A 5G Americas White Paper

OPEN RAN UPDATE

November 2023

Contents

Executive Summary

The Open Radio Access Networks (RAN) industry is dynamically evolving, transitioning from closed, monolithic architectures to open architectures that are based on the decomposition of physical and virtual functions, supporting interoperable interfaces that enable multi-vendor deployments. While encouraging competition among vendors, open RAN simultaneously drives supply chain diversification. This same broadening of the RAN ecosystem opens up innovation opportunities. Simultaneously, Open RAN delivers both a simplified network management, that is now standardized across multiple vendors, as well as being highly scalable through the use of cloud-native operations. Finally, Open RAN facilitates data accessibility, enabling AI/ML based analysis and optimizations.

Importantly, as interoperability standards and testing mature, forecasts predict that Open RAN deployments will gain momentum after 2025, ultimately leading to an estimated 1.3 million Open RAN cell sites by the end of the decade[1]. This momentum can only be achieved through Open RAN transitioning from early deployments that have focused on greenfield deployments into a technology that is widely adopted in brownfield deployments across all mobile network operator segments and geographies.

This technical paper, building on the groundwork laid by previous 5G Americas Open RAN publications, offers updates on the progress made by leading Open RAN standards bodies, the latest advancements in multi-vendor interoperability, and current market deployments. From a standardization standpoint, the technical paper delves into recent developments in Open RAN architecture, security, and architectural elements such as the RAN Intelligent Controllers (RICs).

In this paper, we focus on the recent updates to the O-RAN architecture, including decomposition of the SMO with individual SMO functions integrated within a SBA. The R1 interface has been introduced, which allows the Non-RT RIC to expose information to consuming rApps that perform RAN optimization. From a Near-RT RIC perspective, the role of xApp APIs has been described, enabling xApps to be fully decoupled from the Near-RT RIC platform. Finally, new UE ID capability is described, allowing correlation of events by xApps and rApps and RAN optimizations to be performed on a per-UE basis.

Other recent specification updates are detailed, including use-case updates to improve the performance of Multi-User and Massive MIMO deployments. With spectrum efficiency being a key performance indicator for the RAN, the latest O-RAN specifications have defined new MIMO features for grid-of-beams and non-grid-of-beams optimizations. Advancements in radio resource management are introduced, including introduction of the RAN-Specific Network Slice Subnet Management Function that enables slicing SLA use cases to be realized. O-RAN's shared O-RU capability is introduced, enabling a neutral host to partition the shared O-RU's carrier resources between separate MNO tenants, with each MNO operating carriers using their own dedicated spectrum, and role-based access control permitting those MNO tenants to only configure and receive performance data from their own partitioned resources.

We have also covered advances related to the O-RAN security and architecture. Building on earlier papers that have introduced the activities of O-RAN Working Group 11, updates are provided concerning O-RAN threat modeling, analysis and remediation. Furthermore, updates to the security protocols are described, including mandatory use support of IEEE 802.1X port-based network access control to protect the Open Fronthaul interfaces. ZTA principles related to O-RAN are also detailed. Whereas the RAN was previously considered as a trusted environment, O-RAN is leading the introduction of ZTA into the RAN, ensuring that there is no implicit trust of a

RAN service producer, consumer or RAN asset based upon physical location, network location, or ownership.

The paper describes updates to the RIC and SMO domains. Architectural updates to the RIC are introduced, including the publication of Near-RT-RIC APIs, enabling 3rd party xApps to be hosted on different Near-RT RIC platforms. From an interface perspective, the Y1 interface is described, enabling service to easily consume RAN analytics, as well as the R1 interface that enables rApps to be decoupled from the Non-RT RIC platform functionality. Finally, updates are described that focus on the testing of the multi-vendor interoperable RIC architecture. O-RAN test specifications for the E2 interface are described, including conformance testing requirements to ensure full multi-vendor interoperability between E2 nodes (O-CU CP, O-CU UP, O-DU, O-eNB) and the Near-RT RIC platform.

Continuing the theme of multi-vendor interoperability, the paper reports on the recently announced O-RAN Certification and Badging Program, describing the differences between O-RAN defined certification, IoT badging and E2E badging. Current O-RAN testing programs are described as well as reports of products that have completed Open Fronthaul certification. Complementing O-RANs Certification and Badging, the paper describes TIP's Open RAN System Certification Process and how this is focused on testing of complete RAN systems that may include non-O-RAN components, as well as certification of system integration aspects such as Open RAN configuration and optimization.

Recognizing that Open RAN is the fastest growing segment in the RAN market, but also its smallest, the paper describes progress in both greenfield and brownfield deployments. As interoperability standards and testing mature, operator sentiment is recited, indicating forecasts of large-scale deployments from 2025. This aligns with industry analysis that is forecasting Open RAN deployments gaining momentum after 2025, ultimately leading to an estimated 1.3 million Open RAN cell sites by the end of the decade.

Finally, the foundation of this technical paper is represented by specifications published by O-RAN ALLIANCE in June 2023. However, 5G Americas recognizes that there is significant interest in more recent specification developments which are still work in progress. These topics are covered in the appendix and highlight the continued innovation that is occurring across the Open RAN industry.

1. Introduction

The Open RAN industry is dynamically evolving, transitioning from closed, monolithic architectures to open architectures that are based on the decomposition of physical and virtual functions, supported by interoperable interfaces that enable multi-vendor deployments. This evolution is being fueled by the on-going efforts of the Open RAN industry bodies that are defining and refining Open RAN interfaces and specifications, as well as driving multi-vendor interoperability to enable market deployments. While encouraging competition among vendors, open RAN simultaneously drives supply chain diversification. This same broadening of the RAN ecosystem opens up innovation opportunities. Simultaneously, Open RAN delivers both a simplified network management, that is now standardized across multiple vendors, as well as being highly scalable through the use of cloud-native operations. Finally, Open RAN facilitates data accessibility, enabling AI/ML based analysis and optimizations.

This technical paper provides insights to updates to the Open RAN architecture, specifications, and interoperability testing. Given the dynamic nature of the Open RAN environment, together with the succession of specification updates from the O-RAN ALLIANCE, there continues to be significant work in advancing Open RAN standards. The scope of the material used has been restricted to documentation publicly available as of June 2023, and available for download from https://www.o-ran.org/specifications.

The paper builds on the groundwork laid by previous 5G Americas Open RAN publications. Sections are dedicated to Open RAN standards and specifications, the RAN Intelligent Controllers (RICs), newer interfaces defined in O-RAN ALLIANCE, multi-vendor interoperability, and market deployments. Each section begins with brief summary of material from earlier 5G Americas publications and then offers insights into recent updates since the publication of these earlier papers.

Regarding Open RAN platforms, previous 5G Americas Open RAN papers have highlighted the critical role of selecting the correct hardware platform, hardware acceleration and virtualization environment or Cloud OS[2] [3]. Both “inline” and “lookaside” hardware acceleration approaches have been introduced. While there have been some recent updates from the O-RAN ALLIANCE related to hardware platforms, e.g., including enhancements to defining acceleration abstraction[4], this paper does not provide further detail of recent updates related to Open RAN platforms.

While the foundation of this white paper is represented by specifications published by O-RAN ALLIANCE in June 2023, 5G Americas recognizes that there is significant interest in more recent specification developments which are still work in progress. These topics are covered in an informative annex and highlight the continued innovation that is occurring across the Open RAN industry.

