Open RAN Security and Privacy: Opportunities and Challenges

Madhusanka Liyanage[✠], Abdullah Aydeger[∧]
[✠]Network Softwarization and Security Labs (NetsLab), University College Dublin, Ireland.
[∧]Florida Institute of Technology, USA
Email: madhusanka@ucd.ie, engin.zeydan@cttc.cat, aaydeger@fit.edu

***Abstract*—Open RAN (O-RAN) is a novel industry-level standard for RAN (Radio Access Network) which defines interfaces that support inter-operation between vendors' equipment and offer network flexibility at a lower cost. Open RAN integrates the benefits and advancements of network softwarization and Artificial Intelligence to enhance RAN devices' operation. Open RAN offers new possibilities so different stakeholders can develop the RAN solution in this open ecosystem. However, the benefits of ORAN come with new security and privacy challenges. Open RAN offers an entirely different RAN configuration than what exists today, and it could lead to serious security and privacy issues if mismanaged. Stakeholders are understandably taking a cautious approach towards the secure Open RAN deployment. In particular, the tutorial will provide a deep analysis of the security and privacy risks and challenges associated with Open RAN architecture. Then, we will discuss the possible security and privacy solutions to secure the Open RAN architecture and present relevant security standardisation efforts relevant to Open RAN security. The tutorial will also discuss how Open RAN can be used to deploy more advanced security and privacy solutions in 5G and beyond RAN. Finally, the tutorial will provide enlightening guidance for subsequent research of Open RAN security and privacy at this initial phase of vision towards reality via two demonstrations.**

I. Objectives, Motivation, Timeliness and Intended Audience

A. Objectives, Motivation

Open RAN (O-RAN) introduces standardized interfaces that enable interoperability across vendors' Radio Access Network components, reducing vendor lock-in and supporting cost-efficient, flexible deployments. By incorporating network softwarization and artificial intelligence (AI), O-RAN enhances automation, scalability, and adaptability in next-generation RAN architectures.

Unlike legacy RAN systems built with monolithic, vendor-specific equipment, O-RAN disaggregates baseband processing, offering operators the flexibility to integrate best-of-breed components. This shift builds on architectural progress from 2G to 5G, enabling faster deployment cycles, service innovation, and operational agility.

However, the openness and modularity of O-RAN expand the threat landscape. Decentralized control functions and open interfaces increase vulnerability to attacks, particularly from compromised vendors or misconfigured virtualized components. Softwarization introduces risks such as VNF mismanagement, virtual machine exploits, and insecure orchestration channels. AI components also introduce new threat vectors, including model poisoning, spoofing, and adversarial inputs targeting RAN performance or reliability.

Further complicating matters, AI-enabled spectrum management and traffic optimization in O-RAN can be subverted through malicious signal injection or data manipulation. These risks are exacerbated in multi-vendor environments, where inconsistent security baselines and fragmented governance amplify attack surfaces.

Despite these concerns, O-RAN also presents unique security benefits. Its modular design enables faster patching and fault isolation, while CI/CD integration supports continuous security updates. Operators can more easily monitor, audit, and upgrade individual components, minimizing downtime and improving incident response. Standardized interfaces can help detect misconfigurations and enforce compliance across heterogeneous systems.

Moreover, O-RAN supports automation features like zero-touch provisioning and telemetry-based intrusion detection, which improve resilience. Its flexibility and abstraction layers provide an opportunity to implement stronger isolation, dynamic policy enforcement, and runtime verification mechanisms not feasible in traditional RAN systems.

In summary, while O-RAN poses substantial security and privacy challenges due to its distributed and open nature, it also provides new levers for control, automation, and secure evolution. Realizing its potential requires coordinated standardization, upgraded threat models, and active collaboration between industry, academia, and regulatory stakeholders.

B. Timeliness and Intended audience

1) Why is the topic current and important?: Open RAN is currently one of the most exciting concepts in wireless technology due to its numerous potential benefits, such as greater network management options, lower costs and, more diverse ecosystem of equipment suppliers. Recent open RAN reports indicated that revenue from sales of compatible hardware and software for Open RAN skyrocketed in Q1 2021 and predicted that Open RAN technology could provide a significant boost to global GDP by 2030 [1]. Thus, it is obvious Open RAN is one of major innovation which will be playing a vital role in future mobile network Eco system.

