# Demo: SSxApp: Secure Slicing for O-RAN Deployments

Joshua Moore, Aly Sabri Abdalla, Minglong Zhang, Vuk Marojevic
Department of Electrical and Computer Engineering, Mississippi State University, MS 39762, USA
Email: {jjm702, asa298, mz354, vuk.marojevic}@msstate.edu

***Abstract*—This demonstration explores the security concerns in 5G and beyond networks within open radio access network (O-RAN) deployments, focusing on active attacks disrupting cellular communications. An xApp developed on the open artificial intelligence cellular (OAIC) platform enables on-the-fly creation and management of network slices to mitigate such attacks. The xApp is hosted in the near-real time RAN intelligent controller (RIC) and establishes secure slices for the software radio network it controls. This solution presents a practical approach for resilient and secure network management in dynamic environments.**

***Index Terms*—6G, network intelligence, O-RAN, security, slicing, srsRAN, testbed, xApp.**

## I. Introduction

With the fast deployment of fifth generation (5G) networks, the demands for data communication increase across a broad range of devices, including mobile phones, intelligent vehicles, and the Internet of Things (IoT). In order to facilitate data management and improve network scalability and flexibility, network softwarization technologies, such as software-defined networking (SDN), network function virtualization (NFV), mobile edge computing (MEC), and network slicing are adopted in 5G and future 6G networks. Unfortunately, security-related architectures have not progressed as fast as those data communication technologies.

According to [1], key areas worth attention in handling security concerns are network access, network platform, SDN-NFV based networks, and network slices. Current network security frameworks were originally designed for self-reliant standalone networks that possess complete control over the network resources, spanning from spectrum to infrastructure. However, 5G networks employing SDN and network slicing will share the network infrastructure among multiple operators and service providers, each having distinct security policies and privacy prerequisites. Consequently, there is a need for research on both isolation and interoperability among diverse security systems.

Regarding cellular communications in 5G/6G networks, security primarily pertains to active attacks, which involve adversaries engaging in disruptive actions. Such actions encompass the introduction of targeted interference or intelligent jamming signals, aimed at manipulating user transmissions. Noteworthy illustrations of active attacks involve devices employing alternating data channel attacks, which may involve interfering with alternative frequency bands or control channels to disrupt communications.

The emerging open radio access network (O-RAN), which integrates softwarization, disaggregation, openness and programmability, has attracted significant attention [2]. There are contributions that focus on detecting threats, but only a few conceptual solutions were proposed for securing a RAN slice [3], [4]. We leverage the open artificial intelligence cellular (OAIC) platform, which consists of open-source software[1] implementing the RAN, the near-real time RAN intelligence controller with xApps and the E2 control interface and the documentation[2] to implement a testbed that enables research on RAN slicing, among others. We developed an xApp on the OAIC platform for the on-the-fly creation, management, and allocation of secure network slices. When an attack/intrusion is identified, the secure slicing xApp diminishes the resources allocated to the compromised slice as much as possible while maintaining isolation among slices so that the attacked resources are confined and legitimate users are moved to secure slices.

## II. OAIC Testbed

OAIC is a fully open-source software platform that includes both AI controllers (OAIC-C) as well as an AI testing framework (OAIC-T). By following the architecture of O-RAN and leveraging existing open-source 5G software efforts, software radio user equipment (UE), radio units (O-RUs), central units (O-CUs), distributed units (O-DUs), and RAN Intelligent Controllers (RICs) are implemented in OAIC as shown in Fig. 1(a). The O-RU implements the signal and RF processing of the lower physical (PHY) layer. It is connected to the O-DU via the fronthaul. The O-DU is responsible for the upper PHY layer processing, Medium Access Control (MAC), and Radio Link Control (RLC). It connects to the O-CU for higher protocol layer processing through the midhaul. The O-CU, implements the higher-layer protocols, including the Radio Resource Control (RRC) and the Packet Data Convergence Protocol (PDCP).

The RIC is a architectural component that provides a centralized abstraction of the network and allows operators or third party vendors to implement and deploy custom control plane functions. The non-real time (non-RT) RIC performs network operations that have a time granularity of 1 s and above. The near-RT RIC handles RAN functionalities that involve timescales between 10 and 100 ms.

