A Survey on AI-Empowered Security Solutions for 6G

Byungha You, Donghyeon Kim, and Haejoon Jung
Department of Electronics and Information Convergence Engineering
Kyung Hee University
Yongin-si, 17104, South Korea
{syeon2513, dhkim3988, haejoonjung}@khu.ac.kr

***Abstract*—In the future 6G communications, ground, air, and space networks have been expected to be integrated to achieve global connectivity and coverage of Internet of Everything (IoE) networks. Due to the intensified network complexity in a three-dimensional environment, artificial intelligence (AI) is encouraged to support 6G Open radio access networks (O-RAN) with autonomous management and orchestration. However, at the same time, there will be increasing security vulnerabilities derived from the nature of the new architecture. In this paper, we provide a survey on the security issues and their solutions for AI-enabled O-RAN in 6G space-air-ground integrated networks (SAGINs).**

***Index Terms*—IoE networks, space-air-ground-integrated networks, open Radio Access Networks, artificial intelligence.**

I. Introduction

It is envisaged that global connectivity of Internet of Everything (IoE) networks will be accomplished by integrating satellite networks into terrestrial networks (TN) in future 6G communications. Non-terrestrial networks (NTN) with a coverage range of up to 700 km can provide three-dimensional communications using geostationary Earth orbit (GEO), medium Earth orbit (MEO), and low Earth orbit (LEO) satellites, high-altitude platform stations (HAPS), and unmanned aerial vehicles (UAVs) [1]. They can be used together to serve as backhaul links or relays with high throughput for ground-based tiny cells, hence shrinking the traffic burden in the ground mesh networks [2], [3]. Moreover, the line-of-sight (LoS) channel condition is more commonly available in NTN, which enables the IoE nodes to save their energy or reduce transmission power. Especially, due to their lower latency and higher throughput, UAVs, which can be used for IoE data collection, localization, wireless energy supply, and information dissemination, can be a good companion to satellites for remote and disaster areas [4].

The third dimension of the space-air-ground-integrated network (SAGIN) environment makes the network complexity higher, which gives appropriate prominence to the introduction of comprehensive and automated network control with artificial intelligence (AI) [5], [6]. AI strategies can be harnessed to self-drive Open radio access networks (O-RAN), which with intelligence enables autonomous data-driven control and dynamic allocation of local/satellite radio resources [7]. The concepts of O-RAN architecture such as disaggregation, virtualization, RAN intelligent controllers (RIC), and open interfaces make the goal of O-RAN to be accomplished [6]. For example, O-RAN architectures can build a closed-loop control functionality that jointly optimizes the locations and directional transmission of the UAV [8], or that defines management circulation of the UAV-base stations (UAV-BSs) and manages the distributed computing resources of O-RAN for providing offloading tasks [9]. In addition, O-RAN can overcome the critical obstacles to spectrum-sharing, which include the lack of access and integration between government satellites and cellular systems, by employing intelligence and open interfaces [10]. Assuming multiple LEO satellite constellations, a digital twin approach for network slicing is implemented through optimizing resource allocation in O-RAN architecture in [11].

The seamless connectivity of tremendous heterogeneous devices in 6G three-dimensional networks will increasingly bring into relief the prominence of AI-enabled O-RAN. Despite the efficiency and flexibility of the new paradigm, O-RAN will be followed by severe security threats emanating from its openness. The nature of O-RAN architecture may enlarge the vulnerabilities in O-RAN functionalities and interfaces, impacting several assets such as near-real-time (RT) RIC and the service management orchestration (SMO) of O-RAN [12]. However, the capabilities of traditional security approaches for the network have limitations in assuring safe communications in dynamic and complex networks. In this paper, for this reason, we consider security issues and AI-empowered solutions for 6G SAGINs and O-RAN.

