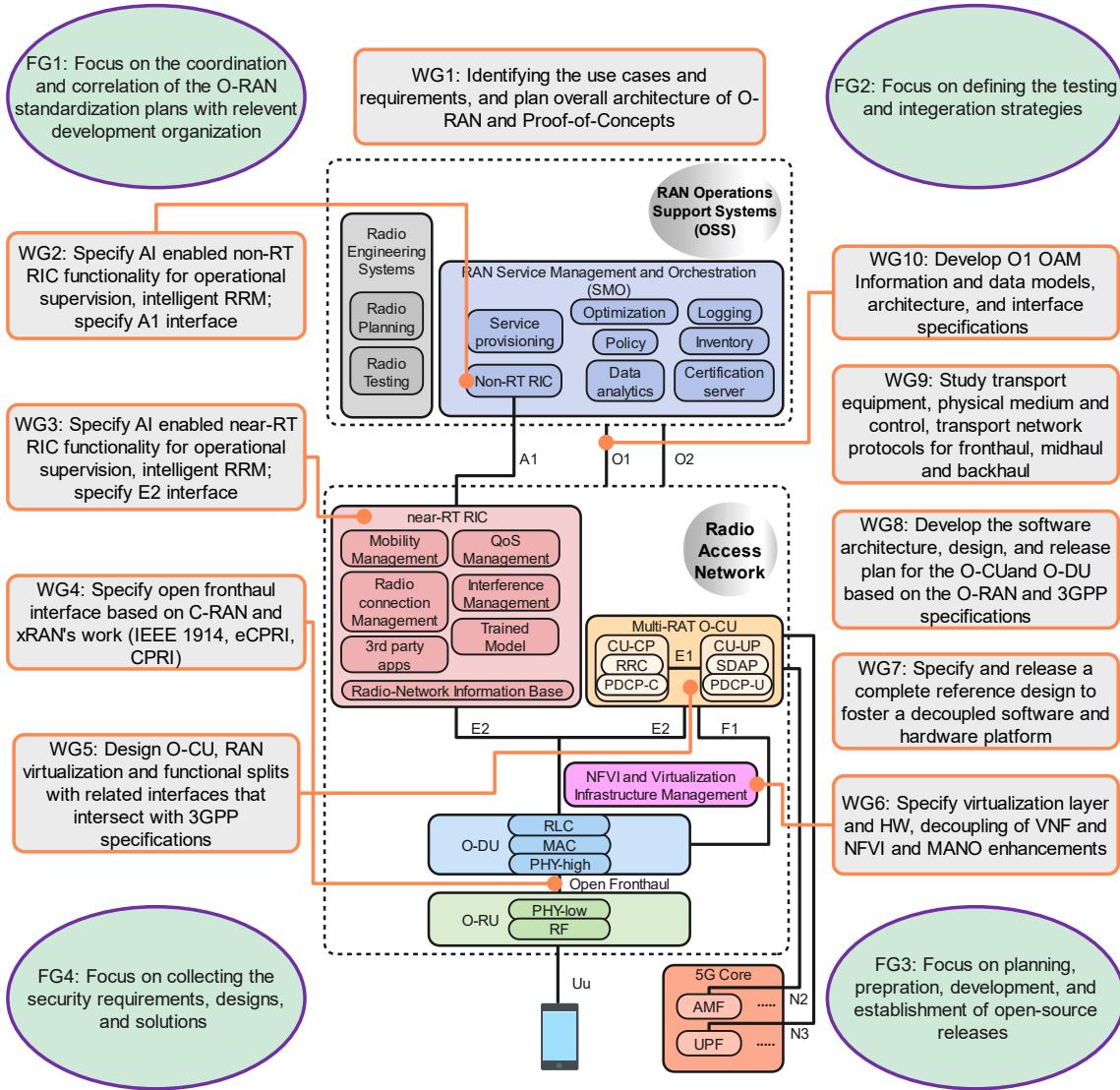


Fig. 2: The O-RAN architecture (center) and the work and focus groups with their objectives.

