LocaRadio: RF Fingerprint-Based Location Authentication for Wireless Networks

Ebuka P Oguchi[‡], Hakim Lado [§], Ryan Evans[†], Ashwin Menon[†], Boyang Wang[†], Nirnimesh Ghose[§]
[‡]Department of Computer and Information Sciences, Spelman College;
[§]School of Computing, University of Nebraska-Lincoln;
[†]Department of Electrical and Computer Engineering, University of Cincinnati
ebukaoguchi@spelman.edu, hlado2@huskers.unl.edu,{evans2ra,menonar}@mail.uc.edu,
boyang.wang@uc.edu, nghose@unl.edu

***Abstract*—We present LocaRadio, a framework for authenticating the locations of wireless devices over RF signals for both indoor and outdoor environments. This novel secret-free authentication framework leverages unique wireless channel properties to verify the location authenticity of network devices. We collect a large-scale dataset with millions of I/Q samples from both indoor and outdoor environments. We exploit hard-to-forge physical layer features, specifically channel impulse response (CIR) signatures from the captured I/Q samples, to establish trust without requiring pre-shared secrets or complex key management. We leverage Convolutional Neural Networks (CNN) architectures (e.g., ResNet-18) to demonstrate the feasibility of location authentication, which achieves an average accuracy of 94.9% (up to 99.95%) in distinguishing legitimate location zones across indoor and outdoor environments. In addition, we also demonstrate that domain shifts caused by distance or hardware variations can be addressed by fine-tuning, restoring location authentication accuracy to more than 85%.**

I. Introduction

Physical-layer authentication (PLA) has gained increasing attention in wireless communication systems because it can be deployed efficiently in wireless systems without the need for a complex public key infrastructure [1]. Unlike traditional cryptographic techniques, PLA authenticates devices or users by exploiting unique characteristics of the wireless signal at the physical layer. Its advantages include low-latency processing, compatibility with heterogeneous environments, and the ability to complement higher-layer mechanisms as part of multi-factor authentication frameworks, thereby enhancing overall system security [1], [2]. When PLA incorporates location information, it leverages the inherent physical security of that location, providing an additional layer of protection. Location-based authentication is therefore well-suited to ubiquitous wireless systems, with applications ranging from safeguarding against compromised credentials to enabling decentralized device-to-device (D2D) authentication [3].

Conventional authentication schemes in wireless systems generally rely on cryptographic techniques such as symmetric keys, passwords, or public key infrastructure [4]. While effective in many settings, these schemes face several limitations in wireless deployments: they require secure key distribution and management in resource-constrained environments, are vulnerable to key compromise attacks, and impose computational overheads that may exceed the capabilities of low-power or underground sensors. Moreover, they remain susceptible to advanced threats such as signal poisoning, message injection, adversarial model extraction, channel manipulation, and replay attacks. To overcome these challenges, PLA has emerged as a complementary solution that leverages the inherent, location-dependent characteristics of wireless channels for secret-free trust establishment. Unlike cryptographic methods that depend on shared secrets, PLA exploits intrinsic channel properties that are tied to the transmitter's physical position, making them extremely difficult for adversaries to forge or reproduce from unauthorized locations.

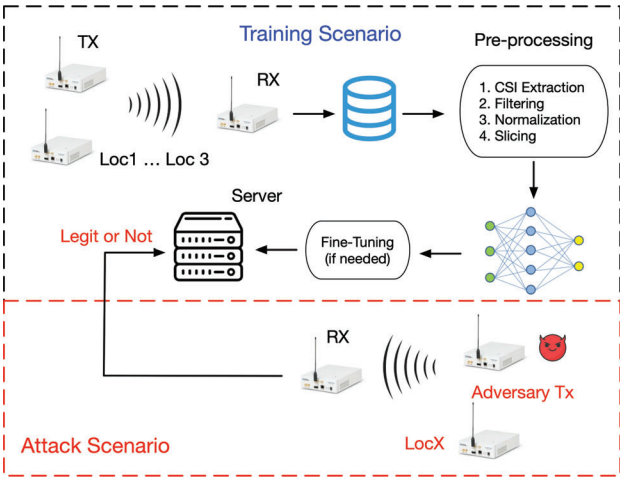


Fig. 1. System overview showing the preprocessing, training, and fine-tuning (if needed) for legitimate locations, then the adversarial attack from location X.

Unique channel-dependent features such as channel state information (CSI), channel impulse response (CIR), and received signal strength (RSS) provide intrinsic, hard-to-forge properties that make them valuable for building secure authentication mechanisms. The distinguishing behaviors of these physical-layer characteristics across different communication channels can be systematically analyzed, measured, and extracted through both model-driven and deep learning approaches, enabling accurate verification of the spatial authenticity of wireless transmissions. For example, CIR fingerprints can be stored as location authentication templates and subsequently compared with newly acquired measurements to determine

whether a device is transmitting from its claimed position [5]–[7].