II. AI-Empowered Security in O-RAN and SAGIN

Software-defined networking (SDN) and network function virtualization (NFV) employed by O-RAN allow existing functionalities of RAN to disaggregate and associate with each other by standardized interfaces. Therefore, the introduction of O-RAN imposes new sorts of security concerns due to its open ecosystem and network intelligence. There could be security attacks against the AI models or control in supporting custom logic for near-RT RIC (xApps) and non-RT RIC (rApps) such as data/model poisoning attacks, evasion attacks, transfer learning attacks, and model inversion [13]–[15]. With these attacks, malicious users can affect the machine-learning data and process including training, testing, and validating, or can exploit the pre-trained models, which threatens the accuracy and effectiveness of allocating and managing the radio resources of O-RAN fronthaul.

In [16], [17], the O-RAN fronthaul is protected by proposing a standard protocol for the security of Layer-2. Under Man-in-the-Middle attacks, it was presented that security traits of O-

979-8-3503-1327-7/23/$31.00 ©2023 IEEE

RAN fronthaul, which are availability, integrity, authenticity, and confidentiality, satisfies the fronthaul requirements with high requisites for performance. Emphasizing the security weakness of missing authentication and authorization in SMO or near-RT RIC, a security strategy of public key infrastructure is proposed with test case analysis in [12]. In the work, they test whether the pretender is detected or not by authorization.

On the other hand, security in O-RAN can be automated by applying AI solutions, where a new architecture of zero trust (ZT) emerges. While the traditional security models allow the authenticated device to be able to access a network resource, network access control (NAC) of ZT architecture requires the long-term security state of the network subject for deciding to grant/deny individual access, not granting trust to a user with authentication. Service-based architectures (SBA)-based intelligent ZT security model is proposed to dynamically assess the risk and evaluate trusts in [18], where O-RAN architecture was utilized to enhance the facilitation of integration. An attack detection framework is proposed in [19], where dynamic ZT architecture is based on the non-cooperative game concept to secure 6G edge computing. The simulation results of the proposed detection techniques show a higher attack detection rate, and lower false positive rate, and reduced network cost compared to the conventional approach.

AI-enabled wireless communications can also facilitate the physical layer designs including optimized beamforming in 6G SAGIN, where a new spectrum of millimeter-wave (mmWave), Terahertz (THz), and visible light is used. However, an offense like the fast-gradient sign method (FGSM) can be applied to pretendedly generate the AI model with the purpose of distracting and manipulating the beamforming vector [20]. Performing adversarial training is one of the countermeasures to such physical layer attacks [21]. Through the training process of regenerating adversarial samples by imitating the security threat strategies, the AI model can prohibit the malicious opponent from distorting the beamforming procedure.

III. Conclusion

SAGIN has been considered as a key ingredient to construct global IoE networks for its huge coverage. At the same time, O-RAN with intelligence can be an effective solution to cope with the increased network complexity with automated and dynamic management capabilities. In this paper, we have considered new security issues in 6G networks such as attacks against the AI models or the O-RAN fronthaul. Further, their AI-empowered security solutions have been reviewed, which include public key infrastructure, ZT architecture, and adversarial training.

Acknowledgement

This work was supported by the Korea government in part under the National Research Foundation of Korea grants (NRF-2022R1A4A3033401, NRF-2022R1F1A1065367, RS-2023-00276086) and in part under the ITRC support programs (IITP-2023-2021-0-02046) and in part under the Convergence security core talent training business support program (IITP-2023-RS-2023-00266615) supervised by the IITP.

References

[1] S. Kota and G. Giambene, “6G integrated non-terrestrial networks: Emerging technologies and challenges,” *in Proc. IEEE Int. Conf. Commun. Workshops*, pp. 1–6, Jun. 2021.

[2] A. Mohammed, A. Mehmood, F.-N. Pavlidou, and M. Mohorcic, “The role of high-altitude platforms (HAPs) in the global wireless connectivity,” *Proc. IEEE*, vol. 99, no. 11, pp. 1939–1953, Nov. 2011.

[3] M. Nemati, B. Al Homssi, S. Krishnan, J. Park, S. Loke, and J. Choi, “Non-terrestrial networks with UAVs: A projection on flying Ad-Hoc networks,” *Drones*, vol. 6, no. 11, p. 334, Oct. 2022.

