xApps for DDoS Attacks Detection and Mitigation in 5G-V2X O-RAN Networks

Mirna Awad, Adam Ait Hamid, Yeogeuch Ranganathan, Nizar Choubik, Rami Langar, and Wael Jaafar

***Abstract*—In this demo, we present a 5G prototype designed to secure V2X communications by leveraging the concept of distributed applications (xApps) in 5G O-RAN. Based on the open-source srsRAN, our framework protects against DDoS attacks by implementing a dual-xApp strategy. The first xApp, called attack detection (AD) detects and identifies DDoS attackers in real-time, using deep learning. The second xApp, named resource control (RC), is executed dynamically to reduce the network resources of identified attackers. We show that our method effectively neutralizes malicious users by minimizing their impact on network performance while maintaining stable operations for legitimate users.**

I. Introduction

The advent of Open Radio Access Networks (O-RAN) has revolutionized the architecture of 5G networks and beyond, offering a flexible, scalable, and vendor-neutral approach that separates hardware and software functions. While this architecture promotes innovation and adaptability, it also exposes the network to vulnerabilities [1]. The disaggregation inherent in O-RAN, which splits network functions into various modular units, creates new entry points for potential cyberattacks. Moreover, traditional security mechanisms are no longer sufficient in these highly dynamic and heterogeneous contexts of 5G networks.

One of the most pressing concerns is the susceptibility of O-RAN-enabled 5G networks to Distributed Denial of Service (DDoS) attacks, which can overwhelm network resources, disrupt services, and compromise the overall performance of the system. In the context of Vehicle-to-Everything (V2X) communications [2], where latency and reliability are essential, such disruptions can have severe consequences, potentially jeopardizing the safety and operations of autonomous vehicles. Consequently, ensuring real-time detection and mitigation of security threats in O-RAN 5G networks is critical.

Our proposed solution consists of integrating deep learning techniques with the O-RAN architecture to detect and mitigate DDoS attacks in real time, ensuring uninterrupted operation of critical applications like autonomous driving. It leverages the Near Real-Time RAN Intelligent Controller (RIC), a pivotal component of O-RAN framework, to implement and deploy advanced security solutions through xApps—software applications designed to enhance network intelligence and responsiveness within the RAN [3].

To demonstrate our solution, we present in this paper a novel 5G prototype framework that aligns with O-RAN principles and integrates machine learning (ML)-driven xApps to detect and mitigate DDoS attacks. Specifically, two xApps were developed, namely the "Attack Detection" (AD) xApp and the "Resource Control" (RC) xApp. The AD xApp continuously monitors live traffic between the RAN and the core network to identify patterns indicative of DDoS attacks. By leveraging deep learning, this xApp detects malicious traffic and flags suspicious IP addresses. At the same time, the RC xApp dynamically reallocates network resources in response to detected attacks. Once an attacker is identified, RC xApp limits the bandwidth available to the malicious user, thereby preventing resource exhaustion for legitimate users. Our framework supports a hybrid environment, integrating both virtual and physical users, demonstrating its versatility and applicability across various 5G use-cases. Our demonstration shows the effectiveness of our xApps in detecting and mitigating DDoS attacks by limiting the bandwidth resources of attackers and limiting the impact on the services of other legitimate users.

The paper is organized as follows: Section II describes our designed 5G framework, explaining its architecture, as well as our xApps for DDoS attack detection and mitigation, while section III describes our demo and obtained results.

II. Framework Description

Our 5G framework is designed to align with O-RAN architecture, emphasizing a disaggregated RAN that enables flexible and scalable network deployments. The architecture supports both physical and virtual User Equipment (UE), providing a hybrid environment that is essential for testing and implementing advanced security solutions in various 5G-related contexts, including V2X communications. Fig.1 provides an overview of our platform's components.

Central to this architecture is the gNodeB (gNB), implemented using the srsRAN 5G project [4]. The gNB is split into a Central Unit (CU) and two Distributed Units (DU1 and DU2), a configuration that reflects the modular and scalable nature of O-RAN. The CU is responsible for handling non-real-time processing and interfacing with the core network, which is implemented using a dockerized instance of Open5GS [5]. DU1 is connected to a

This work was supported by the ANR 5G-INSIGHT project (Grant no. ANR-20-CE25-0015), and by the Innovation for Defence Excellence and Security (IDEaS) program of the Department of National Defence Canada.

Mirna Awad, Rami Langar, and Wael Jaafar are with École de Technologie Supérieure (ÉTS), Montréal, Canada (e-mails: {cc-mirna.awad, rami.langar, wael.jaafar}@etsmtl.ca). Adam Ait Hamid is with University Gustave Eiffel, France (e-mail: adam.ait-hamid@univ-eiffel.fr). Yeogeuch Ranganathan is with Polytech Sorbonne, Paris, France (e-mail: yeogeuch.ranganathan@etu.sorbonne-universite.fr). Nizar Choubik is with INP Bordeaux, France (e-mail: nchoubik@bordeaux-inp.fr).