The O-RAN architecture encompasses the RAN, the operations support systems (OSS), and open interfaces. The design of the O-RAN architecture is in harmony with the 5G new radio (NR) RAN architecture defined by 3GPP. The central unit (CU), distributed unit (DU), and radio unit (RU) of a modern RAN are responsible for delivering diverse functions of the radio protocol stack associated with the radio resource control (RRC), service data adaption protocol (SDAP), packet data convergence protocol (PDCP), radio link control (RLC), MAC, and PHY layers. The O-RAN RU (O-RU) is in charge of establishing the PHY layer connection with the user equipment (UE). It integrates the antenna elements with the radio frequency (RF) processing components, such as transceivers, analog beamformers, and power amplifiers. In addition to the RF processing, the O-RU integrates the lower level PHY layer processing (PHY-low), such as digital beamforming and the fast Fourier transform (FFT)/inverse-FFT. The Open Fronthaul interface connects the O-RU to the O-DU. The O-DU is responsible for the higher level processing functions at the PHY layer (PHY-high), such as channel modulation and

coding/decoding, the MAC layer, and the RLC layer.

The upper layers of the radio protocol—the RRC, the PDCP, and the SDAP—are provided by the O-CU. The design of the O-CU enables the simultaneous operation of both long-term evolution (LTE) O-DUs and 5G NR O-DUs, and is known as multi-radio access technology (multi-RAT). It is supported by the network function virtualization infrastructure (NFVI). The N2 and N3 interfaces are responsible for handling the communications between the multi-RAT O-CU and the access and mobility management function (AMF) and user plane function (UPF) of the 5G core network.

3GPP introduced the F1 interface that connects the CU to the DUs and the E1 interface to enable coordination between the control and user planes at the CU. The O-RAN Alliance establishes the E2 interface, which forwards the measurements from the O-DU and O-CU to the near-RT RIC, and the configuration commands back to the O-CU and O-DU. The near-RT RIC is a logical function that enables near-RT RAN control and optimization. This is implemented through xApps.

The OSS is a component of modern and increasingly

software-defined wireless networks. It is responsible for radio planning and testing and for service management and orchestration (SMO), i.e. for monitoring, and life cycle operation and management functions of the softwareized O-RU, O-DU, O-CU, and near-RT RIC components. There are different subsystems within the OSS for, among other things, data analysis, logging, inventory, certification, and non-RT RIC operations through third-party rApps.

The A1, O1 and O2 interfaces assist with the signaling between the OSS and the RAN. The A1 interfaces facilitates AI related parameter exchange between the non-RT and near-RT RICs. The O1 interface, which is standardized by 3GPP, is used for fault, configuration, and performance management of the RAN nodes. The O2 interface facilitates resource management at the NFVI of virtualized RAN deployments.

#### IV. WHAT O-RAN CAN DO: CAPABILITIES AND USE CASES

O-RAN is disruptive in that it opens up the RAN interfaces to spur innovation and contributions for new developers and vendors. This can provide several benefits, such as reduced cost of maintenance, dynamic services, and quicker time to market for new user and network management services as well as other innovations in the wireless domain. This section summarizes the salient features of O-RAN under three categories.

##### A. RAN Disaggregation, Open Interfaces, and Multi-Vendor Support

Functional splits were introduced in 3GPP Release 15 to allow splitting the base station functionalities into the CU and the DU, implementing the higher and lower layers of the RAN protocol stack, respectively. Although 3GPP defines many split options (Fig. 3a), vendors use proprietary implementations and interfaces which has led to single vendor network solutions. O-RAN adopts FS Option 2 for the F1 interface between the O-DU and O-CU, and Option 7-2x for implementing the fronthaul, the interface between the O-DU and O-RU (Fig. 3b). O-RAN employs a modified version of the common public radio interface (CPRI), the enhanced CPRI (eCPRI), for the fronthaul [7].

The openness of the O-RAN architecture and interfaces enables cellular operators to employ unique strengths of each vendor for a delicate application or service and facilitates RAN function sharing. It is envisaged that the near-RT RIC and non-RT RIC will be able to support different vendors' O-CUs and O-DUs. A direct benefit of the disaggregated RIC architecture and open interfaces (E2 and A1) is that it supports interoperability and flexibility in deployment and independent fault tolerant systems. An example of this is the collaboration between the O-RAN Software Community (OSC) and Open Networking Foundation's SD-RAN and the compatibility between OSC's RIC and software radio solutions such as srsRAN and OpenAirInterface [8], [9].