[4] M. Vaezi, A. Azari, S. R. Khosravirad, M. Shirvanimoghaddam, M. M. Azari, D. Chasaki, and P. Popovski, “Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G,” *IEEE Commun. Surveys & Tutorials*, vol. 24, no. 2, pp. 1117–1174, 2nd Quart. 2022.

[5] T. G. I. Association, “European vision for the 6G network ecosystem,” Jun. 2021, [Online]. Available: https://5g-ppp.eu/european-vision-for-the-6g-network-ecosystem.

[6] R. Campana, C. Amatetti, and A. Vanelli-Coralli, “O-RAN based non-terrestrial networks: Trends and challenges,” *in Proc. Joint Euro. Conf. Networks and Commun. 6G Summit*, pp. 264–269, Jun. 2023.

[7] O. Alliance, “O-RAN: Towards an open and smart RAN,” Oct. 2018, [Online]. Available: https://lightreading-images.s3.amazonaws.com/5gexchange/downloads/O-RAN-WP-FInal-181017.pdf.

[8] L. Bertizzolo, T. X. Tran, J. Buczek, B. Balasubramanian, R. Jana, Y. Zhou, and T. Melodia, “Streaming from the air: Enabling drone-sourced video streaming applications on 5G Open-RAN architectures,” *IEEE Trans. Mobile Computing*, vol. 22, no. 5, pp. 3004–3016, Nov. 2023.

[9] C. Pham, F. Fami, K. K. Nguyen, and M. Cheriet, “When RAN intelligent controller in O-RAN meets Multi-UAV enable wireless network,” *IEEE Trans. Cloud Computing*, pp. 1–15, Jul. 2022, early access.

[10] R. Smith, C. Freeberg, T. Machacek, and V. Ramaswamy, “An O-RAN approach to spectrum sharing between commercial 5G and government satellite systems,” *IEEE Military Commun. Conf. (MILCOM)*, pp. 739–744, Nov. 2021.

[11] H. Al-Hraishawi, M. Alsenwi, J. u. Rehman, E. Lagunas, and S. Chatzinotas, “Digital twin for non-terrestrial networks: Vision, challenges, and enabling technologies,” *arXiv*, May. 2023, [Online]. Available: arXiv:2305.10273.

[12] C. Shen, Y. Xiao, Y. Ma, J. Chen, C.-M. Chiang, S. Chen, and Y. C. Pan, “Security threat analysis and treatment strategy for ORAN,” *Int. Conf. Adv. Commun. Technol.*, pp. 417–422, Feb. 2022.

[13] O. W. G. 11, “O-RAN security threat modeling and remediation analysis 4.0,” Jul. 2022, O-RAN.WG11.O-RAN-Threat-Model-v04.00 Technical Specification.

[14] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, “Open RAN security: Challenges and opportunities,” *J. Network and Computer App.*, vol. 214, p. 103621, Apr. 2023.

[15] M. Polese, L. Bonati, S. D’Oro, S. Basagni, and T. Melodia, “Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges,” *IEEE Commun. Surveys & Tut.*, vol. 25, no. 2, pp. 1376–1411, 2nd Quart. 2023.

[16] D. Dik and M. S. Berger, “Transport security considerations for the Open-RAN fronthaul,” *IEEE 5G World Forum*, pp. 253–258, Oct. 2021.

[17] D. Dik and M. S. Berger, “Open-RAN fronthaul transport security architecture and implementation,” *IEEE Access*, vol. 11, pp. 46 185–46 203, May 2023.

[18] K. Ramezanpour and J. Jagannath, “Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN,” *Computer Networks*, vol. 217, p. 109358, Nov. 2022.

[19] H. Sedjelmaci and N. Ansari, “Zero trust architecture empowered attack detection framework to secure 6G edge computing,” *IEEE Network*, pp. 1–13, Jan. 2023.

[20] I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” *arXiv*, Mar. 2015, [Online]. Available: arXiv:1412.6572v3.

[21] T. F. Rahman, A. S. Abdalla, K. Powell, W. AlQwider, and V. Marojevic, “Network and physical layer attacks and countermeasures to AI-enabled 6G O-RAN,” *arXiv*, Sep. 2022, [Online]. Available: arXiv:2106.02494v2.