Federated Learning for Devices Fingerprinting in Open Radio Access Networks

Saurabh Parkar
ECE Department
Stevens Institute of Technology
Hoboken, USA
sparkar@stevens.edu

Xiaochan Xue
ECE Department
Stevens Institute of Technology
Hoboken, USA
xxue2@stevens.edu

Dr. Shucheng Yu
ECE Department
Stevens Institute of Technology
Hoboken, USA
syu19@stevens.edu

***Abstract*—Open Radio Access Network (O-RAN) offers a transformative approach to cellular network design by promoting a virtualized, open, and intelligent architecture. The increasing complexity and security demands of modern cellular networks necessitate robust methods for device identification and management. This paper provides a way for integrating Federated Learning for device fingerprinting within the Open Radio Access Network (O-RAN) framework, enhancing network security and device management. Our approach leverages unique RF signal characteristics, captured through Channel State Information (CSI), to identify devices without the need for centralized data processing or custom hardware. We set up a real-world experimental environment using the POWDER Wireless testbed, simulating O-RAN with base stations and user equipment. Using a deep learning model to process the CSI data to classify devices. With an xAPP deployed on a Near Real-Time Radio Intelligent Controller (RT-RIC), our model uses a federated learning approach for distributed training across base stations. Initial results demonstrate nearly 99.75% accuracy in device identification, showcasing the potential of our approach to integrate advanced AI techniques in O-RAN for improved network performance and security. This research underscores the feasibility and practical effectiveness of enhancing next-generation cellular networks through O-RAN's open and intelligent architecture.**

Keywords*—*Federated Learning, Fingerprinting, O-RAN, CSI, xAPP.

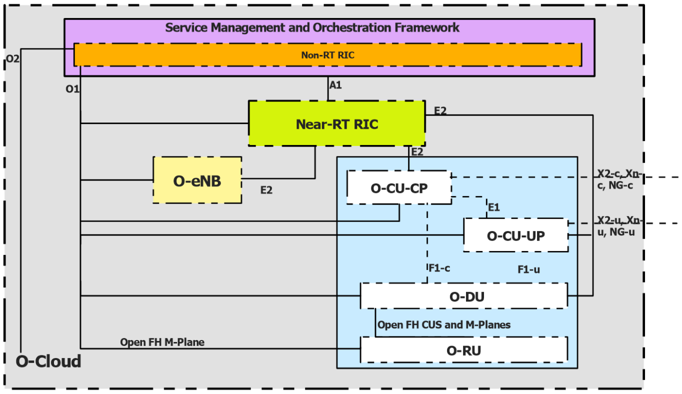


Fig. 1: O-RAN Architecture [1]

I. Introduction

Open Radio Access Networks (O-RAN) present a transformative approach to designing, deploying, and operating cellular networks. It aims to revolutionize the telecom ecosystem by promoting a virtualized, open and intelligent RAN architecture. O-RAN enables disaggregated components to be connected via open interfaces and optimized through intelligent controllers, supporting multi-vendor interoperability and programmatic optimization through data-driven closed-loop control.The architecture is significantly shaped by the O-RAN Alliance, which standardizes open interfaces and promotes the integration of artificial intelligence (AI) and machine learning (ML) for efficient network management and optimization.[1]

O-RAN disaggregates traditional 5G base station architecture into three components: O-Central Unit (O-CU), O-Distributed Unit (O-DU), and O-Radio Unit (O-RU). The O-CU is further split into control plane (O-CU-CP) and user plane (O-CU-UP), allowing for specialized management of control and data traffic, which can be deployed at different locations. The O-DU handles real-time and near-real-time processing tasks for higher-layer PHY functions, making it suitable for edge deployment. The O-RU focuses on RF components and lower-PHY functions, deployed close to the antenna to simplify deployment and reduce costs. These units are connected via open and standardized interfaces, enhancing interoperability and flexibility. This disaggregation offers key benefits such as interoperability between different vendors' equipment, flexibility in deploying network functions, scalability to optimize resource utilization, and fostering innovation through open interfaces. Compared to traditional 5G base stations, O-RAN's architecture is more open, flexible, and cost-effective, enabling a multi-vendor ecosystem and supporting the development of new services and applications by third-party developers.[1]