In this work, we introduce LocaRadio, a framework for authenticating the locations of wireless devices over RF signals for both indoor and outdoor environments. It is a secret-free authentication framework tailored to heterogeneous environments. As illustrated in Fig. 1, LocaRadio leverages hard-to-forge physical-layer features, specifically CIR signatures extracted from received RF signals on the receiver side, to infer locations of transmitters and provide location-based trust establishment without relying on pre-shared secrets or complex key management. The system employs machine learning models to distinguish location-specific channel fingerprints and uses them for location verification, determining whether a transmission originates from a legitimate, pre-authorized location. By exploiting unique channel signatures tied to the physical environment, LocaRadio ensures confidentiality, integrity, and authentication for nodes deployed in wireless networks.

This work's fundamental contribution is a robust location-based authentication framework that enables secret-free trust establishment for wireless devices.

- We present LocaRadio, a secret-free location authentication framework for wireless networks that leverages physical layer characteristics to verify location authenticity without requiring cryptographic key distribution or management. Specifically, we extract CIR information from raw I/Q samples and adopt *Butterworth low-pass filtering* to further filter the data.
- We design and conduct extensive experiments using BPSK-modulated signals with USRP devices across indoor and outdoor scenarios, capturing spatial and temporal variations in real-world settings and demonstrating the feasibility of extracted CIR-based location verification in diverse wireless environments. Our dataset consists of millions of I/Q samples with over 40 GBs in total.
- We evaluate multiple neural network architectures (e.g., ResNet-18) to distinguish location information based on extracted CIR. In addition, we apply fine-tuning to address domain shifts in RF signals and enhance the robustness across diverse environmental conditions, device variations, and domain shifts, improving model generalization across varied wireless environments.
- We provide comprehensive security analysis against sophisticated adversaries using ray-tracing enhanced attackers using advanced channel modeling, demonstrating complete resistance to location spoofing attempts (adversaries achieve only random guessing performance).

Organization. In §II, we discuss the state of the art; next in §III, we introduce the overview of our authentication system. §IV describes the data collection setup, preprocessing, and how we extract CIR information from raw RF signals. §V shows the experimental evaluation. Finally, §VI concludes this work.

TABLE I
COMPARISON OF STATE-OF-THE-ART AND LOCARADIO (OURS)

Method	Indoor & Outdoor	LoS & NLoS
RSS-based [8], [9]	✗	✓
CSI-based [10], [11]	✗	✓
CIR-based [12], [13]	✗	✓
LocaRadio: Ours	✓	✓

II. RELATED WORK

In this section, we discuss the state of the art in location fingerprinting. Table I compares LocaRadio with state-of-the-art location-based authentication approaches.

Location fingerprinting techniques have evolved significantly across different wireless environments. Traditional approaches using RSS [8], [9], CSI [10], [11], and CIR [12], [13] measurements have proven effective in controlled indoor environments, enabling applications such as indoor localization and access control. Similar methods have also been used for outdoor localization [14].

Jin *et al.* experimentally demonstrated the impact of dust in RSS-based localization. Their experimental results show that the average positioning error remains below 6 cm under different dust accumulations [8]. Pu *et al.* introduced a reconfigurable intelligent surface (RIS)-assisted localization approach that employs a variational autoencoder-convolutional neural network (VAE-CNN) generative adversarial network to enhance noisy and low-discriminative RSS features for improved positioning accuracy [9]. Liu *et al.* proposed a Wi-Fi indoor localization method, MSPCA-GTCN, that models access point relationships as an undirected graph and leverages fine-grained CSI fingerprints enhanced through multiscale principal component analysis [10]. Xun *et al.* utilized a deep neural network for passive indoor localization using CSI signals [11]. Liu *et al.* proposed a hard sample meta-learning (HSML) framework for NLoS identification in UWB positioning systems, enabling robust performance across dynamic environments through a two-phase meta-training and fine-grained meta-testing process using CIR data from multiple scenarios [12].

Device fingerprinting has been applied over a broad spectrum of platforms, including Wi-Fi [15], LoRa [16], ZigBee [17], UAVs [18], [19], network interface cards (NICs) [20], and HackRF [21]. However, existing works primarily address device identification and authentication instead of physical location. While these approaches show reliable authentication, they lack robustness in spatial discrimination and do not capture the propagation environment, which is fundamental to location-based verification.

In contrast, in LocaRadio, we utilize CIRs in both indoor and outdoor settings for location-based authentication. We apply deep neural network architectures and fine-tuning to enhance the robustness of LocaRadio. Our methodology is essentially different from device-centric fingerprinting methods since we focus on using location-varying wireless channel features to locate nodes within authorized zones.