2. Open RAN Standards and Specifications

2.1 Introduction

This is the third technical paper from 5G Americas addressing Open RAN. The first technical paper covering the topic was the 2020 paper "Transition Toward Open and Interoperable Networks", which introduced the various ecosystem bodies involved with Open RAN as well as reviewing early operator trials. Building on this foundation was 5G Americas second paper on Open RAN, entitled "The Evolution of Open RAN", which provided updates that covered interoperability of multi-vendor open interfaces, advancements by the O-RAN ALLIANCE and Telecom Infra Project, and enhancements dealing with virtualization and cloudification of RAN functions.

The remainder of this section builds on these foundations, describing recent updates to the Open RAN architecture and specifications since the publication of these earlier papers.

2.2 O-RAN Architectures

Open RAN is the evolution of traditional RAN, in which the hardware and software are decoupled, and disaggregated RAN network functions (NFs) are implemented as cloud native functions (CNFs) to run on top of cloud infrastructure. Intelligent automation in Open RAN is realized using Artificial Intelligence and Machine Learning (AI/ML). As stated by the United States' Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) Report on Open RAN, "Open RAN is O-RAN, Cloud RAN, vRAN, and other technologies"[5].

O-RAN is the Open RAN architecture specified by the O-RAN ALLIANCE to make the RAN open, intelligent and fully interoperable through the specification of new interfaces and automated through the Service Management and Orchestration (SMO) and RAN Intelligent Controllers (RICs) containing AI capabilities with xApps and rApps. The O-RAN architecture specifies the following new open interfaces: A1, E2, O1, O2, R1, Y1, Open Fronthaul (OFH) CUS-Plane, and OFH M-Plane.

The O-RAN ALLIANCE defines O-Cloud as a cloud computing platform comprising a collection of physical infrastructure nodes that meet O-RAN requirements to host the relevant O-RAN functions (i.e., Near-RT RIC, O-CU-CP, O-CU-UP, and O-DU), the supporting software components (such as Operating System, Virtual Machine Monitor, Container Runtime, etc.) and the appropriate management and orchestration functions.

The O-RAN architecture is described further in the O-RAN Architecture Description (OAD) document[6] and is illustrated in Figure 1.

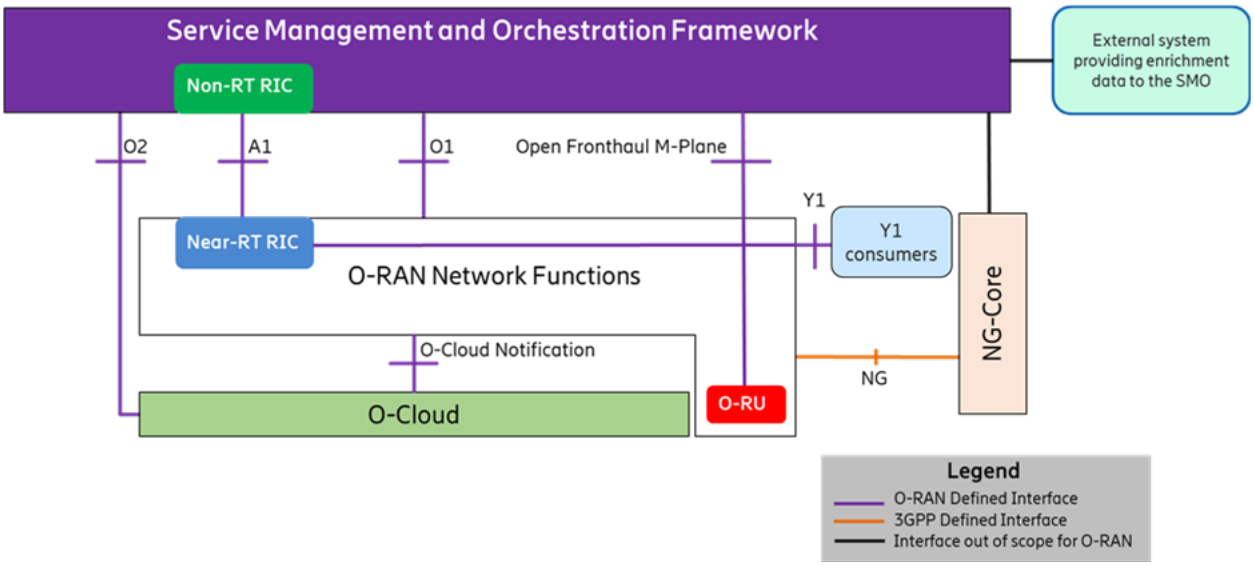
2.3 Recent Updates to Open RAN Architectures

This section describes a selection of recent and significant updates to Open RAN Architectures.

Clarification of interface between SMO and O-RU

Figure 1 illustrates that all the O-RAN NFs, except the Open Radio Unit (O-RU), are expected to be managed via the O1 interface when interfacing the SMO Framework. The Open Fronthaul M-Plane interface, between SMO and O-RU, is designed to support the O-RU management in the hybrid model as opposed to the hierarchical model where there is no direct management connection to the O-RU in a hierarchical-mode lower layer split.

Figure 1: O-RAN Architecture (source: O-RAN Architecture Description)



Service Management and Orchestration (SMO) Service-Based Architecture (SBA)

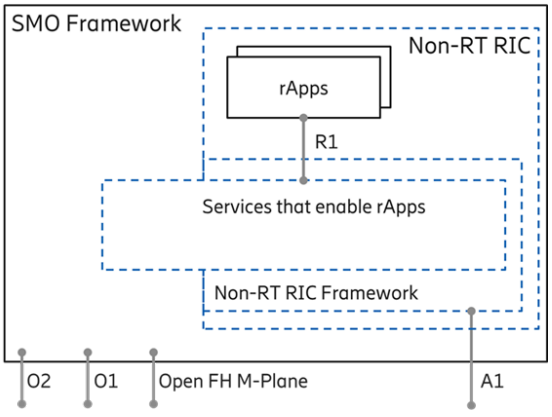
The O-RAN Service Management and Orchestration (SMO) is responsible for RAN domain management and provides SMO services that support the RAN. The SMO is built upon a Service Based Architecture (SBA) where SMO are SMO Services (SMOS) offered by SMO for the following capabilities:

- FCAPS services for O-RAN Network Functions
- Non-RT RIC Services for RAN optimization
- O-Cloud Resources Management and Orchestration Services

The SMO services are provided to the RAN through four interfaces:

- **AI Interface** is used for optimization of the RAN between the Non-RT RIC and the Near-RT RIC
- **O1 Interface** is an OAM interface that provides FCAPS support to O-RAN Network Functions. FCAPS support for the O-RU can be provided via the O1 interface with using the hierarchical model for managing O-RUs
- **Open FH M-Plane Interface** is used to provide FCAPS support to the O-RU when using the hybrid model for managing O-RUs
- **O2 Interface** provides management of the O-Cloud infrastructure resources, workload deployments and OAM of the O-Cloud platform.