O-RAN introduces applications of Artificial Intelligence and Machine Learning Methods into the traditional RAN structure through the integration of RAN Intelligent Controllers. The architecture incorporates two types of RAN Intelligent Controllers (RICs): the Non-Real-Time RIC (Non-RT RIC) and the Near-Real-Time RIC (Near-RT RIC). Near-RT RIC is designed to handle time-sensitive operations and operates in time range of 10ms to 1 second, it is responsible for RAN functions that require real-time control such as resource management. It can make adjustments quickly to ensure optimal network performance. Non-RT RICs handle tasks that are not time sensitive, and operate with time sensitivities of 1 second or greater. It focuses on long term optimization tasks such as policy-based managements and network analytics. It provides optimization policies to Near RT RIC to improve network's efficiency and performance over a longer period. These controllers facilitate intelligent control and orchestration of network resources through policy-based guidance, fine-grained data monitoring, and adaptive control actions. O-RAN's integration of AI and ML fundamentally enhances its capability to manage complex, heterogeneous networks dynamically and efficiently. The disaggregated and open nature of O-RAN allows for seamless incorporation of intelligent controllers that can autonomously optimize network operations, thereby improving performance, reducing costs, and enabling rapid deployment of innovative services. As research and development in this field progress, O-RAN is poised to be a cornerstone in the evolution of next-generation cellular networks.[2]

In a traditional cellular network architecture, the communication process between a User Equipment (UE) and a base station (eNB) involves several message exchanges to establish and maintain connectivity. Initially, the UE sends an access request to the eNB, which responds by prompting the UE for authentication. Throughout the session, data packets are continuously exchanged between the UE and eNB. This process, however, is vulnerable to security threats, such as malicious devices attempting to intercept messages or impersonate the UE or eNB. To mitigate such risks, RF device fingerprinting can be employed. This technique leverages the unique hardware-level imperfections in the radio circuitry of devices to create distinct fingerprints, enabling the identification and authentication of devices at the physical layer itself. By capturing and analyzing the RF signals, specific features such as I/Q imbalance, phase noise, and frequency offset can be extracted to identify the device. This technique enhances security in wireless networks by authenticating devices and detecting unauthorized access.[3] O-RAN can significantly enhance this security process by utilizing their RAN Intelligent Controllers (RICs) that leverage AI for dynamic network management and optimization.

In this paper we implement a Federated Learning workflow over the O-RAN architecture and provide a Radio Fingerprinting method to distinguish between communicating UEs at eNBs using their Channel State Information (CSI) obtained from their transmissions, specifically their Magnitude and and Phase information using a Deep Learning Model. Preliminary results from this model shows a accuracy of around 99%. To maintain the security of transmissions this model is trained at eNBs employing a Federated Learning Method with the Near RT-RIC acting as a global node where we deploy our xAPP which stores the DL Model and its weights and is updated based on training metrics received from eNBs.

The rest of the paper is organized as follows. Section II discusses related work. Our design is elaborated in Section III. The experimental evaluations are illustrated in Section IV. Section V shows the future research directions. Section VI concludes this paper.

II. Related Work

RF (Radio Frequency) fingerprinting's early developments starts as early as 1960s from military sector to modern applications in cellular networks. RF fingerprinting has emerged as a crucial technique for device identification and network security by leveraging unique hardware-specific imperfections in the RF signals of wireless devices. Researches in Radio-Fingerprinting based on slight device imperfections have been in works for a long period but most of these methods use traditional feature extraction approaches but with rise of Deep Learning Methods this task can be achieved more easily.