Depending on the bandwidth and latency requirements, it is possible to deploy the O-CU, O-DU, and near-RT RIC functions centrally or at the edge. They can be implemented

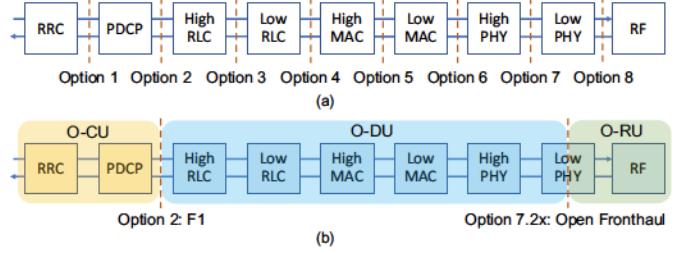


Fig. 3: 3GPP FS options (a) and the O-RAN FSs and interfaces between the O-CU, O-DU, and O-RU (b).

as virtual network functions (VNFs) and be deployed in any RAN tier on commercial off-the-shelf hardware, as has been demonstrated with software radio implementations of 4G/5G RANs [10]. In practice, these are implemented as virtual machines and containers managed by a hypervisor<sup>1</sup> and virtualized infrastructure manager [11], respectively, to ensure scalability, diverse network support, and interoperability. Load management, RT performance optimization, and maintenance of various quality of service (QoS) requirements, among others, can thus be handled through multiple instances of the O-CU and the O-DU that share the same physical resources.

##### B. Support for Different Timescales

One of the main requirements for meeting the heterogeneous 5G services, such as interference management, resource allocation, security, and traffic offloading, is being able to perform RAN operations at the appropriate timescales. A 5G network may respond with resource changes at sub-millisecond time granularity. The O-RAN Alliance defines the closed-loop control of the RAN by enabling the RICs to operate at different timescales:

- **The non-RT control loop** operates at a timescale of at least 1 s through the A1 and O1 interfaces. Examples include instantiation and orchestration of network slices, resource allocation at the infrastructure level and data driven RAN policy guidance to xApps in the near-RT RIC. Such decisions can be taken at frequencies spanning seconds, hours, or even days.
- **The near-RT control loop** operates on a timescale between 10 ms and 1 s through the E2 interface. The xApps leverage user session data and MAC and PHY layer data to optimize the quality of experience (QoE) by controlling time sensitive services, such as resource scheduling, beamforming, load balancing, and handover.

Combining the fast processing at the near-RT RIC with the larger timescale analysis at the non-RT RIC is a unique capability of the O-RAN architecture. Table I shows some of the RAN operations that can be implemented leveraging the different timescale properties of O-RAN enabled by the non-RT and near-RT control loops.

<sup>1</sup>A hypervisor, also known as virtual machine monitor, is software that creates and controls virtual machines.

TABLE I: Representative O-RAN use cases employing AI as defined by the O-RAN Alliance [6].