Figure 2: SMO Architecture (source: O-RAN Architecture Description)



R1 Interface

The Non-Real-Time RAN Intelligent Controller (Non-RT RIC) involves functionality internal to the SMO to support intelligent RAN optimization by providing policy-based guidance, ML model management, and enrichment information via the A1 interface to the Near-RT RIC. The Non-RT RIC can utilize data analytics and AI/ML techniques to determine the RAN optimization actions which can be applied through O1 and O2 interfaces, via SMO services. Non-RT RIC Applications (rApps) are modular applications that leverage the functionality exposed by the Non-RT RIC framework to perform RAN optimization and other functions. The R1 interface is internal to Non-RT RIC, and the services exposed by Non-RT RIC framework over this interface enable rApps to obtain information to trigger intelligent policy and RAN optimization actions. The R1 interface is also used by rApps to share authorized enrichment information with Near-RT RIC and share services and analytics within Non-RT RIC.

xApp APIs

The O-RAN architecture has standardized and defined APIs, which continue to evolve for interfacing between the xApps in the Near-RT RIC and the platform functions of the Near-RT RIC. The APIs are defined to enable an xApp to:

- register itself to the Near-RT RIC platform;
- discover the APIs and the services produced by the platform;
- subscribe and receive notifications about updates to APIs and services produced by the platform;
- access the database/data lakes facilitated by the platform;
- communicate with the subscription management function toward generating subscriptions for accessing RIC services produced by the E2 nodes, such as the O-CU-CP, O-CU-UP, O-DU and O-eNB;
- receive indication message notifications from the E2 nodes via the platform; and
- generate control actions toward the E2 nodes.

xApp APIs are also evolving toward enabling an xApp to access data management and AI/ML services offered by the Near-RT RIC platform.

SMO External Interfaces

The O-RAN architecture also includes SMO external interfaces, which are the interfaces between the SMO and SMO external systems used to import AI enrichment from data sources outside the O-RAN domain to the SMO.

Y1 Interface

The Near-RT RIC provides RAN analytics information services via the Y1 service interface to be consumed by Y1 consumers. The Y1 consumer is “role-played” by entities that are either internal or external to the Public Land Mobile Network (PLMN) trust domain that consumes Y1 RAN analytics information produced by the Near-RT RIC. The services can be consumed by Y1 consumers after mutual authentication and authorization by subscribing to or requesting the RAN analytics information via the Y1 service interface.

User Equipment ID Support in O-RAN Architecture

The Non-RT RIC and Near-RT RIC enable intelligent RAN optimization via A1, O1 and E2 interfaces respectively. To support intelligent RAN optimization, the Non-RT RIC with rApps and Near-RT RIC with xApps utilize the knowledge of different User Equipment (UE)-associated events reported by the O-RAN functions over E2 and O1 interfaces. Both the Non-RT RIC and Near-RT RIC may need to correlate different UE-associated events reported by the O-RAN functions for the same UE.

To facilitate this correlation task, the reporting O-RAN function includes a set of UE-associated identifiers with any reports that contain UE-specific information. Defined UE-associated identifiers are reported by O-RAN functions over O1 and E2 interfaces for any UE-associated information. The Non-RT RIC and Near-RT RIC may initiate messages toward the O-RAN functions which are associated with specific UEs. In such cases, the Non-RT RIC and Near-RT RIC may include one or more of the UE- associated identifiers with any UE-associated messages over A1 and E2 interface for identification of the UE in the O-RAN functions.

O-Cloud Notification API

The O-Cloud Notification Interface allows event consumers such as an Open Distributed Unit (O-DU) deployed on O-Cloud to subscribe to events/status from the O-Cloud. The cloud infrastructure will provide event producers to enable cloud workloads to receive events/status that might be known only to the infrastructure.

2.4 Small Cell Forum (SCF) Option 6 Architecture Split

Small Cell Forum publishes functional application platform interface (FAPI) together with the nFAPI defined transport wrapper, targeted at establishing interoperability and

reducing the cost and risk in deploying virtualized RANs and small cells. The 5G nFAPI specification [7] defines the functional split between the 5G MAC and PHY functions that enables virtualization of the MAC and higher layer functions. In contrast to other lower layer split options, split 6 involves reduced bandwidth requirements, which means high quality fiber is not required to link every DU and RU.

Compared to earlier LTE versions that focused on the P5 physical layer control and the P7 data interfaces, the 5G FAPI specification also defines the P19 frontend control interface, enabling fast, dynamic control of the digital front end and analog beamforming functionality. In contrast to its first release that focused on IP based transports, 5G nFAPI introduces Ethernet transport, re-using the eCPRI protocol together with vendor specific message types to transport nFAPI messages.

Finally, the earlier LTE version on nFAPI had a TR-069 based PNF management object specified in SCF167 [8], describing how an independent neutral host provider can use the specified management object to operate the PNF and partition/slice resources between multiple operators. Instead of TR-069, 5G FAPI supports the P9 interface (defined in [SCF229]), which describes a NETCONF-based/ YANG framework to configure the O-RAN 7.2x Fronthaul interfaces for inline accelerators, using externally defined YANG data models.

2.5 Recent Updates to Standards and Specifications

MU-MIMO and Massive MIMO

The O-RAN ALLIANCE has been evolving use cases related to optimizing the Massive Multiple Input Multiple Output (MIMO) feature in 5G networks and beyond, with a focus on improving the network KPIs of the RAN in areas such as spectral efficiency.

In particular, the O-RAN ALLIANCE has defined use cases related to optimizing the grid-of-beams (GoB) and non-grid-of-beams (Non-GoB) MIMO feature. GoB involves forming a virtual grid within the geographical area of cell coverage and transmission of reference Synchronization Signal Block (SSB) beams across the grids, thereby enabling the UEs to measure their signal strengths with respect to the SSB beams for enhancing connectivity and beam-based mobility robustness (bMRO optimization).

Also, UE-level data transmission is based on UE specific beamforming involving the Channel State Information–Reference Signal (CSI-RS) measurements involving the individual UEs. GoB beamforming optimization is used primarily in FDD bands. Non-GoB MIMO feature does not involve formation of virtual grids, but leverages the Sounding Reference Signal (SRS) feedback from the UE in the uplink toward determining the UE specific beamforming weights for downlink and uplink data transmissions. SRS is primarily used in Time-Division Duplex (TDD) based systems that leverage channel reciprocity between the uplink and downlink channels.

O-RAN ALLIANCE has particularly focused on optimizing the SSB periodicity, SSB duration, number of reference beams within an SSB duration, UE specific beamforming weights, UE specific number of layers, number of UEs within an MU-MIMO spatial group, etc., using service models such as the E2 Service Model for RAN Control (E2SM-RC), defined in O-RAN ALLIANCE Working Group 3.

Slicing Service Level Assurances

The O-RAN ALLIANCE has also defined optimizing radio resource allocation mechanisms related to slicing. This work will go towards guaranteeing service level assurances for individual slices, thereby enhancing not only the network's Quality-of-Service (QoS) but also the UE's Quality-of-Experience (QoE).

In particular, the O-RAN ALLIANCE has focused on slicing architecture in terms of realizing the RAN-specific NSSMF (Network Slice Subnet Management Function) within the SMO toward managing the network slice subnet instances. The O-RAN ALLIANCE has also focused on optimizing the Radio Resource Management (RRM) policies in terms of Data Radio Bearer (DRB) Management, Physical Resource Block (PRB) allocation, and number of Radio Resource Control (RRC)-connected UEs for individual slice instances. Optimizing the RRM policy in terms of minimum, maximum and dedicated radio resources to be allocated from a given cell and to each UE for individual slices from the O-DU has evolved into service models, such as E2 Service Model: Cell Configuration and Control (E2SM-CCC) and E2SM-RC (from O-RAN ALLIANCE Working Group 3), and data models in the O-RAN ALLIANCE.