Channel State Information (CSI) for a network contains all the vital information for the channel in wireless communications. It includes data on how the signal propagates from the transmitter to the receiver, encompassing factors like path loss, scattering, fading, and power delay profile. Ref [4] explores the utilization of CSI in MIMO-OFDM (Multiple Input Multiple Output-Orthogonal Frequency Division Multiplexing) systems for device identification. The authors discuss how hardware-specific imperfections, such as phase noise from RF oscillators, can serve as reliable device fingerprints. They highlight the challenge posed by various sources of phase noise, including Time of Flight (ToF), Sampling Frequency Offset (SFO), and Carrier Frequency Offset (CFO), which complicate the extraction of unique device signatures. The proposed method focuses on isolating the unique phase noise introduced by the RF oscillators within a single transmitter, achieving high identification accuracy using off-the-shelf hardware in real-world settings. This study proves that even use of the same hardware devices still produce a varying results in their transmissions due to slight hardware imperfections and can be easily distinguished based on their CSI information, thus giving a chance to secure authentication on a network at a lower physical level.

In the work by ref. [3], they explore the use of employing a Convolutional Deep Learning Model for distinguishing RF devices based on their CSI information captured in various environmental conditions such as anechoic chambers, real-world scenarios, and wired connections. Their motivation for employing a deep learning (DL) model for RF fingerprinting arises from the unique capabilities of DL models, particularly convolutional neural networks (CNNs), to identify and learn complex and high-dimensional patterns within data. Traditional RF fingerprinting methods rely heavily on manually engineered features and shallow models that often fail to capture the subtle hardware imperfections that are unique to each wireless device. CNNs, with their powerful feature extraction capabilities, can automatically learn these patterns directly from raw I/Q samples, thereby eliminating the need for manual feature engineering. Additionally, DL models are inherently robust to variations in data, such as those introduced by different environmental conditions or channel states. This robustness is crucial for RF fingerprinting, where the wireless channel can introduce significant variability that traditional models may struggle to handle. Following this methodology we develop our model using convolutional layers to train on the CSI Information that we capture over the ORAN Architecture.

Federated Learning (FL) is a method of distributed machine learning that allows for training of models on local devices without sharing of data between devices and hence preserving privacy of data. FL's decentralized nature makes it suitable for environments where data privacy is a primary concern, such as Network Transmissions in this case. The survey by ref. [5] details on integration of Federated Learning within the ORAN architecture and how the distributed nature of FL works in combination with ORAN's decentralized structure. This integration of FL in ORAN provides with a several advantages such as enhanced data privacy, reduced latency, optimized resource utilization, and improved scalability.

III. Our Solution

To implement Federated Learning on O-RAN, we deploy a xAPP on a Near RT-RIC, this xAPP acts as a central node to all the base stations and stores the DL model and its weights. The Near RT-RIC is a crucial component of the O-RAN architecture, it has lower response times and helps in reducing latency in model updates and weight aggregation from several eNBs. When the RIC receives weight updates from all the participating eNBs, the xAPP aggregates weights and sends model updates back to continue training. The xAPP also stores these updates and Model Definition in its Shared Data Layer (SDL) for ease of access to model and reducing program overhead.