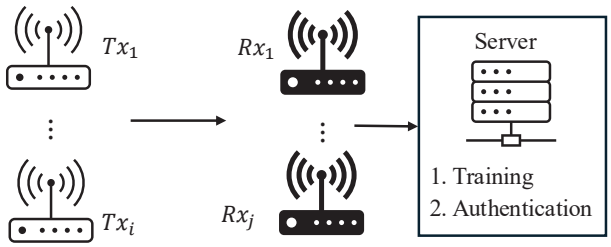


Fig. 2. System model showing transmitters Tx_i sending wireless signals to the receivers Rx_j, which extract CIRs. Labeled CIRs from authorized location zones are used for training and authentication at the server.

III. System Overview and Preliminaries

A. System Model

The proposed system consists of a set of stationary or mobile transmitters denoted by $\mathbf{T}$ and a set of stationary receivers denoted by $\mathbf{R}$, as illustrated in Fig. 2. Formally, we define the transmitter set as $\mathbf{T} = \{\mathrm{Tx}_1, \mathrm{Tx}_2, \ldots, \mathrm{Tx}_m\}$, where each element represents a wireless transmitter, and the receiver set as $\mathbf{R} = \{\mathrm{Rx}_1, \mathrm{Rx}_2, \ldots, \mathrm{Rx}_n\}$, where each element corresponds to a stationary receiver. Each transmitter $\mathrm{Tx}_i \in \mathbf{T}$ periodically broadcasts known pilot signals. Upon reception, each receiver $\mathrm{Rx}_j \in \mathbf{R}$ computes the corresponding channel impulse response (CIR) from the received baseband I/Q samples. The CIR encodes both spatial and temporal properties of the wireless propagation environment and serves as the distinguishing feature for authenticating pre-defined location zones.

The system operates in two distinct phases: a training phase and an authentication phase.

In the ***training phase***, pilot signals are transmitted from pre-defined *authorized location zones*. Each authorized zone is characterized as a distinct and bounded region within the deployment space and is labeled using coordinate-based identifiers (e.g., location01, location02, etc.). Depending on the deployment environment, these zones are represented by two-dimensional coordinates in flat indoor or outdoor scenarios, or three-dimensional coordinates for multi-level environments. The authorized zones are defined independently of the receiver's position, ensuring that the spatial labels reflect only transmitter placement. Each zone is treated as a separate class, and the CIR measurements collected within it are aggregated to form the training dataset for that class.

During the ***authentication phase***, pilot transmissions from a transmitter under test are received, and the CIR is extracted by the receivers. This CIR is then queried against the trained classifier, which predicts the most likely zone of the transmitter. The transmission is accepted if the predicted zone matches the authorized zone claimed by the transmitter, and rejected otherwise; a confidence threshold on the classifier's softmax output can additionally be applied to reject low-confidence predictions. Because the system relies only on the CIR estimated from known pilot signals, it is not tied to a specific communication protocol, which supports flexible deployment across heterogeneous wireless systems.

B. Threat Model

We assume that the training phase occurs in a secure and trusted environment, where only legitimate transmitters operate from authorized zones. Adversarial actions are considered exclusively during the authentication phase. Specifically, an adversary located outside every authorized zone aims to transmit signals that yield spoofed CIRs designed to mislead the classifier into accepting its transmission as originating from an authorized zone. We consider an adversary with knowledge of the legitimate transmitter and receiver positions and of the spatial geometry of the environment, which it can use to synthesize CIRs via ray tracing (Section V-D).

C. Preliminaries and Background

In this subsection, we discuss the basic wireless physical-layer properties we exploit to radio-fingerprint locations. We first discuss the wireless channel properties, followed by the correlation between the channels in space and time.

Large-scale vs. Small-scale Fading for Authentication. Large-scale fading refers to variations in signal strength over relatively large distances or time durations, providing stable location-specific signatures that are valuable for authentication. These variations are primarily caused by path loss and shadowing due to macroscopic terrain features. Under large-scale fading, the CIR records deterministic effects that create consistent location fingerprints, including path attenuation and blockage patterns that are difficult for adversaries to replicate.

Small-scale fading results from reflection, diffraction, and scattering effects that cause rapid signal variations. While these fluctuations can degrade authentication consistency in dynamic situations, they also provide fine-grained location-specific features that enhance security against sophisticated spoofing attempts.

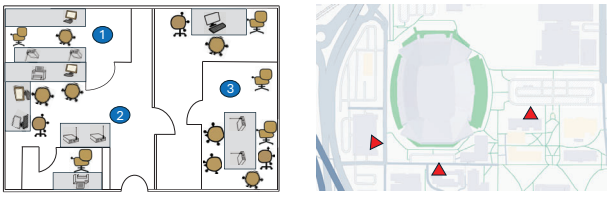
We apply low-pass filtering to the CIR (Section IV) to suppress rapidly varying noise that could compromise location verification, while preserving the stable, location-discriminative channel features needed for reliable authentication decisions.