Shared Open Remote Unit (O-RU)

While much of the focus on Open RAN has been on the transformation of the macro network, the compelling case for multi-vendor interoperable Open RAN must include supporting those indoor and rural deployments that necessitate multi-operator capability. Published in August

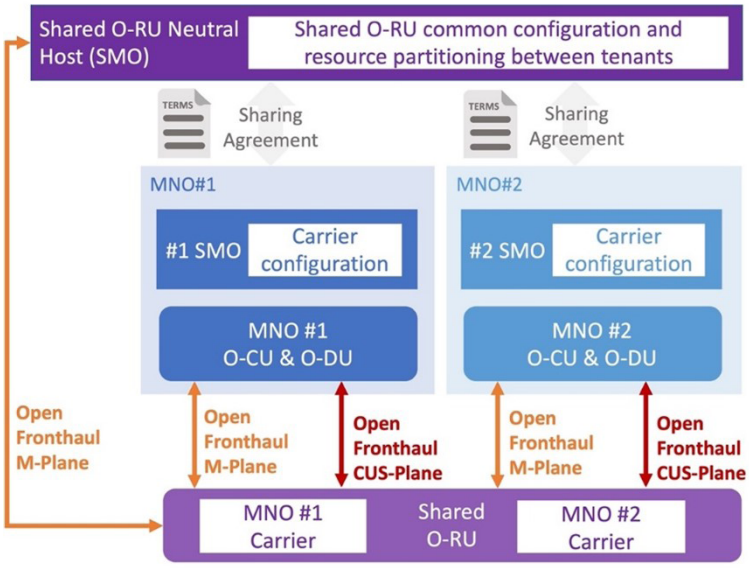
2022, O-RAN Fronthaul version 10[9] saw the introduction of the newly defined “shared O-RU” functionality, enabling the accelerated deployment of shared multi-operator networks, using fully standardized O-RUs.

Different established sharing approaches all face key challenges. Multi-Operator Core Networks (MOCN) simplify the RAN functionality but is operationally complex as exclusively licensed spectrum needs to be shared. Multi-Operator Radio Access Networks (MORAN) simplify operations as each Mobile Network Operator (MNO) uses their own spectrum but adds complexity to the base station. Distributed Antenna Systems (DAS) simplifies interoperability based on attenuated RF interfaces but is complicated by having to bring multiple base stations into the enterprise’s communications room. While shared small cell physical network functions (PNF) simplifies the radio unit but does not define how different operators can configure separate nFAPI service instances.

O-RAN’s newly introduced shared O-RU capability offers the best of all worlds; a simplified O-RU, fully specified multi-vendor interoperability enabling integration with separate MNO remote O-DUs, transport over a packet-based fronthaul network, OAM functionality that enables an enterprise or neutral host to partition the shared O-RU’s carrier resources between separate MNOs with each MNO operating carriers using their own dedicated spectrum, and role based access control permitting those MNOs to only configure and receive performance data from their own partitioned resources.

Figure 3 illustrates one deployment scenario where a neutral host is using the hybrid management model to configure the common shared O-RU aspects while enabling separate MNOs, or tenants, to configure their individual carriers.

Figure 3: O-RAN Shared O-RU operated by a neutral host offering service to two MNOs (source: Cisco)



3. Securing the Open RAN

3.1 Introduction

Previous 5G Americas Open RAN reports have introduced the O-RAN Working Group 11 that is responsible for specifying O-RAN security requirements as O-RAN strives toward a zero-trust architecture (ZTA). The process of threat modeling has been introduced, as well as listing security work items such as security logging and O-RAN's certificate management framework, among others.

The primary objectives of the O-RAN ALLIANCE encompass achieving a secure, open, and interoperable Radio Access Network (RAN). By leveraging security advancements from established standards development organizations such as Third Generation Partnership Project (3GPP) and Internet Engineering Task Force (IETF), O-RAN has developed an O-RAN security architecture designed to enable 5G Communication Service Providers (CSPs) to deploy and operate O-RAN with equal or greater confidence compared to a 3GPP-specified RAN. The O-RAN specifications enhance the security posture by outlining security requirements and controls that effectively mitigate risks across the attack surface, in line with the goals of a Zero-Trust Architecture (ZTA).

This section delves into the inherent security benefits of O-RAN, potential threats, attack surface, and the implementation of security controls to mitigate risks.

3.2 O-RAN Security Architecture

The O-RAN security architecture is based upon the following three O-RAN technical specifications maintained by WG11:

- Security Protocols Specifications[10]
- Security Requirements Specifications[11]
- O-RAN Security Threat Modeling and Remediation Analysis[12]

The test cases to verify proper security implementation of O-RAN security architecture is specified in the O-RAN Technical Specification:

- O-RAN Security Tests Specifications[13]

The threat modeling and risk analysis is used to inform the security requirements and security controls in the Security Requirements Specifications. The O-RAN Threat Modeling and Remediation Analysis document considers external and internal threats to achieve a ZTA. In addition, WG11 maintains security analysis Technical Reports (TRs) for O-RAN network functions and features. These TRs help to drive the requirements in the O-RAN security requirements specification.

3.3 O-RAN Security Benefits and Risks

O-RAN's openness and disaggregated architecture provide the following inherent tradeoffs for security benefits and risks:

- Open-source software
  - » Benefit: Open-source software enables transparency and common control
  - » Risk: Open-source software can be exploited by malicious threat actors

- Open interfaces:
  - Benefit: Open interfaces ensure use of and interoperability of secure protocols and security features
  - Risk: Open interfaces need to have proper security specifications based upon risk analysis
- Disaggregation:
  - Benefit: Disaggregation enables supply chain security through diversity
  - Risk: Disaggregation enables a multi-vendor environment in which the security posture meets the weakest implementation
- Intelligence:
  - Benefit: Increased visibility enables enhanced intelligence leveraging AI and ML.
  - Risk: AI/ML is a known attack vector that needs to have proper security specification in O-RAN.

3.4 O-RAN Threat Analysis

The foundation of security is the threat analysis, which includes identification of threats, attack surface, assets, and stakeholders. The O-RAN architecture includes new interfaces and architecture elements, expanding the attack surface to introduce new security risks. The expansion of the Open RAN attack surface has been acknowledged in reports from the United States National Security Agency's 'Enduring Security Framework' [14] and the Federal Communications Commission's Communications Security, Reliability, and Interoperability (FCC CSRIC) VIII Workgroup 2[15] and European regulators National Cyber Security Centre U.K.[16], Federal Office for Information Security (BSI) Germany[17], and EU NIS Cooperation Group[18].

The O-RAN Threat Modeling and Remediation Analysis document has identified over 125 threats unique to O-RAN, as of version 6.0. Unique threats against the O-RAN system can be grouped into six categories:

- **Architectural threats**, including functions, interfaces, and protocols, as listed below:
  - **Additional O-RAN architecture elements**: SMO, Non-RT RIC (including rApps), and Near-RT RIC (including xApps).
  - **Additional O-RAN open interfaces**: A1, E2, O1, O2, R1, Y1, and Open FH (7-2x).
- **Cloud threats**, including O-Cloud, cloud hardware and software infrastructure.
- **Supply chain threats**, including use of open-source software.
- **Protocol threats**, includes known vulnerabilities to IETF-specified protocols and APIs based upon IETF-specified frameworks.
- **AI/ML threats**, targeting AI/ML used across O-RAN and external data sources.
- **Physical threats**, which are considered outside the scope of O-RAN.