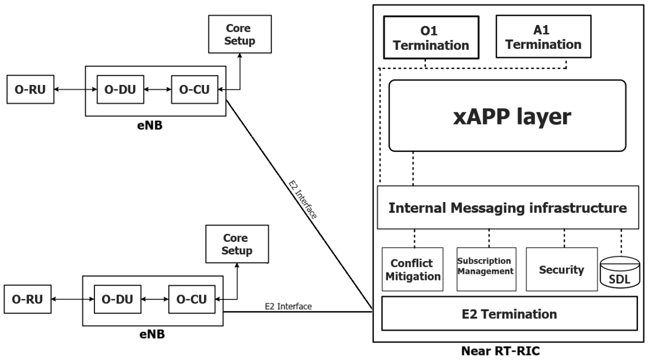


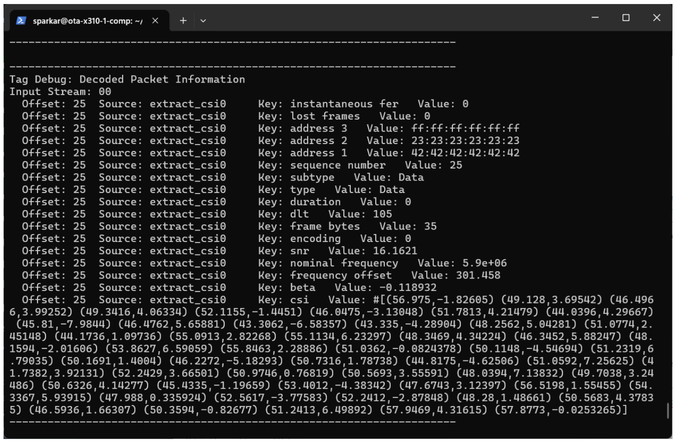
Fig. 2: Communication Between eNBs and RIC

O-RAN offers a disaggregated approach to base-stations. Here we make use of the disaggregated components O-RU and O-DU. The O-RU is responsible for collecting the Raw RF data and other Physical Layer Information from the communicating UEs over the network. We collect the CSI information at O-RU which is then forwarded to O-DU. The O-DU is well-suited for running a computationally intensive task such as model training since it is located closer to the edge computing layers and can utilize resources such as CPUs or GPUs more efficiently.

A. Description of Dataset

We transmitted internet packets using the Open-Source Software GNURadio and Wifi Signal Transmissions as simulated by ref [6] using the BPSK 1/2 encoding under the IEEE 802.11p standards for Transmissions at 5.89GHz. The packets were simple messages passed from UEs to eNBs. These transmissions were done by the simulated UEs to eNBs. At the eNB end we captured these packets and calculated CSI information from them.

Each packet consists of its related attributes such as Source Address (address 1), Destination Address (address 2) and its BSS Gateway (address 3) and a 52 vector raw I/Q data related to each of the packets as shown in fig. 3. Based on this information we setup our transmissions between the UEs and eNBs for 5 hours each for our Training Dataset and 1 hour for Test Dataset, and captured around 188222 combined packets as data points to train our model on.



```
-----------------------------------------------------------------------

-----------------------------------------------------------------------
Tag Debug: Decoded Packet Information
Input Stream: 00
  Offset: 25  Source: extract_csi0     Key: instantaneous fer   Value: 0
  Offset: 25  Source: extract_csi0     Key: lost frames   Value: 0
  Offset: 25  Source: extract_csi0     Key: address 3   Value: ff:ff:ff:ff:ff:ff
  Offset: 25  Source: extract_csi0     Key: address 2   Value: 23:23:23:23:23:23
  Offset: 25  Source: extract_csi0     Key: address 1   Value: 42:42:42:42:42:42
  Offset: 25  Source: extract_csi0     Key: sequence number   Value: 25
  Offset: 25  Source: extract_csi0     Key: subtype   Value: Data
  Offset: 25  Source: extract_csi0     Key: type   Value: Data
  Offset: 25  Source: extract_csi0     Key: duration   Value: 0
  Offset: 25  Source: extract_csi0     Key: dlt   Value: 105
  Offset: 25  Source: extract_csi0     Key: frame bytes   Value: 35
  Offset: 25  Source: extract_csi0     Key: encoding   Value: 0
  Offset: 25  Source: extract_csi0     Key: snr   Value: 16.1621
  Offset: 25  Source: extract_csi0     Key: nominal frequency   Value: 5.9e+06
  Offset: 25  Source: extract_csi0     Key: frequency offset   Value: 301.458
  Offset: 25  Source: extract_csi0     Key: beta   Value: -0.118932
  Offset: 25  Source: extract_csi0     Key: csi   Value: #[(56.975,-1.82605) (49.128,3.69542) (46.496
6,3.99252) (49.3416,4.06334) (52.1155,-1.4451) (46.0475,-3.13048) (51.7813,4.21479) (44.0396,4.29667)
 (45.81,-7.9844) (46.4762,5.65881) (43.3062,-6.58357) (43.335,-4.28904) (48.2562,5.04281) (51.0774,2.
45148) (44.1736,1.09736) (55.0913,2.82268) (55.1134,6.23297) (48.3469,4.34224) (46.3452,5.88247) (48.
1594,-2.01606) (53.8627,6.59059) (55.8463,2.28886) (51.0362,-0.0824378) (50.1148,-4.54694) (51.2319,6
.79035) (50.1691,1.4004) (46.2272,-5.18293) (50.7316,1.78738) (44.8175,-4.62506) (51.0592,7.25625) (4
1.7382,3.92131) (52.2429,3.66501) (50.9746,0.76819) (50.5693,3.55591) (48.0394,7.13832) (49.7038,3.24
486) (50.6326,4.14277) (45.4335,-1.19659) (53.4012,-4.38342) (47.6743,3.12397) (56.5198,1.55455) (54.
3367,5.93915) (47.988,0.335924) (52.5617,-3.77583) (52.2412,-2.87848) (48.28,1.48661) (50.5683,4.3783
5) (46.5936,1.66307) (50.3594,-0.82677) (51.2413,6.49892) (57.9469,4.31615) (57.8773,-0.0253265)]
-----------------------------------------------------------------------
```