Use case	Network layer	AI functionality description	Training host	Inference host	Training data	Action
Massive MIMO beamforming optimization	PHY	Predict the optimal configuration of massive MIMO parameters for each cell according to a global optimization objective designed by the operator.	Non-RT RIC	Non-RT RIC	Key performance indicators (KPIs) related to traffic load, coverage and QoS performance, per beam/area and massive MIMO configuration.	Configure the optimized beam parameters via the O1 interface.
Quality of experience (QoE) optimization	MAC	Predict the application/traffic types, QoE and available bandwidth.	Non-RT RIC	Near-RT RIC	Network level measurement report including UE data, L2 measurement, RAN protocol stack status, cell level information, QoE measurement metrics and user traffic.	E2 control or policy commands towards the RAN for the QoE optimization.
Dynamic spectrum sharing (DSS)	MAC	Predict the short-term traffic demand based on near-RT metrics from the RAN.	Non-RT RIC	Near-RT RIC	Location, DSS modality, cell configuration, used, reserved, requested, and blocked PHY resource blocks (PRBs), number of active UEs, traffic demand, QoS classes, and UE capability information.	E2 control/policy of resource configuration and scheduling coordination.
Network slice subnet instance (NSSI) resource allocation optimization	MAC	Predict of the traffic demand patterns of NSSI at different times and locations.	Non-RT RIC	NA	Measurement counters per slicing subnet instance. These include downlink (DL) and uplink (UL) PRBs used for data traffic, average DL and UL throughput, and the number of packet data unit sessions successfully set up and failed to set up.	Reconfigure the NSSI attributes via the O1 interface and update the Cloud resources via the O2 interface.
Context-based dynamic handover (HO) management for vehicular users	MAC	Customize HO sequences for a UE according to intents, policies, and configurations taking into consideration the high speeds and the heterogeneous environment of vehicular UEs.	Non-RT RIC	Near-RT RIC	Historic data from a vehicular UE over the V1 interface, which include UE location, velocity, and trajectory, measurement reports for serving and neighboring cells, and connection and mobility statistics.	RAN deploys the configuration received from the near-RT RIC over the E2 interface.
Radio resource allocation to unmanned aerial vehicles (UAVs)	MAC	Perform the radio resource allocation for UAVs to tackle challenges such as RF interference, poor KPIs caused by base station antenna patters (side lobes towards sky).	Non-RT RIC	Near-RT RIC	Aerial vehicle related measurement metrics from SMO and based on UE measurement reports, radio channel information, mobility related metrics, flight path, climate, forbidden/limited 3D area information, etc.	The near-RT RIC delivers the radio resource allocation configurations to the O-CU/O-DU over the E2 interface.
Traffic steering	MAC	Traffic steering among various RATs, such as LTE, NR, and Wi-Fi, according to different traffic management objectives.	Non-RT RIC	Near-RT RIC	Measurement reports, cell load statistics cell quality thresholds, channel quality indicator reports and measurement gaps on per-UE or per-frequency basis.	The traffic management policy is activated and transferred to the near-RT RIC via the A1 interface.

### C. AI Integration and xApps/rApps

The O-RAN architecture inherently enables collecting application and radio environmental information to perform intelligent decisions using AI models. The non-RT RIC is a controller of the SMO that provides policy management, AI management, and data enrichment services to the underlying RAN nodes. AI management services include the transfer of the trained AI model to the near-RT RIC and the periodic or triggered updates of the model. The data enrichment capability of the non-RT RIC delivers the required information to the near-RT RIC, which performs data analytics and management functions.

The variability of key performance indicators (KPIs) and QoS levels of 5G use cases along with the existing operation and maintenance functions of cellular networks enable optimizing the cellular performance parameters per cell. The O-RAN technology, on the other hand, enables performance enhancements per UE from the collected long-term traffic, coverage, and observed interference information, among others. Integrating the resource management in the near-RT RIC is beneficial for reducing the burden on the core network as well as reducing the data transfer and time overhead of forwarding

and processing data between the RAN and the core network. This improves the overall efficiency and latency of the system.

AI is expected to improve several functionalities of software-defined RANs. Among those functionalities are load balancing, resource allocation, fault detection, and security. Table I summarizes the currently defined use cases [6] where the O-RAN architecture can provide a major impact in terms of AI control and enhanced RAN performance. It identifies the layers at which the network function is implemented, the AI operations, and the type of data that is required to train these AI models. Preliminary works implementing these use cases with open source software include

- An xApp implementing a basic network slicing framework in srsRAN [8],
- A slice and resource scheduling xApp employing deep reinforcement learning with a fully functional data collection framework [9], and
- A traffic steering xApp developed by the OSC to showcase dynamic handover of users from one cell to another based on traffic predictions [12].

Furthermore, besides collecting and training AI models for xApps in the near-RT RIC, the non-RT RIC can itself host AI-driven rApps, such as AI-based orchestration of network

slices and data-driven policy management, to improve the automation and management of RAN resources and xApps.

## V. WHAT O-RAN CANNOT DO: LIMITATIONS AND R&D DIRECTIONS

This section identifies the major limitations of the current O-RAN specifications and outlines R&D directions to overcome those and spur the evolution of O-RAN as the architectural framework for next generation wireless network deployments.