[1]https://www.fiercewireless.com/wireless/analysts-predict-gdp-upside-as-open-ran-revenue-surges-q1

Security and Privacy have become primary concerns in Open RAN realization as risks can have high consequences. Especially, the core and enable technologies associated with Open RAN can be vulnerable to various security and privacy threats. At the end, these risks associated with Open RAN will impacting 5G and beyond networks as well as its users. Several incidents revealed that the hazard encountered by an infected wireless network, not only affects the security and privacy concerns, but also impedes the complex dynamics of the communications ecosystem. Consequently, the complexity and strength of security attacks have increased in the recent past making the detection or prevention of sabotage a global challenge. Thus, security Open RAN will play a vital role in securing the B5G networks at the end.

2) Why the tutorial may attract a good number of attendees?: In the beyond 5G research and development domains, Open RAN is a very popular concept not only in industry but also in academics. There are many research and SDO (Standard Development Organization) activities already initiated to support the realization of Open RAN. In these research activities, security and privacy is considering as a key focus area for many researcher. Thus, this tutorial would be attractive for people working in these domains. As people have already been in contact with initial use cases and understood the power and the corresponding possibilities leading from Open RAN, the tutorial will be more interesting to need of security and privacy to realize reliable Open RAN deployment.

This Tutorial will be of key interest for:

- **Service Providers:** looking forward to offer new secured services to their customers by adopting Open RAN paradigm. This tutorial will be a great opportunity that can provide insight for the novel security and privacy solutions for B5G Open RAN domain.
- **Network Operators (NOs):** willing equally to reach the large customer base who are going to switch to new Open RAN based services. Ensuring the security and privacy is a key requirement while deploying Open RAN their networks. This tutorial will present many of ways of designing security and privacy in this aspect.
- **Academics:** as for research-based educational institutes, Open RAN security and privacy is an ongoing and hot area of study. This tutorial will be helpful not only for early (Msc, PhD Students) and mid-career (Post Docs) researchers but also for experience researchers. Attendees can identify and learn about new challenges in the domain.
- **Technology Architects:** Soon, Open RAN is going to be established as pervasive underlying paradigm providing massive connectivity and will play a key role in digitization of businesses for all sorts of enterprises. Thus it is high time for technocrats to aligning their business-technologies to the future needs of Open RAN standards. This tutorial provides exposure of new ways of providing security and privacy for Open RAN based B5G networks.

No stringent prerequisites to preclude any tutorial participant from attending, however, minimal background knowledge in network security is required.

II. Name and a short biography of each tutorial presenter

Dr. Madhusanka Liyanage Madhusanka Liyanage is an Associate Professor/Ad Astra Fellow and Director of Network Softwarization and Security Labs (NetsLab) at the School of Computer Science, University College Dublin, Ireland. He is also a Docent/Adjunct Professor at the University of Oulu, Finland, the University of Ruhuna, Sri Lanka and the University of Sri Jayawardhanapura, Sri Lanka. He received his Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. He also received the prestigious Marie Skłodowska-Curie Actions Individual Fellowship and the Government of Ireland Postdoctoral Fellowship during 2018-2020. He is also a senior member of IEEE. In 2020, he received the "2020 IEEE ComSoc Outstanding Young Researcher" award by IEEE ComSoc EMEA. In 2021, 2022, 2023 and 2024 he was ranked among the world's top 2% of scientists (2020, 2021, 2022 & 2023) on the list prepared by Elsevier BV, Stanford University, USA. Also, he was awarded an Irish Research Council (IRC) Research Ally Prize as part of the IRC Researcher of the Year 2021, 2023 and 2024 awards for his positive impact as a supervisor. In 2022, he received "the 2022 Tom Brazil Excellence in Research Award" from the SFI CONNECT Center. Moreover, Madhusanka received a special commendation from the Irish Research Council Ireland for being the IRC Early Career Researcher of 2022. He has co-authored over 250 publications, including three authored books, four edited books with Wiley, and two patents (Google Citations: 20000+, h-index: 60+). Moreover, He has received four Best Paper Awards for SDMN security (at NGMAST 2015), 5G Security (at IEEE CSCN 2017), MEC Security (IEEE MCE 2021) and 5G IoT (ICT Express 2022). Additionally, he has been awarded two research grants and 19 other prestigious awards/scholarships during his research career. Liyanage has worked for more than fifteen E.U., international and national projects in the ICT domain. Moreover, he was the Finnish national coordinator for EU COST Action CA15127 on resilient communication services. He serves as a management committee member for three other EU COST action projects: EU COST Action IC1301, IC1303, CA15107, CA16226, CA2011, and CA20136. Liyanage has over six years of experience in research project management, research group leadership, proposal preparation, project progress documentation, and graduate student co-supervision/mentoring. He has secured over 10 Million euros in research funding via various research projects. He is a P.I. for three large EU H2020/Horizon Europe projects. As a leader of work packages in several projects, he held responsibilities, including SIGMONA and Naked approach projects. Additionally, two research projects (MEVICO and SIGMONA projects) received the CELTIC Excellence and CELTIC Innovation Awards in 2013, 2017, and 2018. He is also an expert consultant at the European Union Agency for Cybersecurity (ENISA). In 2021, Liyanage was elevated as a Funded Investigator of the Science Foundation Ireland CONNECT Research Centre, Ireland. Moreover, he is an expert reviewer at different funding agencies in France, Qatar, UAE, Sri Lanka, and Kazakhstan.