Fig. 3: Decoded Information acquired from Packets

B. Deep Learning Model

For training the data points we built a two-input deep learning model to take the magnitude and phase vectors computed from packet's CSI for classification of UE devices based on their Transmissions fig. 4. Magnitude and Phase were decided to be the primary varying attributes, as they showed a consistent repeating pattern between them on both eNBs, despite these factors varying based on their environmental conditions they showed the most promising results in terms of effects of noise and interferences over the time of transmissions. The model makes uses of one dimensional convolutional layers to find patterns unique to each UE device to before concatenating and passing through further dense layers for classification.

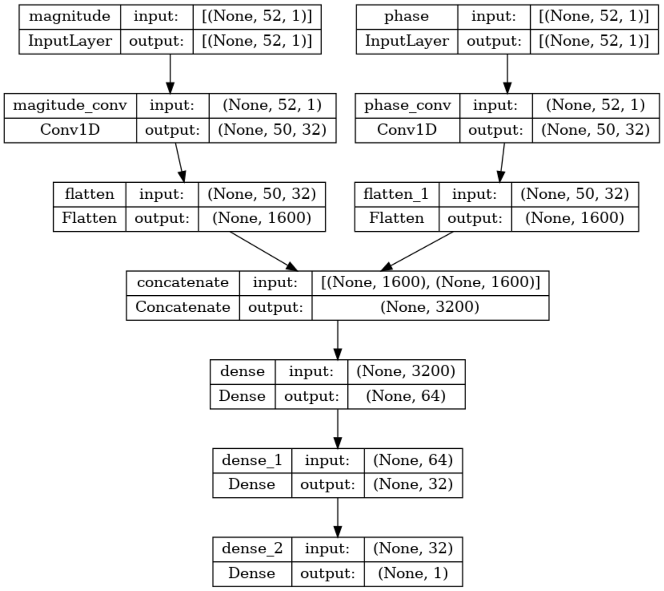


Fig. 4: Deep learning Model

C. Implementation Details

An x-APP is depolyed on Near Real-Time Radio intelligent Controller (RT-RIC) as a central node that stores our model and weights in the RIC's SDL and transmits it to the participating eNBs through the E2-interface, collects the weights from all the participating base stations and aggregates the weights of the model and transmits them back to the base stations as a approach to the federated learning.

The individual eNBs train on the transmissions received on their end for one epoch in mini-batch method to make sure that no data gets repeated and the model receives new data points for each training epoch and transmit weights to base station for aggregation. The approach is dynamic, any base station can join on the process at any time during training acquire the model and current weights and continue training from that state.