We also investigate temporal and spatial correlation in the channel data for authentication system design. While temporal correlation shows the stability of authentication features over time, spatial correlation captures the uniqueness of channel behavior across different positions. Together, these properties inform the design of wireless channel-based authentication in dynamic environments.

D. Spatio-Temporal Channel Correlation

1) Temporal Correlation: Temporal correlation quantifies the statistical relationship between wireless channel properties at different times, directly impacting authentication system stability. It captures how channel characteristics change and whether location-specific features remain consistent over time.

Temporal correlation guides location-based authentication by determining channel predictability for verification decisions. High temporal correlation indicates stable location signatures, allowing longer authentication validity periods. Low



(a) Indoor (b) Outdoor

Fig. 3. Schematic map of the locations used for wireless data collection.

temporal correlation signifies rapid channel variation, requiring more frequent re-authentication or adaptive thresholds to maintain authentication accuracy.

2) Spatial Correlation: Spatial correlation quantifies the statistical relationship between wireless channel properties at different spatial locations, providing the foundation for location-based authentication security. It captures the uniqueness of channel behavior across different positions, enabling discrimination between authorized and unauthorized locations.

Understanding spatial variations in channel characteristics is essential for robust authentication system design. Low spatial correlation across locations ensures that each authorized zone has distinct signatures that adversaries cannot easily replicate from different positions. This property underpins the ability of location authentication techniques to distinguish legitimate from spoofed transmissions across space.

IV. Data Collection and Preprocessing

A. Wireless Transmission Setup

We established a wireless transmission setup for both indoor and outdoor environments using 12 software-defined radio (SDR) USRP devices (B200 and B205mini) operating at 2.4 GHz with a sampling rate of 6.4 MSps. Specifically, for each transmitter–receiver pair, we transmit BPSK-modulated I/Q samples. We chose BPSK for its simplicity, robustness to noise, and low bit error rate (BER) under low signal-to-noise ratio (SNR) conditions. BPSK also requires minimal processing for channel extraction while preserving authentication-relevant channel characteristics, making it computationally efficient and suitable for resource-constrained authentication systems. All USRPs are connected to a Lenovo ThinkPad T14 laptop running GNU Radio.

We collected over-the-air (OTA) BPSK samples at three indoor and three outdoor locations on a university campus, as shown in Fig. 3. At each location (either indoor or outdoor), we set up one receiver and three transmitters, each placed 3 ft from the receiver by default. We then record two minutes of BPSK transmissions between each transmitter and the receiver and save the I/Q samples. Next, we reposition the transmitters at 4, 5, and 6 ft from the receiver and record two minutes of BPSK transmissions for each distance setting. We also replace the receiver while keeping the same set of transmitters and repeat the collection for each distance setting. Compared to the indoor environment, the outdoor environment naturally exhibits higher noise and more severe multipath effects, which makes classifying I/Q samples more challenging.

B. Data Preprocessing

Given the raw I/Q samples collected from each transmission, we perform four preprocessing steps: (1) *extracting the channel impulse response (CIR)*, (2) *filtering*, (3) *data normalization*, and (4) *sliding windows to extract I/Q frames*, before passing the data to a neural network for classification. The raw I/Q samples are discarded after CIR extraction and filtering.

Extracting the Channel Impulse Response. We extract the CIR from the raw I/Q samples, as it characterizes the location-specific wireless propagation signature. We use pilot-based channel estimation [22], [23]: the channel frequency response is estimated from the known pilot symbols and then transformed into the time domain, which preserves the multipath characteristics of the wireless channel.

The channel frequency response is estimated as

$$\hat{H}_j = \frac{Y_j}{P}, \tag{1}$$

where Y_j is the received signal in the frequency domain and P is the known transmitted pilot symbol. The time-domain CIR, $\hat{h}_j[n]$, is then obtained by applying the inverse Fourier transform:

$$\hat{h}_j[n] = \mathcal{F}^{-1}\left\{\frac{Y_j}{P}\right\}. \tag{2}$$

Filtering. Filtering removes noise and hardware imperfections from the I/Q samples, which improves the accuracy of location authentication. We examined several filtering methods: Butterworth low-pass [24], elliptic [25], moving-average [26], and denoising autoencoder (DAE) [27], [28] filtering. In our preliminary experiments, Butterworth low-pass filtering yielded the highest accuracy; we therefore adopt it in LocaRadio. We use a 4th-order Butterworth low-pass filter with a normalized cutoff frequency of 0.8 relative to the Nyquist frequency (i.e., 2.56 MHz at the 6.4 MSps sampling rate), applied in a zero-phase, forward-backward manner so that no phase distortion is introduced into the CIR. Since the filter coefficients are real-valued, this is equivalent to filtering the I and Q components independently.

