An Overview on Open-RAN Security: Issues, Requirements, Discussions

Heejae Park[1], Seonghyeon So[1], Woongsoo Na[2], Wonseok Choi[3], and Laihyuk Park[1]*

[1] Dept of Computer Science and Engineering, Seoul National University of Science and Technology
{prkhj98, thtjdgus0828, lhpark}@seoultech.ac.kr
[2] Department of Software, Kongju National University
wsna@kongju.ac.kr
[3] Telecommunications Technology Association
wschoi@tta.or.kr

Abstract

Open-RAN (O-RAN) has been considered one of the most promising technologies for 5G and 6G systems. O-RAN advocates for openness and intelligence to address the limitations of existing RAN networks. Since O-RAN splits based band units into Distributed Unit (DU), and Centralized Unit (CU), it makes the deployment flexible for updates and installation. Furthermore, O-RAN makes possible to establish a higher level of network automation.However, since O-RAN architecture is different from traditional RAN, various security issues and requirements need to be discussed. Thus, to demonstrate more complete security specifications, we provide O-RAN security issues, O-RAN security requirements and discussions on O-RAN security.

Keywords: O-RAN, Security issues, Security requirements

1 Introduction

With next-generation wireless systems built on a variety of heterogeneous technologies such as terahertz communications, Reconfigurable Intelligent Surface (RIS), and Deep Learning (DL)-based communications [1, 2, 3], cellular networks are becoming more complex. This will increase capital and operational costs for the network operators, since operators need to consistently perform upgrading and maintaining their infrastructure. As a result, network operators will face growing financial and operational burdens, necessitating ongoing investments in infrastructure upgrades and maintenance to stay aligned with evolving market trends, technological advancements, and customer demands. To meet aforementioned requirements, Open-RAN (O-RAN) has emerged as a solution.

O-RAN has been considered one of the most promising technologies for 5G and 6G systems. Unlike conventional RAN systems which are far from open, O-RAN advocates for openness and intelligence to address the limitations of existing RAN networks [4, 5]. O-RAN deployments rely on a framework of disaggregated, virtualized, and software-based components, all interconnected through open and well-defined interfaces. This setup ensures interoperability across various vendors. The process of disaggregation and virtualization empowers flexible deployments and enhances the network's resilience and reconfigurability. [6]. However, since O-RAN architecture is different from traditional RAN, various security issues and requirements need to be considered to ensure high information security. Motivated by aforementioned consideration, this work provides O-RAN security issues, O-RAN security requirements and discussions on O-RAN security.

The 7th International Symposium on Mobile Internet Security (MobiSec'23), Dec 19-21, 2023, Okinawa, Japan, Article No.30
*Corresponding author: Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, 01811, Repulic of Korea, lhpark@seoultech.ac.kr

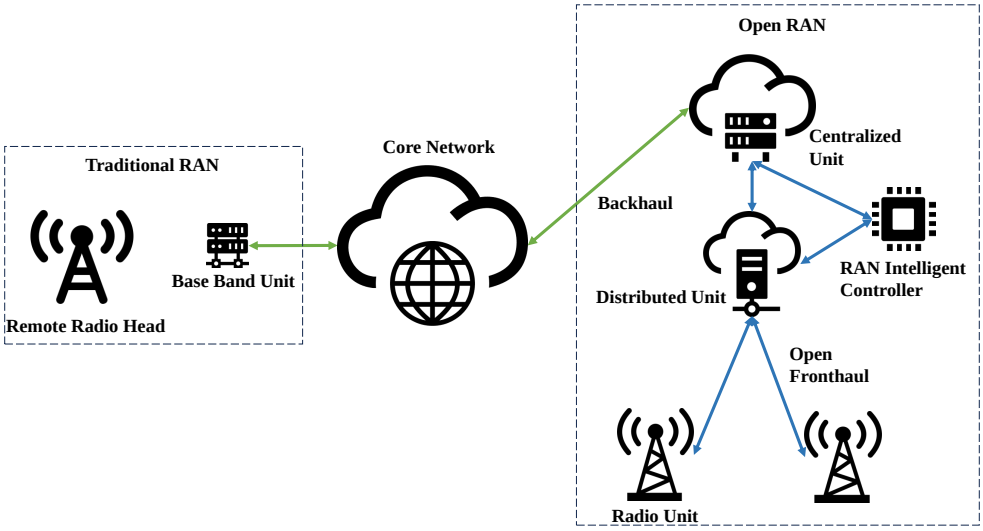

Figure 1: Comparison of O-RAN architecture with traditional RAN

The remainder of this paper is organized as follows. In Section 2, provides brief overview on O-RAN architecture. Section 3 presents several O-RAN security issues. Security requirements of O-RAN components are described in Section 4, and Section 5 provides discussions on O-RAN security. Finally, conclusion is shown in Section 6.

