IEEE INFOCOM WKSHPS: The 11th International Workshop on Computer and Networking Experimental Research using Testbeds (CNERT 2024)

Advancing O-RAN Security: Integrated Intrusion Detection and Secure Slicing xApps

Mohammadreza Kouchaki, Joshua Moore, Minglong Zhang, Vuk Marojevic
Department of Electrical and Computer Engineering, Mississippi State University, USA
Email: {mk1682, jjm702, mz354, vm602}@msstate.edu

IEEE INFOCOM 2024 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) | 979-8-3503-8447-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/INFOCOMWKSHPS61880.2024.10620781

***Abstract*—This paper introduces a novel cellular network security framework that leverages the O-RAN architecture. Central to this framework are two innovative xApps: the Intrusion Detection System xApp (IDSx xApp) and the Secure Slicing xApp (SSxApp). The IDSx xApp employs a self-attention enhanced recursive neural network autoencoder for efficient and precise intrusion detection. The SSxApp is designed for dynamic resource management, ensuring secure network slicing. This integrated approach significantly enhances network resilience against evolving wireless network security threats. This research provides valuable insights into the development and efficacy of these xApps, demonstrating their critical role in safeguarding next-generation cellular networks.**

Keywords: 5G security, real-time intrusion detection, threat detection, secure slicing, O-RAN, xApps.

I. Introduction

The Open Radio Access Network (O-RAN) increases network flexibility, diversity, and performance. However, many security challenges persist in this operating environment. Traditional security frameworks, which were designed for less dynamic networks, are inadequate for O-RAN's unique requirements. Recent studies highlight the vulnerability of O-RAN to sophisticated attacks, including malicious xApps, encryption issues, and risks from artificial intelligence (AI)/ machine learning (ML) algorithms. This evolving threat landscape emphasizes the urgent need for robust and adaptable security measures in O-RAN [1]. Of significant concern are active attacks, including sophisticated jamming and data channel intrusion attacks, which can result in severe consequences such as service outages, privacy breaches, and degraded quality levels, jeopardizing network security, privacy, and availability for end users. The open nature of O-RAN, coupled with commercial off-the-shelf software-defined radios (SDRs), intensifies these risks, creating an environment conducive to cellular attacks, including fake base stations (BS) and malicious user equipment (UEs).

This work addresses challenges in O-RAN through pioneering contributions to intrusion detection and network slicing. We develop an enhanced Recurrent Neural Network (RNN)-based autoencoder with a self-attention layer in the encoder. This innovative approach leverages self-attention mechanisms from transformer architectures to overcome the computational barriers of O-RAN deployments. Additionally, we use Kubernetes for resource allocation to our intrusion detection xApp. Our solution includes two distinct but interactive xApps: the Intrusion Detection System xApp (*IDSx xApp*) for intrusion detection and the Secure Slicing xApp (*SSxApp*) [2] for secure network slicing. The *IDSx xApp* excels in detecting network anomalies, employing the enhanced RNN-based autoencoder with self-attention to effectively identify both known and unknown intrusion strategies. Upon receiving alerts from the *IDSx xApp*, the *SSxApp* dynamically manages network resources to isolate malicious users and safeguard legitimate communication channels. This dual-xApp approach ensures a robust, adaptive, and resilient defense mechanism, safeguarding O-RAN against the evolving landscape of security threats.

The rest of the paper is organized as follows: Section II outlines the O-RAN architecture, followed by the introduction of the proposed xApps. Section IV presents the results. Appendix A provides the demonstration details.

II. O-RAN Architecture

The O-RAN architecture, which is sketched on the left part of Fig. 1, is designed for intelligent network operations. The O-RAN radio unit (O-RU) is responsible for the lower portion of the physical layer. The distributed unit (O-DU) implements the radio link control (RLC), medium access control (MAC), and the higher part of the PHY layer. The Central Unit (O-CU) encapsulates the higher protocol layers. Central and unique to O-RAN are the Near-Real Time RAN Intelligence Controller (Near-RT RIC) and the Non-RT RIC. The Near-RT RIC usually encompasses various xAPPs, which may employ AI/ML to enhance functional extensibility and operational efficiency of the network. The Non-RT RIC focuses on the workflow management and policy guidance. Communication among these components is facilitated via open interfaces, such as E2 and O1 for connecting the Near-RT RIC and the service management and operations (SMO) with the RAN, respectively, and A1 between the Non-RT and the Near-RT RICs [3].

III. xApps Design and Development

A. Design Method

An xApp provides a microservice and is a containerized application designed to be deployed on a Kubernetes platform. We use a Python-based xApp framework, which provides essential features for xApp development, including initialization, health check, communication through the RIC Management Router (RMR) and the Shared Data Layer (SDL). The development process involves delineating primary functions and operations including the creation of data processing classes, AI/ML model, and facilitating interaction with other components and xApps. Containerization

