RF Device Fingerprinting Over Open Radio Access Networks

Saurabh Parkar, Xiaochan Xue, and Shucheng Yu

Introduction

Open Radio Access Networks (O-RAN) aim to transform cellular networks by promoting a virtualized, open, and intelligent architecture. O-RAN facilitates multi-vendor interoperability and optimization through data-driven closed-loop control by connecting disaggregated components via open interfaces and using intelligent controllers. Security in O-RAN can be enhanced with RF fingerprinting, which uses unique hardware imperfections in radio devices to create distinct fingerprints.

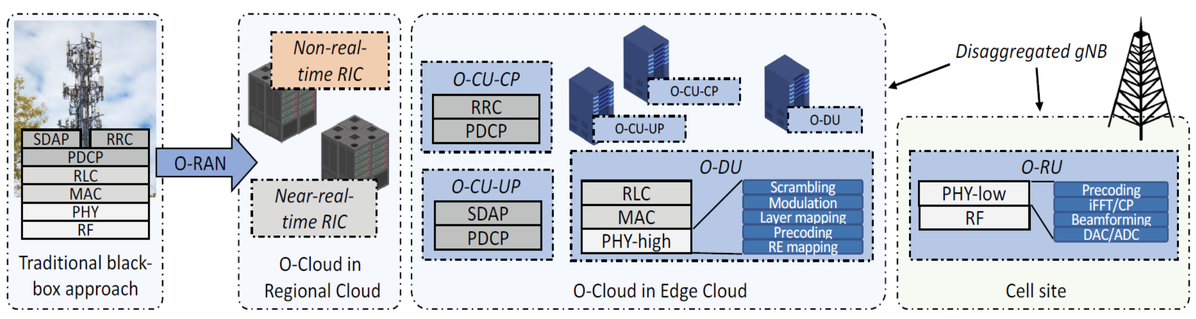

Fig 1. Evolution of the traditional black-box base station architecture (left) toward a virtualized gNB with a functional split (right, including the CU and DU at the edge, and the RU at the cell site).

Background

In traditional cellular networks, the communication process between User Equipment (UE) and base stations (eNB) is vulnerable to security threats like message interception or device impersonation. To address these risks, RF fingerprinting leverages unique hardware imperfections in devices to create distinct and identifiable fingerprints.

By analyzing RF signals, features such as I/Q imbalance, phase noise, and frequency offset can be extracted for device identification and authentication at the physical layer.

Our approach uses Channel State Information (CSI) for RF fingerprinting within the O-RAN framework. Key features identified were the magnitude and phase vectors, which showed consistent and distinguishing patterns unique to each device despite environmental variations. Our deep learning model processes these magnitude and phase vectors using convolutional layers to identify unique device patterns. This model effectively classifies devices based on their CSI data, achieving high accuracy in identification. By focusing on robust features, our approach enhances security and device management within O-RAN, leveraging its disaggregated and intelligent architecture to implement federated learning for continuous model improvement without centralizing sensitive data.

Fig 2.Unique Patterns obtained from CSI of User Equipment at base-stations. (a) Magnitude Patterns Obtained at base-stations, (b) Magnitude Patterns Obtained at base-stations

Our Methodology

POWDER Wireless testbed is used to simulate an O-RAN environment with USRP X-310s for base-stations and B-200s for user equipment. The base-stations are connected to a Near RT-RIC using ORAN's E2-Interface.

CSI data is collected using GNURadio simulating Wi-Fi Signal Transmissions under IEEE 802.11p standards.

The Deep Learning model is built with convolutional layers to process the magnitude and phase vectors extracted from CSI data. These attributes were chosen due to their consistent and distinct patterns and robustness to noise and interference. The model is trained in a federated learning approach at base-stations with an xAPP at Near RT-RIC acting as a central node for weights aggregation.