It is important to also assess the additional elements of the Open RAN attack surface that are shared with other domains of the 5G network. This includes hybrid cloud deployments, cloud native technologies, APIs, and AI/ML. While these attack vectors could be relevant for any cloud deployment, a higher level of due diligence is needed for the deployment of 5G critical infrastructure in the private, public, and hybrid cloud to achieve a Zero-Trust Architecture (ZTA) that provides protection from external and internal threats, which can mitigate risk of reconnaissance and lateral movement. These additional attack vectors and security controls specifications are currently being addressed in O-RAN ALLIANCE WG11 O-Cloud Security and AI/ML security work item teams. FCC CSRIC VIII WG3 identified risks and recommended mitigations for 5G virtualization[19], which is also applicable to Open RAN.

As the O-RAN ALLIANCE continues to evolve the O-RAN architecture, WG11 is conducting security analysis of new functions and interfaces and specifying new security requirements with consideration of external and internal threats to achieve a ZTA. The following O-RAN enhancements are part of WG11's security analysis:

- RAN Analytics Information Exchange (RAIE)
- RAN-Core data sharing
- Shared O-RU

3.5 O-RAN Security Protocols

O-RAN technical specifications[9] [10] provide specifications for configuration and cipher suites with use of the following security protocols on O-RAN interfaces to ensure confidentiality, integrity, availability, and authenticity: SSHv2 (Secure Shell 2.0), TLS 1.2 and 1.3, DTLS (Datagram Transport Layer Security) 1.2, IPsec (Internet Protocol Security), OAuth 2.0, CMPv2, IEEE 802.1X, and NETCONF (Network Configuration Protocol) over Secure Transport.

For further information about configuration and use of O-RAN security protocols see the "Security Protocols Specifications" document[12]. Details about where these protocols are used in O-RAN architecture to enforce confidentiality, authenticity, integrity, and least privilege are specified in the "Security Requirements Specifications" document[11]. O-RAN also provides requirements for SBOM (Software Bill of Materials)[11].

3.6 Considerations for a Zero Trust Architecture

O-RAN is following 3GPP security design tenets and industry best practices working toward the guiding principle of a ZTA, so that O-RAN delivers the level of security expected by 5G network operators and users. Internal and external threats are considered in a ZTA, as defined in the National Institute of Standards and Technology NIST) special publication 800-207[20]. Traditionally, the RAN was considered trusted, but ZTA assumes there is no implicit trust of a user or asset based upon physical location, network location, or ownership.

The O-RAN ALLIANCE has specified the security requirements[13] to include these protocols on external and internal interfaces, consistent with a ZTA:

- Transport Layer Security (TLS) 1.2 and 1.3 for confidentiality and integrity protection.
- Mutual TLS (mTLS) versions 1.2 and 1.3 with PKI-based X.509 certificates for mutual authentication.
- Certificate Management Protocol version 2 (CMPv2) for certificate management.
- OAuth 2.0 for authorization.
- NETCONF Access Control Model (NACM) for authorization.
- Mandatory support of IEEE 802.1X port-based network access control on Open FH.
- Network function robustness against volumetric DDoS attacks.
- Life cycle management for network functions and applications.
- Security event logging.
- Signed and protected Software Bill of Materials (SBOM).

The O-RAN ALLIANCE is continuing to pursue a ZTA as the O-RAN architecture, threats, and controls evolve. Alliance for Telecommunications Industry Solutions (ATIS) is currently addressing ZTA in 5G with North American mobile network operators and vendors and has issued its first report[21].

4. RAN Intelligent Controller & Service Management and Orchestration

4.1 Introduction

Previous 5G Americas Open RAN papers have described how O-RAN has adopted a service-based architecture for the Near-RT RIC, Non-RT RIC, and SMO functions, allowing functions to produce services and exposing capabilities over a services-based interface for 3rd party rApps and xApps to consume. These services are registered in a services registry, from which xApps and rApps can discover the services they need through the O-RAN WG3-defined xApps APIs and rApps APIs defined by O-RAN WG2.

The Near-RT RIC architecture has also been previously described, including detailing platform functions for analytics and AI/ML. These functions include a Data Pipeline for data ingestion and preparation for xApps, training for generic ML models used by multiple O-RAN use cases, and a messaging infrastructure with standardized APIs for multi-vendor interoperability. It also includes Y1 termination, an interface which exposes RAN analytics information to Y1 consumers.

4.2 Recent Updates to RAN Intelligent Controller (RIC) & Service Management and Orchestration

Near-RT-RIC APIs[22]

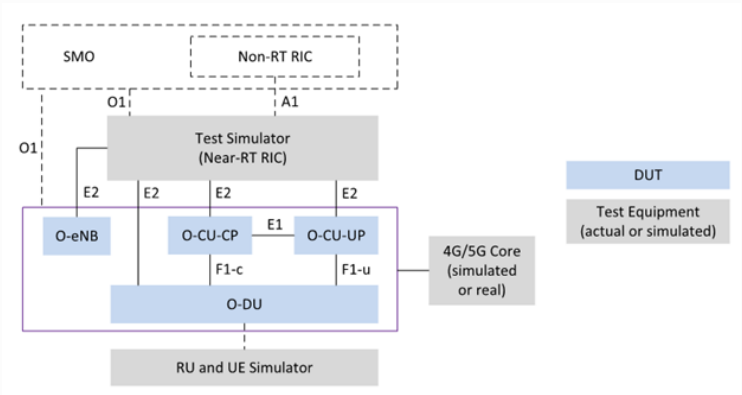
The Near-RT RIC APIs are a collection of well-defined interfaces providing Near-RT RIC platform services. These APIs define the different types of information flows and data models. The Near-RT RIC APIs are essential to host 3rd party xApps in an interoperable way on different Near-RT RIC platforms. Near-RT RIC provides the following Near-RT RIC APIs for xApps:

- **A1 related APIs:** APIs allowing access to A1 related functionality
- **E2 related APIs:** APIs allowing access to E2 related functionality and associated xApp Subscription Management and Conflict Mitigation functionality
- **Management APIs:** APIs allowing access to
- **SDL APIs:** APIs allowing access to Shared Data Layer related functionality
- **Enablement APIs:** APIs between Apps and API enablement functionality

Y1 interface

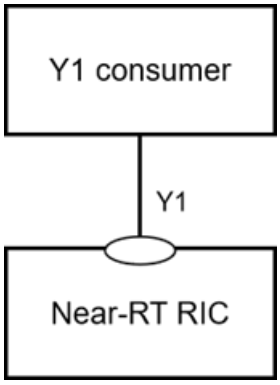
The Y1 interface general architecture and principles have evolved to support the Y1 interface for analytics, as shown in Figure 4 below.

Figure 4: E2 conformance testing for E2 nodes (Source: O-RAN ALLIANCE)



The Y1 interface is an open logical interface that enables services to be accessed by authorized consumers. Preliminary services and operations for the Y1 interface is defined, by means of which the Y1 service consumer can subscribe to receiving notifications/streaming from the Y1 service producer, and the Y1 service consumer can query for RAN analytics information from the Y1 service producer.

Figure 5: Y1 interface general architecture



The subscribe service operation enables an authorized Y1 services consumer to subscribe to the Y1 services producer for receiving notifications pertaining to RAN analytics, and the unsubscribe service operation enables the Y1 service consumer to unsubscribe to notifications from the Y1 services producer. And the query service operation enables the Y1 services consumer to query the Y1 services producer for desired RAN analytics information.