IV. Evaluation

A. Experiment Setup

Utilizing the Testbed provided by POWDER Wireless [7] we set up our experiments to simulate a Open Radio Access Network using X-310 USRPs to simulate Base Stations(eNB), and B-210 USRPs to simulate User Equipments(UE) on O-RAN connected to a Near RT-RIC through the E2 Interface.

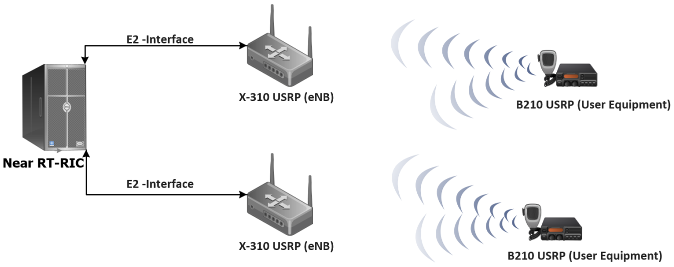


Fig. 5: O-RAN Setup on POWDER testbed

B. Collected Data Analysis

From the collected I/Q data from packets we analysed that the magnitude and phase were the two attributes that produced consistent patterns at the receiving base-stations and were the most distinguishing factors for each of the devices as shown in fig. 6 and fig. 7.

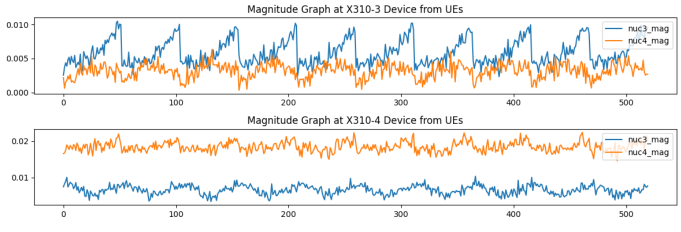


Fig. 6: Comparison of Magnitudes from Two UEs Received on each of the eNB

To set a baseline we first gathered all the data at a single node and trained on it in a 80-20 train-test split and achieved 99.42% percent accuracy on training and 97.69% accuracy on validation set as shown in fig. 8. This high accuracy was expected since both the devices give a easily distinguishable fingerprint, despite these factors being dependant on the physical and environmental factors such distances, location and radio interferences' between the X-310s and B210s.

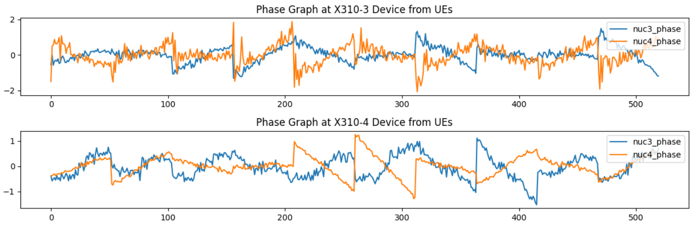


Fig. 7: Comparison of Phases from Two UEs Received on each of the eNBs

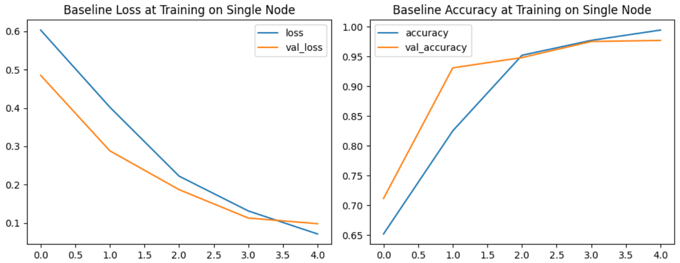


Fig. 8: Training metrics of Model Training on Single Node.

C. Federated Learning Results

Based on the previous results we then implemented the federated learning process on our O-RAN setup. The difference here with respect to baseline is that eNBs only train on their individual transmission received on their end and not on other eNBs as well. For federated learning we setup two eNBs connected to Near RT-RIC and two UEs as shown in fig 5. The results for federated learning show similar results as compared to the baseline model. This implementation is able to achieve a training accuracy of 99.63% and validation accuracy of 98.46% at one eNB and 99.75% training accuracy and 98.61% validation accuracy on the other as shown in fig 9.