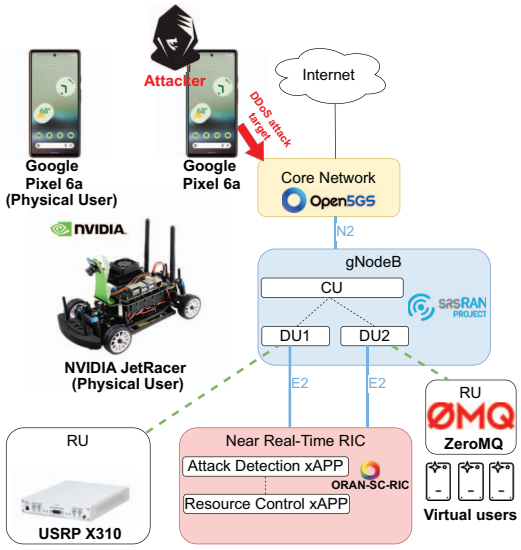

Fig. 1. Architecture and components of the O-RAN based 5G-V2X prototype.

USRP X310 card using the UHD driver to facilitate the management of physical UEs, including smartphones and the JetRacer robot. These devices represent the physical layer of our testbed and are critical in demonstrating the framework's effectiveness in a V2X environment. In contrast, DU2 utilizes the *ZeroMQ* protocol to manage virtual UEs, instantiated through the srsUE framework. This hybrid approach allows our framework to accommodate both physical and virtual users, thus enhancing its versatility and applicability for different scenarios.

At the heart of our platform's intelligence is the Near Real-Time RIC, deployed in a dockerized environment using the O-RAN Software Community's ORAN SC Controller [3]. The RIC is essential for managing radio resources dynamically and for executing xApps that enhance both the performance and security of the network. We have implemented two key xApps on the RIC: 1) *AD xApp:* This ML-driven xApp continuously analyzes live traffic on the network interface between the RAN and the core network. It uses a Convolutional Neural Network (CNN) learning model based on *LUCID* [6] to detect DDoS attacks and identify suspicious IP addresses associated with malicious traffic. This real-time attack detection method enables preemptive action before attackers can cause significant harm to the network, and 2) *RC xApp:* Upon detection of a potential DDoS attack, this xApp intervenes by dynamically reallocating network resources to effectively limit the bandwidth available to the attacker and mitigate the impact of the attack, thus ensuring that legitimate users are not adversely affected. The proposed framework not only ensures the security and stability of the network but also highlights the potential integration of ML-driven cybersecurity solutions within the O-RAN architecture.

III. Demo Description and Results

The demonstration is designed to validate the effectiveness of our 5G prototype framework in detecting and mitigating DDoS attacks within an O-RAN-enabled 5G-V2X system. The demo setup involves a hybrid configuration that includes both physical and virtual UEs, reflecting a real scenario for V2X. The UEs consist of two *Google Pixel 6a* smartphones and a *Waveshare Nvidia JetRacer* robot connected to the 5G network via a smartphone hotspot. The robot relies on real-time updates from a remote edge server located in the RAN to maintain its trajectory. Also, we consider a single virtual UE.

After launching the platform's components and connecting UEs, we experiment with two scenarios 1 and 2. In Scenario 1, a DDoS attack is launched using the *Mausezahn* tool [7], executed from an Ubuntu PC connected to the smartphone's hotspot, and where AD and RC xApps are inactive. The attack targets the 5G core network by flooding it with malicious traffic and disrupt communications between UEs and the core network. Once started, DDoS degrades the network's performance and disruptions are rapidly noticed. Hence, the robot exhibits abnormal behavior, such as deviating from its intended path or losing stability. This disruption demonstrates the vulnerability of O-RAN 5G networks to DDoS, particularly for critical V2X applications. In Scenario 2, the same experiment is repeated with our AD and RC xApps activated. The AD xApp continuously monitors the network traffic and identifies malicious patterns characteristic of DDoS. We demonstrate the xApp's efficiency through, in addition to DDoS traffic, the generation of benign traffic from a smartphone (ICMP Ping) and the virtual UE (HTTP traffic). Upon detecting the attack, the AD xApp flags the IP address of the attacker for immediate intervention. In response, the RC xApp dynamically reallocates network resources, in particular by reducing the bandwidth available to the attacker. By doing so, the impact of the DDoS attack is minimized while ensuring that legitimate users continue to operate seamlessly. With both xApps being activated, the robot regains stable communication with the server, thus operating normally and maintaining its trajectory without disruptions.

Our short demo video can be found at [8]. The results of this demonstration highlight the effectiveness of our O-RAN 5G framework for DDoS attack detection and mitigation in real-time. The proposed xApps efficiently identify and neutralize DDoS while preserving the network's stability.

References

[1] M. Liyanage, A. Braeken, and al., "Open RAN security: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 214, p. 103621, 2023.

[2] R. Sedar, C. Kalalas, and al., "A comprehensive survey of V2X cybersecurity mechanisms and future research paths," *IEEE Op. J. Commun. Soc.*, vol. 4, pp. 325–391, 2023.

[3] O.-R. ALLIANCE. O-RAN SC Projects. [Online]. Available: https://docs.o-ran-sc.org/en/latest/projects.html#near-realtime-ran-intelligent-controller-ric

[4] SRS. srsRAN Project. [Online]. Available: https://www.srsran.com/5g

[5] [Online]. Available: https://open5gs.org/

[6] R. Doriguzzi-Corin, S. Millar, and al., "Lucid: A practical, lightweight deep learning solution for DDoS attack detection," *IEEE Trans. Netw. Serv. Mngt.*, vol. 17, no. 2, 2020.

[7] Netsniff-ng. Mausezahn. [Online]. Available: http://netsniff-ng.org/

[8] xApps for DDoS Attacks Detection and Mitigation in 5G-V2X O-RAN Networks (Demo Video). [Online]. Available: https://youtu.be/eKtyxKewMo4