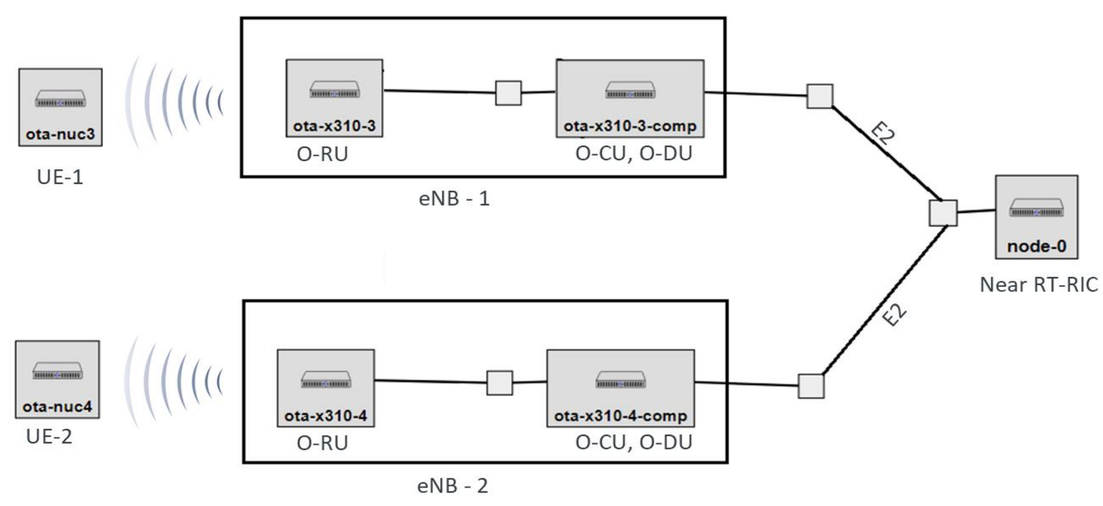

Fig 6. ORAN Topology over Powder

Simulation Results

Initial training on a single node resulted in a training accuracy of 99.42% and a validation accuracy of 97.69%. This high accuracy indicates the effectiveness of using CSI data for device fingerprinting.

Implementing Federated Learning across multiple base stations showed comparable results. Training accuracy reached 99.63% and 99.75% on different eNBs, with validation accuracies of 98.46% and 98.61%, respectively. This distributed approach ensures continuous model improvement while preserving data privacy.

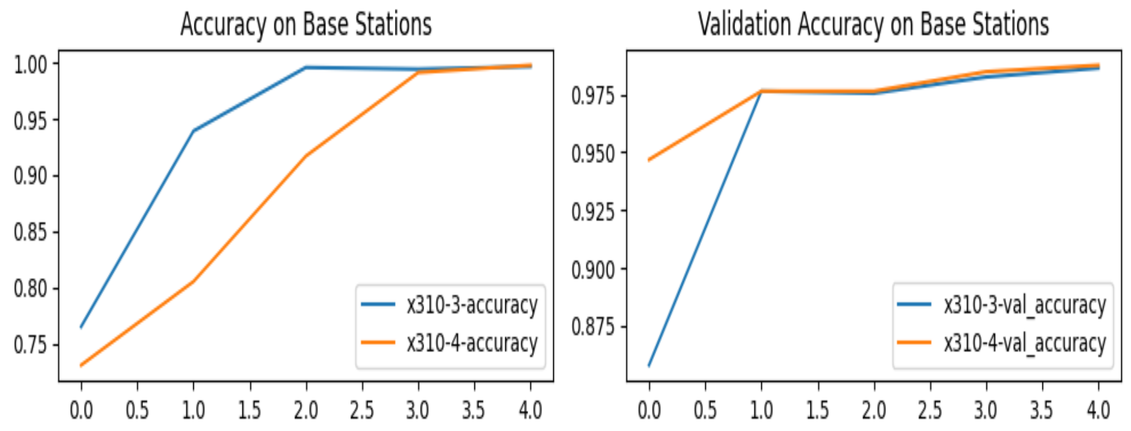

Fig 4. Model Accuracies on base-stations.

Conclusion

Our ORAN simulation has displayed the feasibility of integrating a deep learning methodologies for RF device fingerprinting within the O-RAN framework. The federated learning method allows for distributed training across multiple base stations, ensuring continuous model improvement without centralizing sensitive data. The results highlight the potential of advanced AI techniques in dynamically and efficiently managing complex, heterogeneous networks.

References

[1] M. Polese, L. Bonati, et al., "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," arXiv:2202.01032, 2022.

[2] A. Al-Shawabka, F. Restuccia, et al., "Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting," in IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, 2020, pp. 646-655. doi: 10.1109/INFOCOM41043.2020.9155259.