979-8-3503-8447-5/24/$31.00 ©2024 IEEE

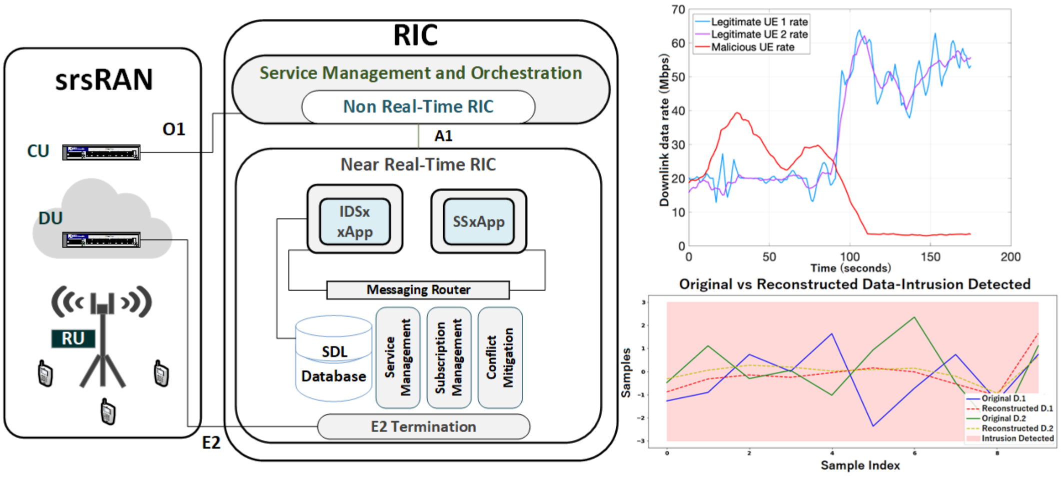

Fig. 1: O-RAN security architecture (left); intrusion detection (IDSx xApp) and throughput control (SSxApp) (right).

is achieved with Docker. This includes creating Docker images and configuring their deployment as pods within the Kubernetes cluster. Upon deployment, the xApp undergoes an onboarding process. Once onboarded, it is capable of interacting with the RAN infrastructure through the E2 interface and with other xApps via the SDL and RMR [4].

B. Intrusion Dtection: IDSx xApp

The *IDSx xApp* leverages an advanced RNN-based autoencoder with multi-head attention. It specializes on time-series anomaly analysis, essential for network security. The architecture integrates an encoder, transforming data into a latent space, and a decoder for reconstruction. Its RNN component, which is critical for temporal data handling, is enhanced with recursive connections. Key to this model is the self-attention mechanism in the encoding phase, which calculates and normalizes the alignment scores to form attention weights. These weights create a context vector, emphasizing the important data segments for effective anomaly detection. The model incorporates Long Short-Term Memory (LSTM) units to mitigate the vanishing gradient problem of RNNs, ensuring long-term data retention and processing. This integration of LSTM and self-attention in the encoder forms a powerful solution for anomaly detection using autoencoders.

C. Secure Slicing: SSxApp

Once the *IDSx xApp* identifies network intrusions, it communicates this information to the *SSxApp* via the RMR for initiating secure slicing in O-RAN. *SSxApp*, adapting OAIC's [1] near-RT RIC framework, uses a customized version of srsRAN with a slice-aware scheduler for resource block allocation within network slices. The setup, integrating the E2 agent of OAIC's RIC, enables *SSxApp* to enforce security policies, aligning with real-time RAN traffic and user requirements. The SSxApp deployment, managed through the command line or REST application programming interfaces, facilitates continuous monitoring and adaptive slicing based on service model metrics, addressing user-specific needs via asynchronous E2 control messages. The *IDSx xApp* and *SSxApp* collaborate to maintain network integrity. The *IDSx xApp* identifies malicious UEs, and the *SSxApp* responds by binding them to an isolated slice with limited or no resources. This dynamic interplay ensures swift isolation of malicious UEs, securing and optimizing resource distribution among legitimate network users.

IV. Deployment and Results

We fine-tune, train and test the intrusion detection *IDSx xApp* by creating diverse wireless attack scenarios. Central to our data driven strategy is the precise collection of UE-gNodeB communication patterns, which includes traffic patterns, signal strength, error rates, packet sizes, and frequency of connections. Abnormal patterns can be recognized by the *IDSx xApp* through its fully trained model. Upon detecting an anomaly, the *IDSx xApp* interacts with the *SSxApp* via the RMR. The *SSxApp* then reallocates resources and isolates suspicious UEs to a separate network slice, ensuring effective mitigation of a potential threat. The right part of Fig. 1 illustrates that the *SSxApp* moves the malicious UE (e.g., a jammer) to the insecure slice and largely reduces its accessible resources (i.e., bandwidth and time), thus suppressing its data rate, once jamming signals are detected at time 90 second, which is detected by the *IDSx xApp*.

Acknowledgment

This work is supported by NSF and OUSD under Grant ITE2326898, as part of the NSF Convergence Accelerator Track G: Securely Operating Through 5G Infrastructure Program and CNS-2120442.

References

[1] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN Security: Challenges and opportunities," 2022.

[2] J. Moore, A. S. Abdalla, M. Zhang, and V. Marojevic, "Demo: SSxApp: Secure Slicing for O-RAN Deployments," in *2023 IEEE Military Communications Conference (MILCOM)*, 2023, pp. 251–252.

[3] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1376–1411, 2023.

[4] M. Kouchaki and V. Marojevic, "Actor-critic network for O-RAN resource allocation: xApp design, deployment, and analysis," in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 968–973.

[1] OAIC: https://www.openaicellular.org/