2 Brief Overview on O-RAN

- **O-RAN Architecture**: Fig. 1 shows the comparison of O-RAN and traditional RAN architecture. O-RAN architecture consists of multiple components: 1) Radio Unit (RU), 2) Distributed Unit (DU), 3) Centralized Unit (CU), and 4) RAN Intelligence Controller (RIC) [7]. RU, DU, and CU are called O-RU, O-DU, and O-CU in O-RAN specifications [8]. The RU is responsible for processing radio signal and has a physical layer. O-RAN system splits the traditional RAN's based band unit into DU and CU. RU is equipped with antennas and has the responsibility of processing signals such as transmitting, receiving, digitizing, and amplifying [7]. DU is typically physically positioned in proximity to the RU, whereas CU is positioned nearer to the core network. RIC is a key element that execute real-time optimization and resource allocation by leveraging data gathered from both the network and end users. Fig. 2 shows the high level architecture of O-RAN. Service Management and Orchestration (SMO) which manages the RAN domain and oversees network function's lifecycle management is a main component of the O-RAN architecture. O-RAN splits O-CU into two parts: O-CU Control Plane (CP) and O-CU User Plane (UP). In addition, RIC is split into non-real-time RIC (Non-RT RIC) and near-real-time (Near-RT RIC). Non-RT RIC is installed in SMO and it addresses the request within non-real-time. The Near-RT RIC is located in the edge servers or regional cloud environments and it executes network optimization actions within near-real-time. O-Cloud is a cloud computing platform and it consists of physical infrastructure. O-Cloud hosts the network functions related to O-RAN such as cloud network functions (CNFs) and virtual network functions (VNFs) which are used by O-RAN components.

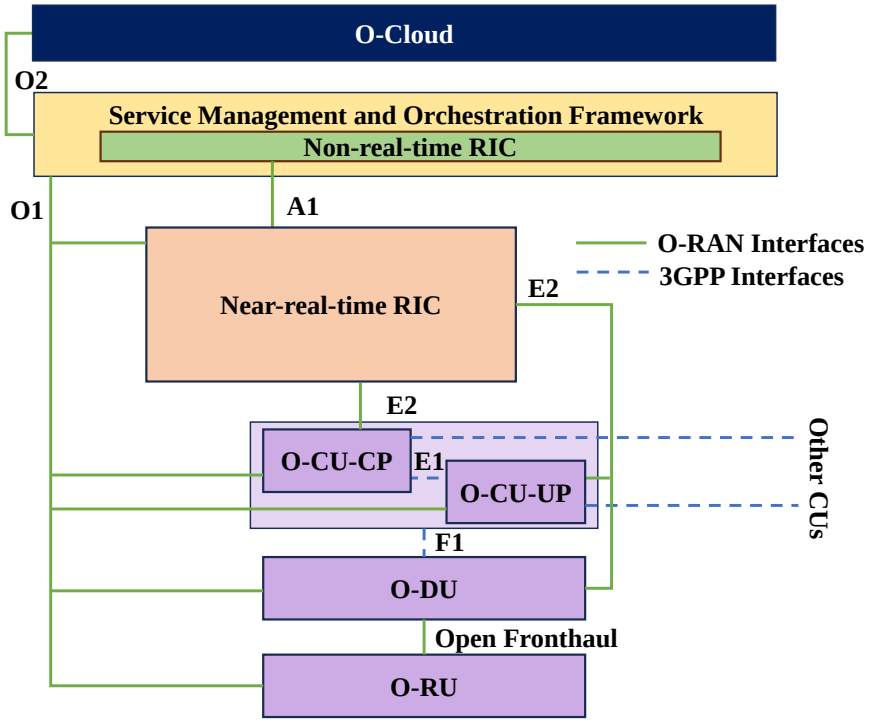

Figure 2: High level architecture of O-RAN

In addition, There are several interfaces: A1, O1, O2, and E2. A1 connects Non-RT RIC and Near-RT RIC. O1 connects SMO to all O-RAN components, while O2 connects SMO and O-Cloud for supporting additional computing resource. E2 connects Near-RT RIC and the E2 nodes, i.e., O-DUs, O-CUs.