Normalization. We normalize the data to improve numerical stability and convergence speed during training. Normalization ensures that the inputs are uniformly scaled, so that differences in signal magnitude across settings do not impair the models' ability to learn the temporal and spatial features needed for location authentication. Before scaling, zero-valued and NaN samples are removed, which stabilizes training and improves the robustness of authentication in both indoor and outdoor environments.

Sliding Windows to Extract I/Q Frames. We segment the CIR-derived complex I/Q sequences into fixed-length traces $\mathbf{x}^{(i)} = [x_1^{(i)}, \ldots, x_L^{(i)}]$, where $x_k^{(i)} = x_k^{\mathrm{R},(i)} + j x_k^{\mathrm{I},(i)}$, using a sliding window. Each trace serves as one input instance for location authentication. A window length and stride of $L = w = 288$ yield non-overlapping segments, which improves efficiency, avoids redundant samples, and prevents overfitting to local temporal patterns. Overlapping windows

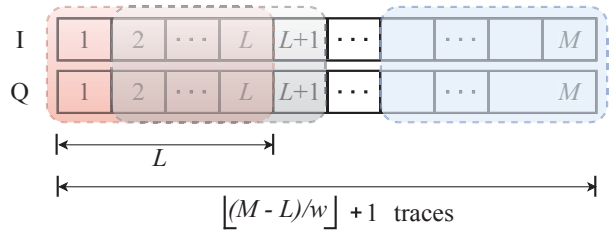


Fig. 4. Sliding-window segmentation of complex I/Q samples with trace length L and stride w, producing $\lfloor (M-L)/w \rfloor + 1$ traces from a sequence of M samples ($\lfloor M/L \rfloor$ non-overlapping traces for $w = L$).

($w < L$) inflate test accuracy through data leakage between training and test traces; in our preliminary experiments, non-overlapping segmentation yielded 3–5% higher accuracy on temporally separated test data, indicating better generalization.

From a sequence of M CIR-derived I/Q samples, the method produces $N = \lfloor (M-L)/w \rfloor + 1$ traces, which for $w = L$ reduces to $N = \lfloor M/L \rfloor$ disjoint temporal segments of channel evolution. Each trace is min–max normalized and fed into the model as a tensor of shape (batch size, $2, L$), with separate channels for I and Q. Models are trained directly in the time domain, without frequency transformation.

Input: Sequence of complex I/Q samples derived from filtered CIR: $\{x_1, x_2, \ldots, x_M\}$
Output: Preprocessed trace set $\mathcal{X} = \{\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(N)}\}$
Set trace length L and stride w
Initialize trace index $i \leftarrow 1$
for $k = 1$ **to** $M - L + 1$ **by** w **do**
  Extract trace: $\mathbf{x}^{(i)} \leftarrow [x_k, x_{k+1}, \ldots, x_{k+L-1}]$
  Normalize $\mathrm{Re}(\mathbf{x}^{(i)})$ and $\mathrm{Im}(\mathbf{x}^{(i)})$ via min–max scaling
  Store $\mathbf{x}^{(i)}$ in $\mathcal{X}$
  $i \leftarrow i + 1$
end
return $\mathcal{X}$

Algorithm 1: Sliding Window-Based I/Q Trace Extraction and Preprocessing.

C. Dataset

We store the I/Q samples after CIR extraction and filtering. The overall dataset consists of millions of I/Q samples (over 40 GB) from both indoor and outdoor environments with four distance settings (3, 4, 5, and 6 ft). Normalization and sliding windows are applied on the fly during experiments.

V. Evaluation

Experiment Setting. We conducted all authentication experiments on a Dell Precision 7920 Tower equipped with an Intel Xeon Gold 625 CPU (32 cores, 3.90 GHz), 384 GB RAM, and 4.1 TB storage, running Ubuntu 22.04. Model training and evaluation were accelerated using an NVIDIA RTX A6000 GPU (48 GB memory, TF32 tensor cores) under CUDA 12.4 with TensorFlow-Keras.

Neural Networks. We examine multiple neural networks, including ResNet-18, ResNet-50, Encoder, and Transformer.

	ResNet-18	ResNet-50	Encoder	Transformer
indoor-3ft	99.95	99.95	94.55	34.05
indoor-4ft	99.38	95.65	32.29	33.10
indoor-5ft	85.91	62.90	32.76	32.57
indoor-6ft	99.17	92.34	30.55	29.34
outdoor-3ft	96.35	78.05	99.32	98.04
outdoor-4ft	96.69	82.00	99.46	97.60
outdoor-5ft	85.01	55.02	94.43	76.76
outdoor-6ft	96.56	79.91	99.29	97.50

TABLE II
Location Classification Accuracy (%) over Three Locations (Train and Test with Same Setting)

For the activation function, we use ReLU for all the experiments, as other activations, such as Linear, do not provide promising results in our preliminary experiments. The ResNet-18 model, for instance, consists of 37,807,243 parameters. It has 4 convolution blocks, 4 identity blocks, 2 convolution layers, and 1 residual block.