R1 (Non-RT RIC) interface APIs

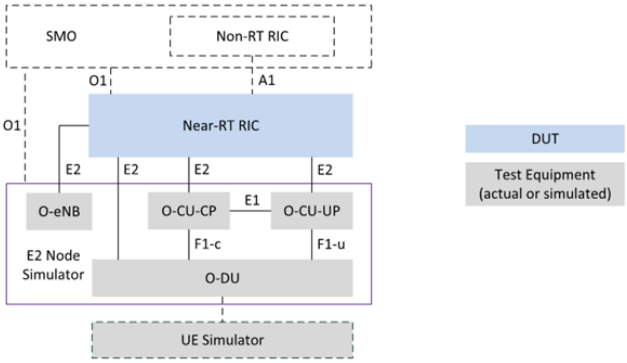
The R1 application protocol procedures and the relevant APIs for the messages have been defined for enabling the interfacing between the rApps and the Non-RT RIC framework. All interaction between the rApps and the Non-RT RIC framework occur through the R1 interface. As an example, rApps use the Service Registration API to register the services they produce with the Non-RT RIC framework, and the Services Discovery API to discover the registered services. The rApps use the subscription API to subscribe to event-based notifications involving the services and the APIs that expose the services.

Similar to service management APIs, R1 interface has also defined APIs for data management in terms of registering the data types produced by the rApps, discovering the data types produced by the framework for the rApps, accessing the data produced by the framework, and transferring/ delivering data using Push or Pull mechanisms.

Test specification updates

Test methodologies and test cases are defined for the E2 interface between the Near-RT RIC and the E2 nodes. The test methodologies include: (i) conformance testing, and (ii) interoperability testing. The test configuration for E2 conformance testing of the Near-RT RIC as the device under test (DUT) is shown in Figure 5 and the test configuration for E2 conformance testing of the different types of E2 nodes as DUT is shown in Figure 6. Conformance testing has been defined for E2 Application Protocol (E2AP) procedures to test whether the behavior of the DUTs are conformant to the expected behavior mandated in the E2AP specifications. Interoperability test cases have also been defined for these E2 procedures to test the interoperability of the E2AP procedure. Test tools such as protocol analyzer, a TAP interface and device log collector tools are used to evaluate the test cases and specifications.

Figure 6: E2 conformance testing for Near-RT RIC (Source: O-RAN ALLIANCE)



5. Multi-Vendor Interoperability

5.1 Introduction

Previous 5G Americas Open RAN papers have described the plugfests conducted by the O-RAN ALLIANCE to demonstrate multi-vendor interoperability. Highlights of such plugfests have included the demonstrations of interoperability in Open Fronthaul implementations, Near-Real-Time RIC and Non-Real-Time RIC, O-Cloud products, integration of O-RAN network functions with the O-Cloud platform, security tests, and advanced use cases utilizing O-RAN specifications. TIP's Test and Integration Project Group is focused on defining and accelerating the development of test materials, test plans, and other documents for testing, compliance and interoperability of OpenRAN systems.

5.2 Recent Updates

In April 2023, the O-RAN ALLIANCE announced the O-RAN Certification and Badging Program, operated by the Open Testing and Integration Centers (OTICs)[23]. Certification and Badging of O-RAN solutions ensures confidence in the O-RAN solutions for both operator and vendor communities. O-RAN Certificates and Badges are issued by OTIC (Open Testing and Integration Center).

- O-RAN certifications validate and certify that a vendor product is compliant to a related set of O-RAN defined interface specifications through a set of O-RAN defined conformance tests.
- O-RAN IoT badging proves interoperability of a pair of products based on a set of baseline features and parameters through a set of O-RAN defined interoperability tests. Optionally, optional/advanced features can be tested.
- O-RAN End-to-End (E2E) Badging proves interoperability of a group of products using O-RAN interfaces based on E2E test specifications.

The certification and interoperability procedures are defined O-RAN ALLIANCE Test and Integration Focus Group Certification and Badging Processes and Procedures[24]. The current certification procedures cover off the O-RAN Open Fronthaul Control, User, Synchronization and Management plane aspects allowing O-DU and O-RU equipment to be certified. The current interoperability procedures include Open Fronthaul as well Xn, X2 and F1-C interfaces. The current end-to-end system test procedures [25] include functional tests related to the O-RAN architecture, such as inter-O-DU and inter-O-CU mobility as well as optional security assurance tests to prevent fronthaul control and synchronization plane denial of service attacks.

The current list of certified and badged products is available on the O-RAN website (https://www.o-ran.org/testing-integration). As of July 2023, this list indicates that eight products have successfully received Open Fronthaul certification, one pair of products have received the Open Fronthaul IoT badge, and one complete system has received the End-to-End Badge.

5.3 Open RAN System Certification Process

TIP's Open RAN System Certification Process (SCOPE) [26] is designed to create structural efficiencies within the RAN supply chain, enabling operators and vendors to streamline efforts and reduce the complexities inherent in the integration and testing of carrier-grade Open RAN.

SCOPE builds on O-RAN OTIC testing delivers product conformance and interface testing to focus on delivering certification of subsystems in full Open RAN solutions. Non-functional

requirements including performance, security, operability, and stability are covered as well as “negative” testing to ensure Open RAN solutions perform consistently in unexpected circumstances.

5.4 NTIA 5G Challenge

From April 2022, the National Telecommunications and Information Administration (NTIA) has run its “5G Challenge” competition. This aims to accelerate the adoption of 5G open interfaces, interoperable subsystems, secure networks, and multi-vendor operability. The 2022 event showcased successful network integrated subsystems from five different vendors: user equipment (UE), radio unit (RU), distributed unit (DU), central unit (CU), and Core.

In 2023, the challenge continues with focus on the O-RAN interface Open Fronthaul (DU to RU) based on lower layer functional split “7-2x” as well as the 3GPP defined Xn interface that will be used to demonstrate mobility/handover between CU equipment for different vendors.

6. Market & Deployments

6.1 Introduction

Previous 5G Americas Open RAN papers have detailed deployments by various mobile operators. British Telecom (BT) announced a trial with RIC installed across multiple sites, Deutsche Telekom (DT) has implemented O-RAN in Germany, and Telecom Italia (TIM) has introduced the first 5G Open RAN standalone connection. Rakuten has built a fully virtualized, cloud native network and Vodafone is building a virtualized RAN environment. Telefónica has deployed Open RAN trials for 4G LTE and 5G in several countries and has built an Open RAN network in one country, plus validated a 5G Open RAN "all-in-one" small cell.

Bharti Airtel, India's Tier-I mobile network operator, plans to deploy 10,000 cell sites based on Open RAN in rural areas, with an initial deployment of 2,500 cell sites before scaling up.

6.2 Recent Deployment Updates

Since the publication of the last technical paper from 5G Americas, there has been significant progress in Open RAN deployments. This section provides example public references of deployments of open RAN technology that were available in August 2023. Importantly, these references indicate the increasing recognition that it is now not a question of if Open RAN will be deployed, but rather when and how much. While Open RAN is the fastest growing segment in the RAN market, it is also the smallest. Barriers to adoption are increasingly being addressed, including feature parity, performance and system integration efforts.

The real time status of Open RAN globally can be seen from the O-RAN map https://map.o-ran.org as maintained by the network operators of the O-RAN alliance.

In 2022, GSMA's Mobile World Live surveyed executives from 119 global network operators[27]. The results indicate a strong majority of surveyed operators (81%) say they have O-RAN on their network technology roadmaps. More than half (57%) expect to deploy it within the next two years. Implementation strategies vary, with the majority (74%) planning to use a RAN automation platform as part of their O-RAN architectures and nearly half (47%) planning to unify network management systems.