### A. End-to-End Security

The O-RAN architecture enables the dynamic disaggregation of functionalities, the introduction of new functions, protocols, components, and interfaces. The new components, interfaces, and the lower layer split (LLS) however expands the threat surface and makes O-RAN prone to additional security risks beyond those of the 3GPP architecture. The O-RAN security threats can be categorized in six primary classes [13]:

- 1) The first threat class is related to the new functions that O-RAN adds, which include the SMO and the RICs. A misconfiguration or missing authentication process related to these functions can become a severe threat to network operations.
- 2) The second class is characterized by the improper or missing ciphering of the data sent across the open interfaces A1, E2, O1, O2, and the fronthaul.
- 3) The third class of attacks comes from the LLS—the 7-2x split—that introduces vulnerabilities via possible decision conflicts among the O-RAN components.
- 4) The fourth threat class results from the functional decoupling and multi-vendor support. This can lead to the reliance on different security levels and the lack of a root of trust.
- 5) The fifth class comes from the disaggregation of software and hardware and the virtualization of the O-RAN system that lacks sufficient security measures.
- 6) The sixth class stems from the implementation of O-RAN using open-source software. This raises security risks where an adversary may be able to replicate and test the software and system operations to find loopholes and design attacks that may be difficult to detect.

Figure 4 illustrates the potential security vulnerabilities that could be exploited to compromise the confidentiality, integrity, and availability of next generation wireless networks implementing the O-RAN architecture. Security threats can target the architecture, the open-source software-defined procedures, and the AI subsystem. An example of a security attack would be hijacking an operator's RAN infrastructure and resources by exploiting the vulnerabilities of remote access privileges provided to other operators in the RAN sharing scenario. Hijacking is a type of network security attack in which the attacker takes control of one or more network functions, the open-source software, or the AI subsystem in this case. Exploiting a vulnerability refers to a set of actions that an attacker takes after finding a weakness in the hardware or software to proceed with a targeted attack.

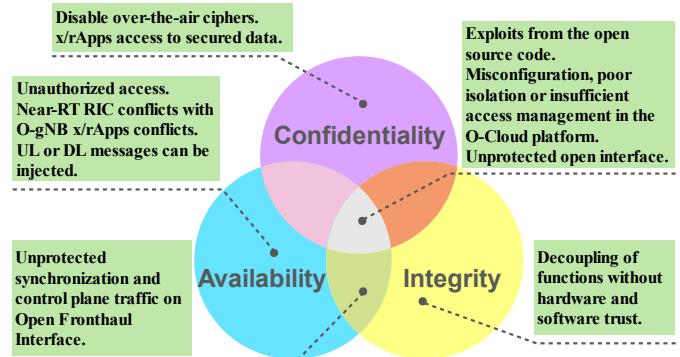


Fig. 4: Potential security vulnerabilities of O-RAN.

The O-RAN Alliance has established a security focus group which aims to define the security requirements, designs, and solutions for O-RAN security threats. There are more R&D directions that need to be explored. These include the mutual authentication for verifying access to O-RAN system and prevent malicious applications and components, mechanisms enabling trusted implementation of xApps and AI models, and cryptography with secure key management, including key generation, storage, rotation, and revocation. Figure 5 indicates the need for employing mutual authentication mechanisms over the O-RAN interfaces to preserve the privacy and confidentiality of the data. The decoupling of hardware and software requires a trust chain from bottom up. One promising solution to mitigate security risks in this context is the adoption of a zero-trust security framework that assumes no implicit trust and continuously evaluates the risks.

### B. Deterministic Latency

Open interfaces and multi-vendor support spur innovation. This, however, makes it more difficult to control and optimize the data and control plane latency. The general concept and latency model of the O-RAN architecture is based on the eCPRI reference model for delay management.

The O-RU constraint is typically preset as it depends on the hardware. The signal transfer between the O-RU and O-DU is expected to have a relative time error over the synchronization plane of  $3 \mu\text{s}$  ( $\pm 1.5 \mu\text{s}$ ). In order to ensure the reception of data within the established delay boundaries, the transmitter and the receiver need to define a transmission and a reception window, respectively. These windows are defined with respect to each other, where the reception window must be greater than or equal to the sum of the transmission window and the transport variations for the uplink and the downlink transmissions. Based on the O-RAN specifications, the parameters used for defining the reception and transmission windows must be reported with an accuracy of 200 ns.