Given a dataset, we always split it into 80:10:10 for training, validation, and testing. More specifically, for each distance setting, we extract 10,000 I/Q frames per location, where each I/Q frame consists of 288 I/Q samples, after we apply the sliding window method (with stride = 288). In other words, for data from each distance (from the same indoor/outdoor setting, the receiver, and the group of transmitters), 30,000 I/Q frames are involved in the evaluation, where 24,000 I/Q frames are used for training, and 3,000 I/Q frames are used for testing. We train a neural network with 100 epochs with an early stop patience of 10 epochs.

A. Experiment 1: Same Settings

We first train and test neural networks with I/Q frames from the indoor 3 ft setting. Then, we repeat the training and testing for I/Q frames from other settings, including indoor (4ft, 5ft, 6ft) and outdoor (3ft, 4ft, 5ft, 6ft). We summarize the results in Table II. All the I/Q frames we use are filtered with Butterworth filtering by default during the preprocessing step.

We can observe that, overall, ResNet-18, achieves high accuracy and the results are consistent across different settings. ResNet-50 is less effective than ResNet-18. On the other hand, Encoder and Transformer fail to achieve promising results in most of the indoor settings. Therefore, we will primarily use ResNet-18 and ResNet-50 in the remaining experiments.

B. Experiment 2: Cross Settings

We test the robustness of location classification over I/Q samples by training a neural network with one setting (e.g., indoor-3ft) but testing it with another setting (e.g., indoor-4ft). We summarize the results observed from ResNet-18 and resNet-50 in Table III.

We can observe that location classification is extremely sensitive to domain shifts over I/Q samples due to changes in distance and wireless environment, where the accuracy drops to random guess (i.e., 1/3).

C. Experiment 3: Addressing Domain Shifts with Fine-Tuning

To address the accuracy drop in the cross-settings, we apply fine-tuning, where the last 3 layers of a neural network trained

Test	Train (indoor-3ft) ResNet-18	Train (indoor-3ft) ResNet-50	Train (outdoor-3ft) ResNet-18	Train (outdoor-3ft) ResNet-50
indoor-3ft	99.95	99.95	33.33	33.44
indoor-4ft	31.62	33.33	33.09	33.09
indoor-5ft	34.35	32.01	33.34	33.34
indoor-6ft	34.21	35.21	33.41	33.34
outdoor-3ft	34.91	34.63	89.13	73.32
outdoor-4ft	30.51	33.48	31.37	47.47
outdoor-5ft	32.17	33.86	39.17	42.54
outdoor-6ft	26.75	30.79	37.82	46.26

TABLE III
LOCATION CLASSIFICATION ACCURACY (%) OVER THREE LOCATIONS (RESNET-18 AND RESNET-50, **TRAIN WITH INDOOR-3FT** AND TEST WITH CROSS SETTING)

with one setting (e.g., outdoor-3 ft) are fine-tuned with I/Q frames from a new setting (e.g., outdoor-4 ft). Each trained model is obtained from our previous experiment (trained with 24,000 I/Q frames). We fine-tune it with $N\%$ of I/Q frames from each new setting and then test it with 3,000 I/Q from the new setting. There are no overlaps between fine-tuning traces and test traces. Each model is fine-tuned with 30 epochs with an early stop of 10 epochs.

No. of Frames for Tuning	Tuning Time (sec)	Accuracy
baseline	NA	33.31
1,500	32	54.20
3,000	30	58.53
6,000	39	76.83
9,000	43	81.53
12,000	48	54.50
15,000	52	85.78

TABLE IV
LOCATION CLASSIFICATION ACCURACY (%) OVER THREE LOCATIONS (RESNET-18, TRAIN: OUTDOOR-3FT, TUNE & TEST: OUTDOOR-4FT)

We observe that fine-tuning can improve the accuracy of a neural network in the cross setting. as shown in Table IV and Table V. A greater number of fine-tuning frames leads to a higher accuracy improvement. However, a reasonable large amount of labeled frames (e.g., more than 6,000) are needed from the new setting to reach a reasonable level of accuracy with fine-tuning. We have consistent observations when perform fine-tuning over other datasets with different distance setting. The fine-tuning time is relatively minimal and can be completed typically within a minute.