In February 2023, Tarek Amin, Rakuten Symphony's former CEO, was interviewed by TMN's Keith Dyer when they provided an update on deployment status from a greenfield deployment perspective[28]. Rakuten mobile's Open RAN deployment now approaches 60,000 macro base stations, over 12,000 5G base stations, and a massive number of enterprise small cells. There is nothing proprietary in any of Rakuten's interfaces, as all interfaces are open in the RAN and the Core. Rakuten has focused on system integration blueprints, delivering a system with interchangeable vendors.

In the same month, DISH Wireless announced the commercialization of the DISH 5G cloud-based Open RAN network. DISH's standalone 5G network is based on an Open RAN ecosystem[29]. The commercial service was deployed using virtualized RAN (vRAN) from two 5 Americas companies for 15K sites, 90k radios supporting the DISH unique spectrum and covering 75% of the US population.

In regard to brownfield deployments, U.K. telecommunications group Vodafone claimed it achieved the first commercial urban deployment of Open RAN (O-RAN) in Europe in late 2022, trialing the technology in two U.K. towns to provide mobile subscribers with data download rates of up to 700 Mbps[30].

In January 2023, KDDI announced that it had started commercial deployment of 5G Open vRAN sites in Japan[31]. The KDDI deployment uses virtualized CU (vCU) and virtualized DU (vDU) and radio units (MMU: Massive MIMO Units) interconnected using O-RAN ALLIANCE's Open Fronthaul Control and User Synchronization (CUS)-plane and M-Plane interfaces.

In February 2023, Deutsche Telekom announced its first commercial deployment of Open RAN with multiple partners[32]. Supporting 2G, 4G and 5G services, the solution focuses on open fronthaul based network deployment. Deutsche Telekom is partnered with several vendors for initial commercial deployments across its European footprint.

In regard to this deployment, Abdu Mudesir, Deutsche Telekom Group CTO & CTO Germany stated, "Open RAN has matured over the last months in both stability and performance, which has given us the confidence for an initial commercial deployment. . . we will use our collaboration as the springboard to accelerate Open RAN development and create a path to deployment at scale."

Both Vodafone and DT joined Orange, TIM and Telefónica at Mobile World Congress 2023 to announce that they are "ready for Open RAN by 2025"[33]. The operators reported that small trials were already in place, with new pilots to be announced during 2023 and larger scale deployments from 2025. This is a shift in the original schedule from the five operators that had originally targeted large scale roll out in 2022.

Michaël Trabbia, CTIO at Orange, said: "The significant progress made recently by the Open RAN industry has given us the assurance that open and cloud native RAN is now geared up for first commercial deployments in brownfield networks within Europe from 2023 onwards."[34]

In March 2023, AT&T announced that it had completed a trial of Near Real-Time RIC running xApps using O-RAN ALLIANCE's E2 interface specification[35]. The trial used E2SM (service model) policy services for dynamic RAN optimization.

Conclusion

The Open RAN industry is dynamically evolving, transitioning from closed, monolithic architectures to open architectures that are based on the decomposition of physical and virtual functions, supported by multi-vendor interoperable interfaces. With O-RAN ALLIANCE updating its specifications 3-times a year, there is a continual updating of Open RAN specifications, introducing new Open RAN functionality to address new requirements and deployment use cases. This paper builds on the groundwork laid by previous 5G Americas Open RAN publications, focusing on providing updates on the progress made by leading Open RAN standards bodies, the latest advancements in multi-vendor interoperability, and current market deployments and trials. Due to the rapidly evolving landscape, these updates reflect a snapshot of the open RAN market in August 2023. Readers should expect continued market momentum in terms of new use-cases, requirements, enhancements together with increasing deployments as Open RAN transitions from early deployments into a technology that is widely adopted across all mobile network operator segments and geographies.

Appendix

On-Going Open RAN Architectural Developments

The main body of this technical paper describes update to the Open RAN published as of June 2023. Recognizing that there is significant interest in more recent specification developments which are still work in progress, this section highlights the continued innovation that is occurring across the Open RAN industry.

Uplink Performance Improvement (ULPI)

Although still work in progress, several industry commentators[36], have reported on the on-going work within the O-RAN ALLIANCE Open Fronthaul WG4 concerning a study into ULPI (UpLink Performance Improvement). ULPI is being considered as an optional enhancement to the current Open Fronthaul specification to improve UL air interface performance by shifting certain processing functions from the O-DU to O-RU while minimizing the fronthaul bit rate, e.g., the number of streams reduced to the number of layers. ULPI is proposed as a new kind of beamforming, called “DMRS (Demodulation Reference Signal) beamforming” or “DMRS-BF”. ULPI is supported in two different ways:

- DMRS beamforming without equalization in the O-RU “DMRS-BF-NEQ”
- DMRS beamforming with equalization in the O-RU “DMRS-BF-EQ”.

Both are meant to co-exist with the existing types of beamforming such as Weight-based Dynamic Beam Forming (WDBF), Channel Information based Beam Forming (CIBF) and predefined beamforming. Any given spatial stream is expected to use a single type of beamforming e.g., UL WDBF, DMRS-BF-NEQ or DMRS-BF-EQ based on endpoint configuration. Like the existing beamforming methods, the O-DU needs to convey certain information to the O-RU pertaining to support DMRS-BF-NEQ or DMRS-BF-EQ. The main information to be conveyed is the DMRS configuration, associated with the multiple layers used for SU-MIMO or MU-MIMO user group data layers in the supported UEs.

Energy Savings in O-RAN

The O-RAN ALLIANCE has highlighted energy efficiency as driving the prioritization of key requirements as part of its release program[37]. This work is being led by the recently formed O-RAN Sustainability Focus Group (SuFG), focusing on optimizing EC (Energy Consumption), reducing environmental impact, and creating more energy-efficient and environmentally friendly mobile networks[38]. EC can be reduced by improving the EE (Energy Efficiency) of the network, and by introducing different ES (Energy Saving) mechanisms.

Already commercial O-RUs are offering energy savings techniques, including advanced sleep control and power amplifier control[39].

The O-RAN ALLIANCE is currently developing the following ES features to achieve the above goals:

- The carrier and cell switch off/on: this feature aims at reducing O-CU/O-DU/O-RU power consumption by switching off/on one or more carriers or a cell of a given technology.
- RF channel switch off/on: this feature aims at reducing power consumption of O-RU by switching off/on certain RF channels.
- The Advanced Sleep Mode: this feature is expected to reduce power consumption by partially switching off O-RU components.
- Cloud resource energy saving mode: this feature attempts to reduce power consumption by various components of cloud.

Massive/MU-MIMO Beamforming

The O-RAN ALLIANCE is in the process of investigating new massive MIMO capabilities, including where the O-RU executes a DMRS beamforming algorithm allowing an enhancement of uplink performance. Within this approach the O-RU may also execute an equalization operation, providing a tradeoff between O-RU complexity and uplink air interface performance.