More Info URL: http://madhusanka.com

Dr. Abdullah Aydeger is currently an assistant professor at the Electrical Engineering and Computer Science Department at FIT. Prior to joining FIT in August 2022, he was an assistant professor at the School of Computing at Southern Illinois University, Carbondale, since 2020. Dr. Aydeger obtained a Ph.D. Degree in Computer and Electrical Engineering from Florida International University in 2020. His research interests are post-quantum cryptography, network security, and virtualization.

III. A description of the topics the tutorial will address, emphasizing their timeliness

The tutorial will address following technical issues,

- Illustration of Open RAN architecture
- Identify the key areas of Open RAN security,
- Discuss the impact and necessity of Open RAN security and Privacy for beyond 5G network deployments
- Highlight the security challenges related to key Open RAN enabling technologies, i.e. AI, Network Softwarization, Open Interfaces
- Comprehensive view of privacy/ trust in Open RAN architecture
- Discuss activities in standardization bodies related to Open RAN Security and Privacy
- Present holistic overview on ongoing research projects related to Open RAN security.
- Future research directions

IV. An outline of the tutorial content, including its tentative schedule and the presenters for each section

The tutorial is planned as a half-day event and it will last for 3 hours of technical content. Outline is presented in Table I

TABLE I
Outline and Schedule of the Tutorial

Time Duration	**Broad topic to be covered**
00 - 10 min	Introduction Open RAN Architecture and Components
10 - 40 min	Open RAN Security and Privacy Threat
40 - 70 min	Open RAN Security in post-quantum era
70 - 85 min	AI for ORAN security (Two Demos of Use of FL and XAI for attack detection) • Demo 1: Securing xApps in Open RAN: A Hierarchical Approach to Authentication and Authorisation • Demo 2: PQC security for ORAN
85 - 90 min	Conclusion, Future directions and open challenges

V. A description of the past and relevant experience of the speaker(s) on the topic of the tutorial

Moreover, Dr Madhusanka has extensive research experience in 5G and beyond Security domains who have organized numerous tutorial in various IEEE conferences such as,