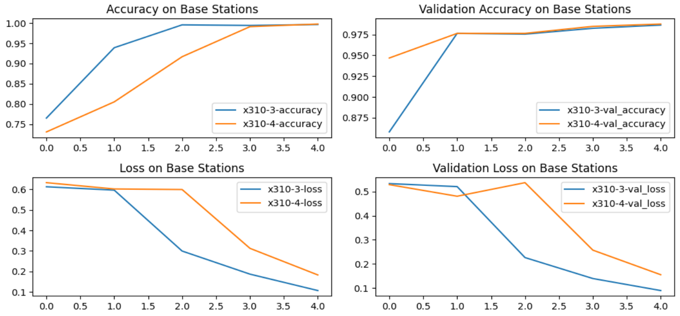


Fig. 9: Training Metrics of Model implemented in Federated Learning

V. Future Directions

Although the Radio Fingerprinting model here works with a high accuracy of 99% in this project it could be limited due to lack of availability of Datasets on Radio Transmissions history. This issue was also mentioned by ref. [3] wherein they state that despite the need for RF Fingerprinting on increase to enchance network security the lack of available resources and datasets makes it a tough challenge. Future work will focus on expanding the dataset to include a broader variety of RF devices and transmissions, aiming to further enhance the model's performance and generalizability across different O-RAN setups. This research underscores the promise of O-RAN's open and intelligent architecture in driving the evolution of next-generation cellular networks, paving the way for more secure, efficient, and scalable wireless communication systems.

VI. Conclusion

This paper has demonstrated the successful integration of Federated Learning and deep learning methodologies for radio device fingerprinting within the O-RAN framework. By leveraging unique imperfections in RF signals, we achieved highly accurate device identification, enhancing network security and device management. The experimental setup using the POWDER Wireless testbed and the deployment of the deep learning model on the Near RT-RIC showcased the feasibility and effectiveness of this approach. The federated learning method allowed 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. This research underscores the promise of O-RAN's open and intelligent architecture in driving the evolution of next-generation cellular networks, paving the way for more secure, efficient, and scalable wireless communication systems.

References

[1] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges," *arXiv preprint arXiv:2202.01032*, 2022.

[2] B. Brik, H. Chergui, L. Zanzi, F. Devoti, A. Ksentini, M. S. Siddiqui, X. Costa-Pérez, and C. Verikoukis, "A survey on explainable ai for sixth generation (6g) open radio access network (o-ran): Architecture, use cases, challenges and research directions," *arXiv preprint arXiv:2307.00319*, 2023.

[3] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. Costa Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, and T. Melodia, "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," pp. 646–655, 2020.

[4] L. N. Kandel, Z. Zhang, and S. Yu, "Exploiting csi-mimo for accurate and efficient device identification," pp. 1–6, 2019.

[5] N. Islam, F. Monir, M. M. Mahbubul Syeed, M. Hasan, and M. F. Uddin, "Federated learning integration in o- ran: A concise review," pp. 283–288, 2023.

[6] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "Performance Assessment of IEEE 802.11p with an Open Source SDR-based Prototype," *IEEE Transactions on Mobile Computing*, vol. 17, no. 5, pp. 1162–1175, May 2018.

[7] J. Breen, A. Buffmire, J. Duerig, K. Dutt, E. Eide, M. Hibler, D. Johnson, S. K. Kasera, E. Lewis, D. Maas, A. Orange, N. Patwari, D. Reading, R. Ricci, D. Schurig, L. B. Stoller, J. Van der Merwe, K. Webb, and G. Wong, "Powder: Platform for open wireless data-driven experimental research," p. 17–24, 2020. [Online]. Available: https://doi.org/10.1145/3411276.3412204