Acronyms

AI: Artificial Intelligence

ATIS: Alliance for Telecommunications Industry Solutions

BT: British Telecom

CHIPS: Creating Helpful Incentives to Produce Semiconductors for America

CIBF: Channel Information based Beam Forming

CNF: Cloud native functions

CPU: Central Processing Unit

CSP: Communication Service Providers

CU: Central unit

DDoS: Distributed Denial of Service

DME: Data Management and Exposure

DMRS: Demodulation Reference Signal

DRB: Data Radio Bearer

DT: Deutsche Telekom

DU: Distributed unit

DUT: Device under test

EC: Energy Consumption

EE: Energy Efficiency

ES: Energy Saving

FAPI: Functional application platform interface

FDD: Frequency Division Duplex

FOCOM: Federated O-Cloud Orchestration and Management

GoB: Grid-of-beams

GPP: General Purpose Processor

GPU: Graphical Processing Unit

HW: Hardware

IoT: Internet of Things

IP: Internet Protocol

KPI: Key Performance Indicator

LTE: Long Term Evolution

MAC: Medium Access Control

MIMO: Multiple Input Multiple Output

ML: Machine Learning

MNO: Mobile Network Operator

MOCN: Multi-Operator Core Network

MWC: Mobile World Congress

NACM: NETCONF Access Control Model

NETCONF: NETwork CONFiguration protocol

NF: Network functions

NSSMF: Network Slice Subnet Management Function

NTIA: National Telecommunications and Information Administration

OAD: O-RAN Architecture Description

OAI: Open Air Interface

OFH: Open FrontHaul

OpenRAN: Open Radio Access Network

OTIC: Open Testing and Integration Center

PHY: Physical Layer

PLMN: Public Land Mobile Network

PNF: Physical Network Function

PRB: Physical Resource Block

QoE: Quality-of-Experience

QoS: Quality-of-Service

RAN: Radio Access Network

RBAC: Role Based Access Control

RF: Radio Frequency

RIC: RAN intelligent controller

RRC: Radio Resource Connection

RRM: Radio Resource Management

RU: Radio unit

SBA: Service based Architecture

SBOM: Software Bill of Materials

SCF: Small Cell Forum

SCOPE: System Certification Process

SME: Service Management and Exposure

SMO: Service Management and Orchestration

SMOF: SMO Functions

SMOS: SMO are SMO Services

SRS: Sounding Reference Signal

SSB: Synchronization signal block

SuFG: Sustainability Focus Group

TIP: Telecom Infra Project

TR: Technical Reports

UE: User equipment

UL: Uplink

ULPI: Uplink Performance Improvement

WDBF: Weight-based Dynamic Beam Forming

YANG: Yet Another Next Generation – data modeling language

ZTA: Zero-trust architecture

Acknowledgments

5G Americas' Mission Statement: 5G Americas facilitates and advocates for the advancement and transformation of 5G and beyond throughout the Americas.

5G Americas' Board of Governors members include Airspan Networks, Antel, AT&T, Cable & Wireless, Ciena, Cisco, Crown Castle, Ericsson, Liberty Latin America, Mavenir, Nokia, Qualcomm Incorporated, Rogers Communications Inc., Samsung, T-Mobile USA, Inc., Telefónica, VMware and WOM.

5G Americas would like to recognize the significant project leadership and important contributions of group leaders Mark Grayson of Cisco and Rajarajan Sivaraj of Mavenir, along with many representatives from member companies on 5G Americas' Board of Governors who participated in the development of this technical paper.

Endnotes

1 https://mcusercontent.com/ea97723d4f3a656d7478894bd/files/77b246cd-3920-a65e-bf6a-86c715100572/RAN_Research_Open_RAN_Equipment_Forecast_2023_2030_Executive_Summary.pdf

2 https://www.5gamericas.org/transition-toward-open-interoperable-networks/

3 https://www.5gamericas.org/the-evolution-of-open-ran/

4 O-RAN.WG6.AAL-GAnP-R003-v06.00 "O-RAN Acceleration Abstraction Layer General Aspects and Principles 6.0"

5 Report on Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment, US FCC CSRIC VIII WG2, Dec 2022

6 "O-RAN Architecture Description" O-RAN.WG1.OAD-R003-v09.00

7 "5G nFAPI Specifications", SCF225, https://www.scf.io/en/download.php?doc=225

8 "NFAPI service: 1.0 service object definition", SCF167, https://scf.io/en/download.php?doc=167

9 "O-RAN Management Plane Specification", O-RAN.WG4.MP.0-v10.00, O-RAN ALLIANCE

10 O-RAN Security Protocol Specification, O-RAN Alliance WG11

11 O-RAN Security Requirements Specification, O-RAN Alliance WG11

12 O-RAN Threat Modeling and Remediation Analysis, O-RAN Alliance WG11

13 O-RAN Security Test Specifications, O-RAN Alliance WG11

14 Open Radio Access Network Security Considerations, US NSA ESF, September 2022.

15 Report on Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment, US FCC CSRIC VIII WG2, Dec 2022

16 Summary of the NCSC's security analysis for the UK telecoms sector

17 Open Risk Analysis, BSI Germany, english translation, February 2022

18 Cybersecurity of Open Radio Access Networks | Shaping Europe's digital future (europa.eu) EU NIS Cooperation Group May 11, 2022

19 Report on How Virtualization Technologies can be used to Promote 5G Security and Reliability, US FCC CSRIC VIII WG3, Dec 2022

20 Zero Trust Architecture (ZTA), NIST SP 800-207, S. Rose, O. Borchert, S. Mitchell, S. Connelly, US DoC NIST, August 2020

21 Enhanced Zero Trust and 5G, ATIS, July 2023

22 "O-RAN Near-RT RIC APIs specification v1.0", O-RAN-WG3.RICAPI-R003-v01.00

23 Overview of Open Testing and Integration Centre (OTIC) and O-RAN Certification and Badging Program - White Paper, April 2023

24 O-RAN.TIFG.Cert-Badge.0-R003-v07.00 "O-RAN Test and Integration Focus Group: Certification and Badging Processes and Procedures"

25 O-RAN.TIFG.E2E-Test.0-v04.0 "O-RAN Test and Integration Focus Group: End-to-end Test Specification"

26 TIP's Open RAN System Certification process (SCOPE): Aligning the Industry and Accelerating Open RAN Commercial Deployments

27 https://content.hclindustrysaas.com/c/gsma-mobile-world-live-survey-report?x=wn5yyu&_pfses=jsn3QaHNkv7qJy1K4QySMkNL

28 https://the-mobile-network.com/2023/02/so-what-is-the-truth-about-open-ran/

29 https://about.dish.com/2023-02-22-DISH-Wireless-Launches-Virtual-Open-RAN-5G-Network-with-Samsung

30 https://www.vodafone.co.uk/newscentre/press-release/openran-deployed-in-urban-locations-in-european-first/

31 https://www.samsung.com/global/business/networks/insights/press-release/0125-kddi-starts-commercial-deployment-of-5g-open-vran-sites-in-japan-in-collaboration-with-samsung-electronics-and-fujitsu-limited/

32 https://www.telekom.com/en/media/media-information/archive/first-commercial-open-ran-in-2023-1027618

33 https://www.capacitymedia.com/article/2bb6obhqx5avgyejn4740/news/big-five-mobile-operators-ready-for-open-ran-by-2025

34 https://newsroom.orange.com/major-european-operators-accelerate-progress-on-open-ran-maturity-security-and-energy-efficiency/

35 https://www.sdxcentral.com/articles/news/att-nokia-run-ric-e2-interface-trial/2023/03/

36 https://www.analysysmason.com/contentassets/950b1c8aeec346a0b45446eafa7fd77b/analysys_mason_oran_specifications_ericsson_jun2023_rma18.pdf

37 https://www.o-ran.org/ecosystem-resources

38 "O-RAN Sustainability Focus Group (SuFG)", https://o-ran.org/about#technical-workgroup

39 https://www.fujitsu.com/global/documents/products/network/solutions/Fujitsu-Radio-Unit.pdf