- Tutorial on "The Role of Distributed Ledger Technology (DLT) for Beyond 5G Networks" at IEEE ICIN 2022 [2]
- Tutorial on "6G Security and Privacy Vision Towards Reality" at IEEE CCNC 2022 [3]
- Tutorial on "6G Security and Privacy Vision Towards Reality" at IEEE 5GWF 2021 [4]
- Tutorial on "Blockchain, IoT and 5G – The Trio to Mitigate Current and Post COVID-19 Challenges" at IEEE 5GWF 2021 [5]
- Tutorial on "Security and Privacy of 5G and Beyond 5G Networks" at IEEE CCNC 2021 [6]
- Tutorial on "5G Security and Privacy:Issues, Potential Solutions and Future Directions", IEEE Globecom 2020 [7]
- Workshop on "5G Security and Privacy" at ICAC 2020 [8]
- Tutorial on "Blockchain-powered 5G-IoT Ecosystem vis-'a-vis COVID-19: Opportunities and Challenges" at IEEE ANTS 2020 [9]
- Tutorial on "Role of Blockchain in Beyond 5G Networks" at IEEE 5GWF 2020 [10]
- Tutorial on "5G Security and Privacy: Issues, Potential Solutions and Future Directions" at IEEE Netsoft 2020 [11]
- Tutorial on "Blockchain for 5G and IoT: Use cases, Opportunities and Challenges" at IEEE CCNC 2020 [12]
- 3-day Workshop on "Security of 5G and SDN" at SSIC 2019 Conference[13]
- Special Session on "Secure 5G Telecommunication Networks" at ICCT'19 conference[14]
- 3-day Workshop on "Road to 5G Security" at LPU 2019 [15]
- Tutorial Presentation by E. Zeydan, M. Liyanage: "Leveraging Data Engineering and Distributed Ledger Technologies for the Realization of B5G/6G Networks" presented at:
  - in the 15th International Conference on Network of the Future (NoF 2024), October 02-04, 2024, Castelldefels (Barcelona), Spain.

[2]https://www.icin-conference.org/tutorials/
[3]https://ccnc2022.ieee-ccnc.org/program/tutorials
[4]https://ieee-wf-5g.org/2021-applications-tutorials/#TUT-8
[5]https://ieee-wf-5g.org/2021-applications-tutorials/#TUT-4
[6]https://ccnc2021.ieee-ccnc.org/program/tutorials#security
[7]https://globecom2020.ieee-globecom.org/program/tutorials#tut01
[8]https://icac.lk/
[9]https://ants2020.ieee-comsoc-ants.org/wp-content/uploads/sites/223/2020/12/Tutorials.pdf
[10]https://ieee-wf-5g.org/5g-applications-tutorials/#TUT03
[11]https://netsoft2020.ieee-netsoft.org/program/tutorials/
[12]https://ccnc2020.ieee-ccnc.org/program/tutorials#tut-03
[13]https://ssic2019.com/gworkshop.html
[14]https://www.icct.co.in/specialsession3.php
[15]http://www.spadelpu.com/Roadto5GSecurity-SPADE.html

  - in the 2024 IEEE International Conference on Smart Mobility (SM), September 16-18, 2024, Niagara Falls-Fallsview, Ontario, Canada.
  - 2024 International Conference on Computer, Information and Telecommunication Systems, July 17-19, 2024, Girona, Spain .
- Tutorial Presentation by M. Liyanage and E. Zeydan, "Redefining Telecommunications: Data Engineering and Blockchain for B5G/6G Networks", to be present at
  - 45th IEEE International Conference on Distributed Computing Systems (ICDCS), 20-23 July 2025, Glasgow, UK .
  - 11th IEEE International Conference on Network Softwarization (NetSoft), 23–27 June 2025 // Budapest, Hungary .
- Tutorial Presentation by M. Liyanage and E. Zeydan, "A Tutorial on Leveraging Data Engineering and Blockchain for Improved Network Management and Orchestration in B5G/6G Networks", presented at The 7th International Conference on Blockchain Computing and Applications (BCCA 2025), 14–17 October, 2025 – Dubrovnik, Croatia (approved).
- Tutorial Presentation by M. Liyanage and E. Zeydan, "Applying Data Engineering and Blockchain for B5G/6G Networks: A Step-by-Step Tutorial", presented at 2025 IEEE International Conference on Cyber Security and Resilience (IEEE CSR), August 4–6, 2025, Crete, Greece (approved).
- Tutorial Presentations by Dr. Aydeger and Dr. Zeydan: "Quantum Secure 6G: The Framework and Proof-of-Concept" presented at ACM SAC 2025, "Quantum Secure 6G: The Framework and Proof-of-Concept" presented at IEEE CCNC 2025.

VI. A DESCRIPTION OF PREVIOUS TUTORIAL EXPERIENCE OF THE SPEAKER(S), INCLUDING DETAILS OF ANY PAST VERSIONS OF THE TUTORIAL

This tutorial has not been presented in any other venue. However, we are well-qualified to present it as our previous experiences on similar topics on other tutorials at various conferences.