[1]OAIC github: https://github.com/openaicellular/oaic
[2]OAIC: https://www.openaicellular.org/

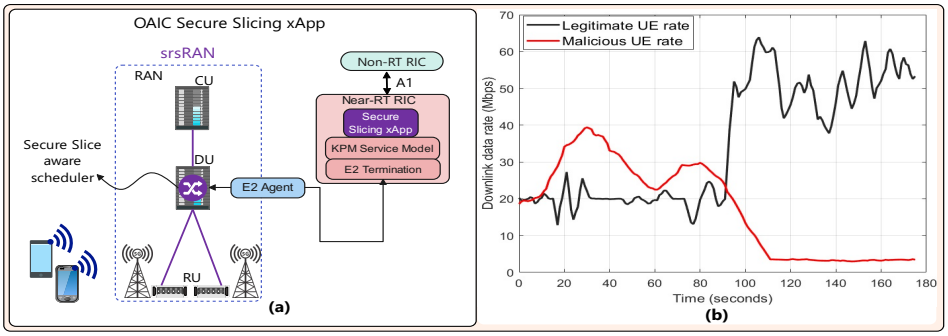


Fig. 1: The OAIC SSxApp testbed (a) and SSxApp controlled throughput for legitimate and malicious UEs (b).

It hosts applications called *xApps*. Both the non-RT RIC and the near-RT RIC can interface with O-CU/O-DU and between themselves through standardized interfaces for data collection (O1), AI inference model deployment (A1), and O-CU/O-DU monitoring and control (E2).

## III. Secure Slicing xApp Implementation

The main components for the implementation and deployment of the secure slicing xApp (SSxApp) are a modified version of POWDER's NexRAN xApp [5] operating inside of OAIC's near-RT RIC along with the E2-enabled srsRAN as shown in Fig. 1(a). The srsRAN is modified with a slice aware scheduler which implements a proportional slicing method for the served users among different slices.

The E2 agent acts as a distinct entity, separate from the RAN protocol stack, and is designed to interface with specific RAN functions. After successfully setup of the E2 interface between the RAN and OAIC's near-RT RIC, the SSxApp can be onboarded to the OAIC platform using the command line interface or the REST APIs of the xApp onboarder tool. The SSxApp is now ready to monitor the exchanged traffic with the RAN and apply different security policies to preserve the confidentiality and privacy of wireless communications. The SSxApp collects the different reported RAN metrics from the service model (SM). Subsequently, the SSxApp slices the RAN resources into different slices where several users will be bound based on their requirements through asynchronous E2 control message. After that, the SSxApp will keep track of historical metrics collected through the SM into the influx database for identifying any malicious UE activities.

In this setup, we implement two UEs connected to srsRAN over ZMQ, where both of the UEs initially are bound to the same slice of a 20 MHz LTE cell with 100 shared physical resource blocks (PRBs). Traffic is exchanged over the connection using Iperf3. The malicious UE is running a modified instruction set that vastly increases its number of requests for resources. The xApp decision is taken after 10 successive KPM reports, relying on historical data and the environment context. Decisions are mapped onto E2 invocations and sent to the NodeB via the E2 control messages. In the given scenario, the average throughput threshold ranges from 18 to 30 Mbps. However, the malicious UE exhibits significantly higher throughput, surpassing this range for approximately 25% of the evaluation period. The results, demonstrated in Fig.1(b), illustrate the implementation of SSxApp, where a malicious UE is intentionally disassociated from its current slice and reassigned to an isolated, secure slice, while the other UE regains its resource share thereafter. This process effectively isolates the malicious UE from slices containing other UEs, enhancing the security and integrity of the network.

## IV. Demonstration

We adapted and deployed the SSxApp in the OAIC testbed. In this demonstration, we will showcase the powerful functionality of SSxApp in a real-world scenario. Our aim is to mitigate a malicious UE that attempts to flood the network with requests for degrading the network's performance. Utilizing the SSxApp, the UE metrics are monitored in real time and proactive measures prevent such disruptive scenarios from occurring. Additionally, we will visually present the impact of these actions by plotting the network's throughput, providing users with a clear understanding of the point at which the intervention occurs.

## Acknowledgment

This work is supported by NSF CCRI OAIC program (grant no. 2120442), as well as NSF and Office of the Under Secretary of Defense (OUSD) – Research and Engineering, under Grant ITE2326898, as part of the NSF Convergence Accelerator Track G: Securely Operating Through 5G Infrastructure Program.

## References

[1] Y. Siriwardhana *et al.*, "AI and 6G security: Opportunities and challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit*, June 2021, pp. 616–621.

[2] A. S. Abdalla *et al.*, "Toward next generation open radio access networks–what O-RAN can and cannot do!" *IEEE Network*, pp. 1–8, 2022.

[3] A. Thantharate *et al.*, "Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond," in *Proc. 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 852–857.

[4] Q. Liu *et al.*, "Learning-assisted secure end-to-end network slicing for cyber-physical systems," *IEEE Network*, vol. 34, no. 3, pp. 37–43, 2020.

[5] D. Johnson *et al.*, "Nexran: Closed-loop ran slicing in powder -a top-to-bottom open-source open-ran use case," in *Proc. ACM WiNTECH*, 2021, p. 17–23.