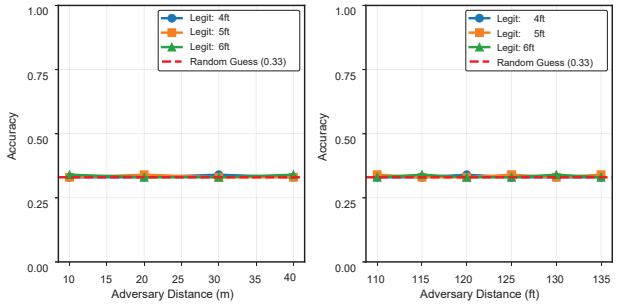
We also observe that different transmitters or receivers would also cause domain shifts, which lead to low accuracy in location authentication. Fortunately, fine-tuning can also be utilized to overcome domain shifts in this case. For instance, when we train a ResNet-18 with outdoor-3ft using I/Q frames collected from a transmitter TX-A and then test location authentication with I/Q frames collected from a transmitter TX-B (using the same set of retrievers), the baseline accuracy only achieves 33.31% (i.e., random guess). However, when we perform fine-tuning, the accuracy regains when we increase the number of fine-tuning I/Q frames.

D. Experiment 4: Analysis against Ray Tracing

In this section, we first discuss our adversary's ability to model the CIR using the ray-tracing channel reconstruction method. Ray tracing has been used both to model physical-layer attacks [29] and to characterize indoor propagation [30].

No. of Frames for Tuning	Tuning Time (sec)	Accuracy (%)
baseline	NA	33.31
1,500	33	89.58
3,000	34	83.62
6,000	39	97.05
9,000	44	97.73
12,000	55	98.81
15,000	55	99.01

TABLE V
LOCATION CLASSIFICATION ACCURACY (%) OVER THREE LOCATIONS (RESNET-18, TRAIN: OUTDOOR-3FT-TX-A; TUNE & TEST OUTDOOR-3FT-TX-B)



(a) Indoor (b) Outdoor

Fig. 5. Accuracy of ResNet-18 given CIR data generated by ray tracing

We model an adversary that uses a hybrid 3D ray-tracing framework to replicate legitimate channel characteristics in an attempt to bypass location-based authentication. Specifically, the ray tracer synthesizes CIR data by accounting for deterministic reflections, diffuse scattering, shadow fading, Ricean fading, delay spread, and multipath clusters. We simulate both LoS and NLoS conditions, including occluded scenarios in which walls obstruct the direct path and cases in which adversarial transmitters are shifted by 3 m from legitimate LoS positions. CIR data are generated across adversary distances of 10–40 m indoors and 110–135 ft (approximately 34–41 m) outdoors, yielding synthetic adversarial samples in the same format as our measured CIR dataset. This adversary models an attacker with detailed geometric knowledge of the environment who uses computationally intensive propagation modeling to mimic legitimate transmitter signatures.

To evaluate the robustness of our authentication given CIR data generated by the ray-tracing method, we pass these CIR data to trained ResNet-18s from our CIR data collected from USRPs. Our results show that these CIR data generated by ray tracing can only achieve random guess, i.e., 1/3, which indicates an adversary fails to bypass location authentication given the CIR data produced from racy tracing, as shown in Fig. 5.

VI. CONCLUSION

We present LocaRadio, a framework for authenticating the locations of wireless devices over RF signals for both indoor and outdoor environments. Our results show that specific neural network architectures can distinguish the signatures from CIR data, which can be utilized for pre-defined location authentication (i.e., proofing that a transmission originates from a device in a pre-defined zone). We also demonstrate that

domain shifts in RF signals caused by distance and hardware can be mitigated by fine-tuning.

ACKNOWLEDGMENT

The authors thank reviewers for their comments and suggestions. This work was partially supported by National Science Foundation (CNS-2225160 and CNS-2225161).

REFERENCES

[1] N. Xie, J. Zhang, and Q. Zhang, "Security provided by the physical layer in wireless communications," *IEEE Network*, vol. 37, no. 5, pp. 42–48, 2023.

[2] M. Mitev, M. Shakiba-Herfeh, A. Chorti, M. Reed, and S. Baghaee, "A physical layer, zero-round-trip-time, multifactor authentication protocol," *IEEE Access*, vol. 10, pp. 74 555–74 571, 2022.

[3] A. Shahidinejad and J. Abawajy, "Decentralized lattice-based device-to-device authentication for the edge-enabled IoT," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6623–6633, 2023.

[4] N. Sklavos, M. Manninger, X. Zhang, O. Koufopavlou, V. Hassler, P. Kitsos, M. Mcloone, P. Hamalainen, A. P. Fournaris, V. Rijmen *et al.*, *Wireless security and cryptography: specifications and implementations*. CRC Press, 2017.

[5] R. Kong and H. Chen, "DeepCRF: Deep learning-enhanced CSI-based RF fingerprinting for channel-resilient WiFi device identification," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 264–278, 2025.

[6] ——, "Towards channel-resilient CSI-based RF fingerprinting using deep learning," in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2024, pp. 1–6.

[7] ——, "CSI-RFF: Leveraging micro-signals on CSI for RF fingerprinting of commodity WiFi," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 5301–5315, 2024.