The above timing requirements cannot be guaranteed when an O-RAN system communicates with another system that does not follow the O-RAN delay specifications. This may lead to cases where the packets are transmitted or received too early, before the start of the window, or too late, after the end of the window. Such packets should be discarded. However,

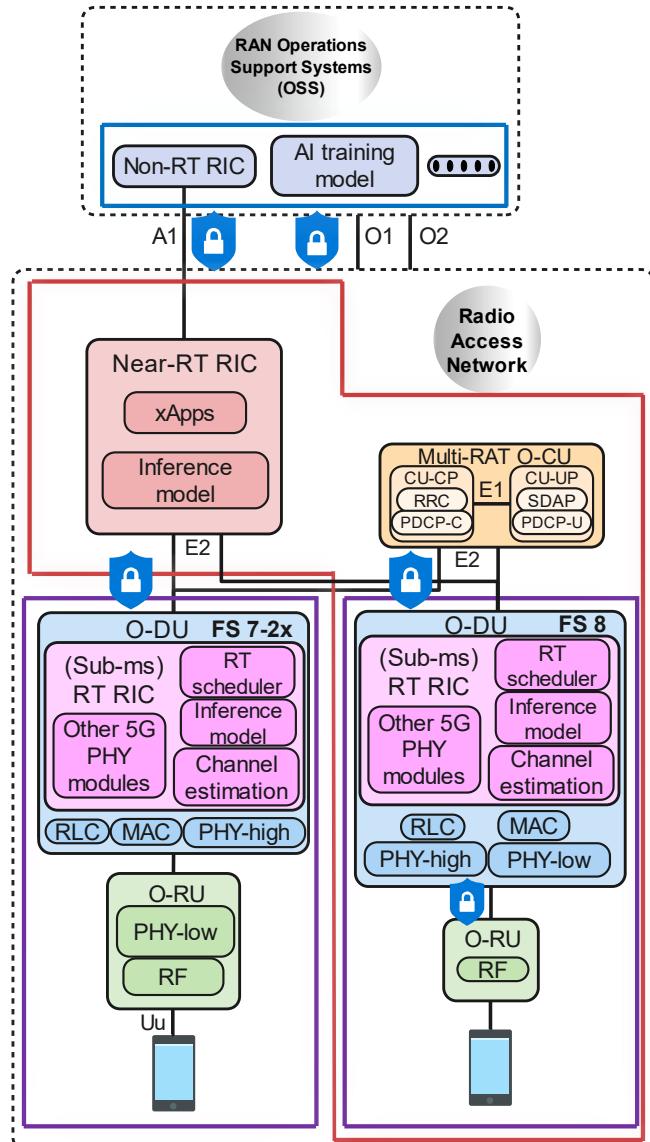


Fig. 5: Proposed next generation O-RAN architecture extensions: O-DU/O-RU splits, RT RIC, and RT control loop.

the specification do not impede processing too early or too late packets which may disturb the O-RAN timing process of control or user plane packets.

When we compare this to the CPRI and eCPRI timing specifications, we notice that the CPRI uses strictly periodic scheduling with the k28.5 time marker that makes the latency and delay measurement more deterministic. The eCPRI, on the other hand, relies on statistical synchronization without a fixed time marker such as the precision time protocol.

A future R&D direction to tackle this challenge is the dynamic FS [3]. The dynamic FS relies on varying the placement of the different network functions of the O-RAN architecture to satisfy the latency requirements based on feedback from the network. Figure 5 illustrates how the future O-RAN architecture can support multiple FSs supported by a single near-RT RIC to satisfy different timing requirements.

### C. PHY Layer RT Control

As discussed previously, one of the foremost benefits of the near-RT RIC is the intelligent and fine-grained RAN control functionalities at both the O-CU and the O-DU through the E2 interface. While the near-RT RIC could perform rudimentary control of PHY layer functions, such as reducing the beam search space, the timescale at which it operates (10 ms – 1 s) makes it difficult to control many of the PHY layer processes. This necessitates the introduction of a (sub-millisecond) real-time controller hosted at either the O-CU or the O-DU.