- **Advantages of O-RAN**: The benefits of O-RAN are listed as follows [6, 9, 10]:

  1. The unification of the software enabled architecture makes the network more suitable for future communication.
  2. Spliting based band units into DUs and CUs makes the deployment flexible for updates and installation.
  3. The plug-and-play feature of O-RAN, coupled with various promising techniques, is anticipated to lower maintenance costs.
  4. It is possible to establish a higher level of automation within the network.
  5. Open and interoperable interfaces enable operators to integrate equipment from various vendors, thereby expanding the RAN ecosystem to include smaller players.

3 O-RAN Security Issues

The usage of O-RAN has many advantages, but it has several issues. In this section, we investigate four O-RAN security issues: Privacy Attacks, Open-Source Software Attacks, Threats against Wireless Functionalities, and Physical Threats.

- **Privacy Attacks**: Often, sensitive user data is unintentionally exposed through communication services that collect a wide range of personal information, much of which is not essential for the service functionality [2]. In some cases, adversaries can even extract these personal details, such as their location, User Equipment (UE) priority, trajectory, and preferences in O-RAN system. Hence, it is imperative to establish well-defined guidelines to handle the challenges caused by interfaces and emerging participants within the O-RAN system [7].

- **Open-Source Software Attacks**: Given that O-RAN is anticipated to rely on open-source code, it becomes particularly susceptible to this form of attack. A trusted developer can potentially introduce a backdoor deliberately by inserting a malicious code into an open-source code for the O-RAN system [7].

- **Threats against Wireless Functionalities**: Attacks targeting either the RUs or the open fronthaul interface connecting RUs and DUs can result in a deterioration of performance. These attacks involve actions like data or synchronization signal jamming and denial of service. Furthermore, when different vendors' equipment is integrated into the network, it can reduce network performance due to configuration mismatches or differences in supported functionalities [6].

- **Physical Threats**: The additional hardware installed to support the O-RAN can be compromised by attackers with physical access to the O-RAN system. These attacks may encompass disrupting power availability, reconfiguring cabling, adding hardware backdoors, or compromising sensitive data.

4 Security Requirements of O-RAN

Since O-RAN is different from traditional communication systems, various requirements need to be investigated. This section describes the security requirements of each O-RAN components and interfaces [11].

- **SMO**: SMO shall provide the authentication of internal requests, external systems, resource owners, servers, and clients, as well as the authorization of service requests obtained from external systems. Also SMO shall be able to recover from a volumetric Distributed Denial of Service (DDoS) attack without experiencing a catastrophic failure.

- **Non-RT RIC**: Non-RT RIC shall support authentication as a resource owner/server and client who shall provide authorization to requests from Non-RT RIC Applications (rApps) as a client. And then rApps shall supply client authorization requests to the Non-RT RIC Framework.

- **Near-RT RIC**: During Software Development Life cycle (SDL) registration, Near-RT RIC shall validate Extended Application (xApp) access to the Near-RT RIC database and provide allowed access. Mutual authentication shall be used for any communication between xApps and the Near-RT RIC platform Application Programming Interfaces (APIs).

- **O-CU-CP/UP**: O-CU-CP and O-CU-UP shall meet the security requirements for gNB-CU-CP and gNB-CU-UP respectively, as specified in [8].
- **O-DU**: O-DU shall meet the security requirements for gNB-DU as specified in [8].
- **O-Cloud**: Users who access to O-RAN system need to be authenticated, authorized, and recommended to use Multi-Factor Authentication (MFA). O-Cloud Platform is responsible for monitoring App/VNF/CNF packages downloaded from the O-Cloud images repository. Its objective is to detect and flag any unauthorized modifications, deletions, or insertions within these packages. In addition, O-Cloud is designed to provide robust protection for keys and algorithms used in code signing, encryption, and decryption processes.
- **A1 Interface**: A1 interface shall meet confidentiality, integrity, replay protection and mutual authentication and authorization. And it shall support mutual Transport Layer Security (mTLS) for Non-RT RICs and one or more Near-RT RICs to mutually authenticate and support Open Authorization (OAuth) 2.0 authentication.
- **O1 Interface**: Through an encrypted transport and least privilege access control utilizing the network configuration access control model, O1 interface shall meet confidentiality, integrity, and authenticity requirements. In O1 interface, the network configuration access control model (NACM) shall give operators the ability to limit user access to a preconfigured subset of all available Network Configuration (NETCONF) protocol operations and material in order to administer O-RAN functions effectively and securely.
- **O2 Interface**: O2 interface shall meet confidentiality, integrity, replay protection and data origin authentication. Providers of Management Services and Transport Layer Security (TLS) users are required to comply with the O-RAN security protocols specifications for TLS support at O2 interface.
- **E2 Interface**: Also E2 interface shall meet confidentiality, integrity, replay protection and data origin authentication. According to the O-RAN Security Protocols Specifications, Internet Protocol Security (IPsec) shall be provided for security protection at the IP layer on the E2 interface.