[8] L. Jin, Q. Jiang, S. Yu, H. Xu, M. Xie, X. Li, D. Ma *et al.*, "Lightweight RSS-based visible light positioning considering dust accumulation," *Journal of Lightwave Technology*, 2025.

[9] Q. Pu, W. Yu, X. Lan, M. Zhou, and X. Yang, "A novel RIS-aided indoor localization in single access point scenarios via generative AI," *IEEE Internet of Things Journal*, 2025.

[10] X. Liu, R. Wu, H. Zhang, Z. Chen, Y. Liu, and T. Qiu, "Graph temporal convolution network-based WiFi indoor localization using fine-grained CSI fingerprint," *IEEE Sensors Journal*, 2025.

[11] W. Xun, L. Sun, C. Han, Z. Lin, and J. Guo, "Depthwise separable convolution based passive indoor localization using CSI fingerprint," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2020, pp. 1–6.

[12] Y. Liu, H. Si, G. O. Boateng, X. Guo, Y. Cao, B. Qian, and N. Ansari, "Hard sample meta-learning for CIR NLOS identification in UWB positioning," *IEEE Internet of Things Journal*, 2025.

[13] D. Boshoff, M. M. Zhou, R. E. Nkrow, B. Silva, and G. P. Hancke, "UWB physical layer key sharing using the frequency domain CIR magnitude," *IEEE Transactions on Industrial Informatics*, 2025.

[14] O. Canovas, P. E. Lopez-de Teruel, and A. Ruiz, "Detecting indoor/outdoor places using WiFi signals and AdaBoost," *IEEE Sensors Journal*, vol. 17, no. 5, pp. 1443–1453, 2017.

[15] O. Ureten and N. Serinken, "Bayesian detection of Wi-Fi transmitter RF fingerprints," *Electronics Letters*, vol. 41, no. 6, pp. 373–374, 2005.

[16] M. Nair, T. Cappello, S. Dang, V. Kalokidou, and M. A. Beach, "RF fingerprinting of LoRa transmitters using machine learning with self-organizing maps for cyber intrusion detection," in *2022 IEEE/MTT-S International Microwave Symposium-IMS 2022*. IEEE, 2022, pp. 491–494.

[17] J. Yu, A. Hu, G. Li, and L. Peng, "A robust RF fingerprinting approach using multisampling convolutional neural network," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6786–6799, 2019.

[18] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 60–76, 2020.

[19] N. Ondus, "RF fingerprinting unmanned aerial vehicles," M.S. Thesis, Embry-Riddle Aeronautical University, Daytona Beach, FL, Dec. 2021.

[20] C. Corbett, R. Beyah, and J. Copeland, "A passive approach to wireless NIC identification," in *2006 IEEE International Conference on Communications*, vol. 5. IEEE, 2006, pp. 2329–2334.

[21] H. Fu, X. Zhang, and L. Peng, "Comparison of receiver front-end differences for RF fingerprint based IoT device identification," in *2023 8th International Conference on Signal and Image Processing (ICSIP)*. IEEE, 2023, pp. 979–984.

[22] Z. Zhou, K. Wan, Y. Zhang, X. Shao, J. Guo, and Y. Gong, "A survey of artificial intelligence enabled channel estimation methods: Recent advance, performance, and outlook," *Artificial Intelligence Review*, vol. 58, no. 6, p. 177, April 2025. [Online]. Available: https://link.springer.com/article/10.1007/s10462-025-11202-0

[23] S.-H. Lee and Y.-H. Kim, "Noise-canceling channel estimation schemes based on the CIR length estimation for IEEE 802.11p/OFDM systems," *Electronics*, vol. 13, no. 6, p. 1110, March 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/6/1110

[24] S. Butterworth, "On the theory of filter amplifiers," *Wireless Engineer*, vol. 7, no. 6, pp. 536–541, 1930.

[25] A. V. Oppenheim, R. W. Schafer, and J. R. Buck, *Discrete-time signal processing*. Prentice Hall, 1999.

[26] S. W. Smith, *The Scientist and Engineer's Guide to Digital Signal Processing*. California Technical Publishing, 1997.

[27] P. Vincent, H. Larochelle, Y. Bengio, and P.-A. Manzagol, "Extracting and composing robust features with denoising autoencoders," in *Proceedings of the 25th international conference on Machine learning*, 2008, pp. 1096–1103.

[28] H. Zhang, X. Wu, and Y. Liu, "Channel estimation using denoising autoencoder in OFDM systems," *IEEE Access*, vol. 7, pp. 110 160–110 169, 2019.

[29] P. Walther, M. Richter, and T. Strufe, "Ray-tracing based inference attacks on physical layer security," *Electronic Communications of the EASST*, vol. 80, 2021.

[30] E. Kilcioglu and C. Oestges, "Ray-tracing based RIS deployment optimization for indoor coverage enhancement," *IEEE Open Journal of Antennas and Propagation*, 2025.