We propose integrating a third control loop, the real-time control loop enabled by the RT RIC, which can possibly be situated in the O-CU, O-DU, or O-RU. Although the RT RIC can host any type of lower layer RAN control functionality, which we call *zApps*—third-party control applications hosted in the envisioned RT RIC—the introduction of AI will enable dealing with the complexity of the PHY layer, heterogeneous resources, and operating environments for building highly configurable, yet manageable RANs. Research has shown that the performance of the RAN can be improved by employing data-driven learning techniques [3], [9], [14], [15]. Obstacles for realizing this include the compute power of the nodes (O-CU/O-DU), the energy efficiency, the ability of AI models to deliver decisions at sub-millisecond timescale (response time constraints), and the amount of signaling overhead for low-level PHY layer control. These are critical factors that might have an adverse impact on fulfilling the promises of low-latency next generation cellular networks.

Promising solutions to the above problem include running the *zApps* at near-constant time complexity combined with subject-matter expert validation [15] and developing a new class of highly accurate and lightweight AI algorithms, such as echo state networks, which are less data intensive. The integration of RAN hardware acceleration within O-RAN is expected to augment the performance of x86 based server platforms that implement O-CUs and O-DUs.

### D. Testing of AI-Driven O-RAN Functionalities

Wireless network intelligence is enabled in O-RAN through AI-driven xApps and deployments in the near-RT and non-RT RICs. However, the unpredictable behavior of the AI algorithms, specifically when considering a closed-loop AI controller, may lead to unstable system configurations and performance losses. Poorly-designed AI solutions can degrade the quality of decisions made by the xApps, rApps, and the envisioned *zApps*. In addition, xApps, rApps, and *zApps* may be incompatible and have opposing objectives that can lead to unstable network operations.

It is therefore critical to evaluate and test the stability and robustness of the AI algorithms to be deployed to avoid untested configurations, conflicting decisions, or exposure of vulnerabilities. In addition to standardized predeployment test, measurement, and certification procedures, testing and maintenance needs to be an integral part of the O-RAN operations. Such online testing procedures within the intelligent controllers of O-RAN need to monitor and assess the employed AI algorithms for adapting to unfamiliar data or operational

environments, such as excessive noise or RF interference, unexpected signals, or conflicting messages from the network or the users. In addition, the testing framework should be capable of defining the competence of the AI algorithms to cope with the randomness and variations of the data and cases of incomplete, uncertain, or missing training data. The interpretability and explainability of AI algorithms have to be considered within the O-RAN testing workflow where more research and data are needed. The interpretability shows how accurate the output of the model is given a certain input. The explainability illustrates how the internal mechanisms and designs of the AI model affect the output.

Testing should encompass the AI models and the data because AI models may fail despite regular data or they may fail because false data is injected. We recommend integrating services into the AI workflow for such testing and validation and into next-generation RAN processes for delivering high-fidelity live representations of all functions that are running on O-RAN deployments, where one O-CU, O-DU, and O-RU configuration may differ from another within the same operator and across operators and services.

## VI. CONCLUSIONS

O-RAN defines a disruptive architecture for realizing next generation wireless networks. It specifies open interfaces and logical elements that support intelligence, disaggregation, software-defined, virtualization, and collaboration. We conducted a survey among researchers, developers, and practitioners to explore their interests in O-RAN and their needs for 6G R&D. As a result of our survey, we identify critical limitations of the current O-RAN specifications in terms of security, latency, real-time control, and testing of AI-based RAN control applications. We outline the technologies and R&D opportunities to overcome these limitations and extend the O-RAN architectural capabilities.

## ACKNOWLEDGEMENT

This work was supported in part by the National Science Foundation under grant numbers 2120411 and 2120442.

## REFERENCES

- [1] L. Bonati, S. D’Oro, M. Polese, S. Basagni, and T. Melodia, “Intelligence and learning in O-RAN for data-driven NextG cellular networks,” pp. 1–7, 2021, <https://arxiv.org/abs/2012.01263>.
- [2] S. Niknam, et al., “Intelligent O-RAN for Beyond 5G and 6G wireless networks,” pp. 1–7, 2020, <https://arxiv.org/abs/2005.08374>.
- [3] T. Pamuklu, M. Erol-Kantarci, and C. Ersoy, “Reinforcement learning based dynamic function splitting in disaggregated green open RANs,” in *IEEE International Conference on Communications*, June 2021, pp. 1–6.