5 Discussions on O-RAN Security

As traditional based band unit is replaced by DUs and CUs and the openness of the O-RAN is encouraging the vendors to be more competitive with their advanced apparatus, O-RAN is more economically beneficial than traditional RAN. However, with their open interfaces and modules, the deployment of O-RAN systems raises significant security concerns. The potential consequences of these vulnerabilities can be addressed through a combination of automated security solutions and the establishment of secure communication protocols that encompass confidentiality, integrity, and accountability. Furthermore, to enhance security within O-RAN, the integration of AI or ML-driven firewalls and Intrusion Detection Systems (IDS) is essential for safeguarding its subdomains [12]. However, it's important to note that the security overhead associated with these solutions contributes to operational expenses (OpEx).

In addition, impact of Quantum Computing (QC) on O-RAN system can be discussed [7]. Quantum Computing (QC) represents an unprecedented level of computing power, surpassing the capabilities of a state-of-the-art supercomputer. Thus, with its computing capabilities, QC can assist O-RAN by processing the RIC computation tasks in the real-time. However, from the perspective of

security, QC poses a threat to the security of communication networks, since it challenges the complexity of cryptographic algorithms. To solve this problem, Quantum Resistance (QR) cryptography was proposed. Therefore, QR based security strategies can be discussed for ensuring the security of the O-RAN system.

6 Conclusion

O-RAN has been considered one of the most promising technologies due to its openness and intelligence. However, since O-RAN architecture is different from conventional RAN system, there can be various security issues such as privacy attacks, open-source software attacks, threats against wireless functionalities, and physical threats. Furthermore, security requirements of O-RAN and discussions on O-RAN security are also investigated to demonstrate more complete security specifications for future networks. In future work, more security threats and solution strategy for each threats can be analyzed.

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. RS-2022-00166729). This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2023-RS-2022-00156353) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

[1] Heejae Park, Tri-Hai Nguyen, and Laihyuk Park. Federated deep learning for ris-assisted uav-enabled wireless communications. In *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pages 831–833. IEEE, 2022.

[2] Hongyang Du, Jiayi Zhang, Ke Guan, Dusit Niyato, Huiying Jiao, Zhiqin Wang, and Thomas Kürner. Performance and optimization of reconfigurable intelligent surface aided thz communications. *IEEE Transactions on Communications*, 70(5):3575–3593, 2022.

[3] Heejae Park, Tri-Hai Nguyen, and Laihyuk Park. Reconfigurable intelligent surface-assisted system models for uplink communications. In *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pages 828–830. IEEE, 2022.

[4] CT Shen, YY Xiao, YW Ma, JL Chen, Cheng-Mou Chiang, SJ Chen, and YC Pan. Security threat analysis and treatment strategy for oran. In *2022 24th International Conference on Advanced Communication Technology (ICACT)*, pages 417–422. IEEE, 2022.

[5] Min Suk Kang. Potential security concerns at the physical layer of 6g cellular systems. In *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pages 981–984. IEEE, 2022.

[6] Michele Polese, Leonardo Bonati, Salvatore D'oro, Stefano Basagni, and Tommaso Melodia. Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges. *IEEE Communications Surveys & Tutorials*, 2023.

[7] Madhusanka Liyanage, An Braeken, Shahriar Shahabuddin, and Pasika Ranaweera. Open ran security: Challenges and opportunities. *Journal of Network and Computer Applications*, 214:103621, 2023.

[8] 3rd Gener. Partnership Project (3GPP). Security architecture and procedures for 5g system: Ts 33.501 v17. 7.0. 2020.

[9] Sameer Kumar Singh, Rohit Singh, and Brijesh Kumbhani. The evolution of radio access network towards open-ran: Challenges and opportunities. In *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pages 1–6. IEEE, 2020.

[10] Aly S Abdalla, Pratheek S Upadhyaya, Vijay K Shah, and Vuk Marojevic. Toward next generation open radio access networks: What o-ran can and cannot do! *IEEE Network*, 36(6):206–213, 2022.

[11] O-RAN Alliance. O-ran specification. available online: https://www.o-ran.org/specifications. 2022.

[12] Bouziane Brik, Hatim Chergui, Lanfranco Zanzi, Francesco Devoti, Adlen Ksentini, Muhammad Shuaib Siddiqui, Xavier Costa-Pérez, and Christos Verikoukis. A survey on explainable ai for 6g o-ran: Architecture, use cases, challenges and research directions. *arXiv preprint arXiv:2307.00319*, 2023.