- [4] L. Bertizzolo, T. X. Tran, J. Buczek, B. Balasubramanian, R. Jana, Y. Zhou, and T. Melodia, “Streaming from the air: Enabling high data-rate 5G cellular links for drone streaming applications,” pp. 1–13, 2021, <https://arxiv.org/abs/2101.08681>.
- [5] Open-RAN Alliance, “O-RAN: towards an open and smart RAN,” *White Paper*, pp. 1–19, 2018.
- [6] C. Li and A. Akman, “O-RAN use cases and deployment scenarios. towards open and smart ran,” *White paper*, 2020.
- [7] A. Umesh, T. Yajima, T. Uchino, and S. Okuyam, “Overview of O-RAN fronthaul specifications,” in *NTT DOCOMO Technical Journal*, vol. 21, no. 01, 2019, pp. 46–59.
- [8] D. Johnson, D. Maas, and J. Van Der Merwe, “Nexran: Closed-loop ran slicing in powder-a top-to-bottom open-source open-ran use case,” in *Proceedings of the 15th ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization*, 2022, pp. 17–23.
- [9] M. Polese, L. Bonati, S. D’Oro, S. Basagni, and T. Melodia, “Colo-RAN: Developing machine learning-based xApps for open RAN closed-loop control on programmable experimental platforms,” *arXiv preprint arXiv:2112.09559*, 2021.
- [10] A. S. Abdalla, A. Yingst, K. Powell, A. Gelonch-Bosch, and V. Marojevic, “Open source software radio platform for research on cellular networked uavs: It works!” *IEEE Commun. Mag.*, vol. 60, no. 2, pp. 60–66, 2022.
- [11] M. Floriach-Pigem, G. Xercavins-Torregrosa, A. Gelonch-Bosch, and V. Marojevic, “Creating tailored and adaptive network services with the open orchestration C-RAN framework,” in *2018 IEEE 5G World Forum (5GWF)*, 2018, pp. 89–92.
- [12] M. Dryjański, Ł. Kułacz, and A. Kliks, “Toward modular and flexible open RAN implementations in 6G networks: Traffic steering use case and O-RAN xApps,” *MDPI Sensors*, vol. 21, no. 24, p. 8173, 2021.
- [13] O-RAN - Security Focus Group (SFG), “O-RAN Security Threat Modeling and Remediation Analysis,” Open-RAN Alliance, Technical Specification, 07 2021, version 02.00.01.
- [14] H. Mohammadi and V. Marojevic, “Artificial neuronal networks for empowering radio transceivers: Opportunities and challenges,” in *IEEE Vehicular Technology Conference (VTC2021-Fall)*, 2021, pp. 1–5.
- [15] F. B. Mismar and J. Hoydis, “Unsupervised learning in next-generation networks: Real-time performance self-diagnosis,” *IEEE Communications Letters*, vol. 25, no. 10, p. 3330–3334, Oct 2021.

## BIOGRAPHIES

**Aly Sabri Abdalla** (asa298@msstate.edu) is a PhD candidate in the Department of Electrical and Computer Engineering at Mississippi State University, Starkville, MS, USA. His research interests are on scheduling, congestion control and wireless security for vehicular ad-hoc and UAV networks.

**Pratheek S. Upadhyaya** (pratheek@vt.edu) is a PhD student in the Department of Electrical and Computer Engineering at Virginia Polytechnic and State University, Blacksburg, VA, USA. His research interests include scheduling, 5G/next-G communications, AI/ML applications in wireless communications and spectrum sharing.

**Vijay K. Shah** (vshah22@gmu.edu) is an assistant professor of cybersecurity engineering at George Mason University, Fairfax, VA, USA. His research interests include 5G/next-G communications, AI/ML, wireless security, and wireless testbed development.

**Vuk Marojevic** (vuk.marojevic@msstate.edu) is an associate professor in electrical and computer engineering at Mississippi State University, Starkville, MS, USA. His research interests include resource management, vehicle-to-everything communications and wireless security with application to cellular communications, mission-critical networks, and unmanned aircraft systems.