Detecting Spoofed Remote ID Messages Using Radio-Frequency Fingerprints: A Python-Based Simulation Study

Harkiran Kaur Bhullar, Ashley Moinard, Laxima Niure Kandel
Department of Electrical Engineering and Computer Science
Embry-Riddle Aeronautical University
Daytona Beach, FL, USA
bhullarh@my.erau.edu, moinarda@my.erau.edu, niurekal@erau.edu

Abstract—**Remote ID (RID) is now required for most drones so that they can be identified while flying. But because RID messages are broadcast in the open without encryption, an attacker can spoof these signals to hide a real drone or impersonate a legitimate one. In this work, we study whether radio-frequency fingerprints (RFF), hardware-induced signal imperfections unique to each device, can detect such spoofing attacks. We built a Python-based simulator that creates virtual drones, generates ASTM-style RID messages, applies realistic hardware imperfections based on device type (consumer drone, cheap clone, or SDR), and models wireless channel effects to produce raw I/Q data. Each device type produces distinct RFF characteristics that persist even after channel degradation. We generated approximately 3,000 labeled samples across three classes and trained multiple classifiers on the raw I/Q data. Our results show that a 1D Convolutional Neural Network achieves 93.97% accuracy in distinguishing legitimate RID signals from spoofed ones, with Random Forest and Logistic Regression achieving 89.29% and 82.14% respectively. These results demonstrate that while attackers can copy RID message content, they cannot replicate the hardware fingerprint of the legitimate transmitter, enabling RF-based spoofing detection.**

Index Terms—**Remote Identification, RF Fingerprinting, UAV Security, Spoofing Detection, Machine Learning, I/Q Signal Processing**

I. Introduction

Remote Identification (RID) has become an important requirement for most small unmanned aerial systems (sUAS). RID allows a drone to broadcast information such as its identity, position, and velocity to anyone nearby. This helps improve safety, supports rule enforcement, and prepares the airspace for future low-altitude traffic management. Right now, RID messages are sent out in plain text over the air with no encryption or protection—just open signals. If someone has even a cheap radio receiver, they can pick up everything a drone is broadcasting. That creates an opportunity for abuse. For example, someone could grab a real RID message, save it, and send it again later. They could also tweak parts of the message to pretend the drone has a different ID or is flying in another spot. With tricks like that, it is possible to make a drone appear where it is not or hide one that actually is there. As drones become more common, problems like this stop being theoretical and start becoming actual risks for keeping the airspace safe and organized.

Many researchers have studied how to strengthen drone communication and detect malicious activity. Wisse et al. introduced A2RID [1], an authentication system that allows drones to verify their identity anonymously while still preventing message tampering. While cryptographic protections for RID have been proposed [7], these approaches usually require new hardware or major updates to existing standards.

Another line of research focuses on radio-frequency (RF) features and machine learning. Xu et al. [2] demonstrated adaptive RF fingerprint decomposition for micro-UAV detection using machine learning techniques. Allahham et al. [3] proposed a multi-channel 1D convolutional neural network approach for RF-based drone detection and identification, showing that deep learning can effectively extract discriminative features from raw RF signals. Ezuma et al. [4] showed that RF fingerprints from drone remote controllers can distinguish between different UAV models, even in the presence of WiFi and Bluetooth interference.

Additional work studies spoofing and navigation-layer threats. Pardhasaradhi and Cenkeramaddi [5] examined GPS spoofing against drones and used distributed radar tracking to detect false position information. Network-level intrusion detection has also been widely explored, with many systems attempting to identify unusual communication patterns or unknown devices using machine-learning models [6], though these methods generally target networked drones rather than broadcast-based RID. A broader survey by Belwafi et al. [7] provides an in-depth overview of modern RID systems and the remaining challenges in identifying drones securely.

Overall, prior work shows that while many tools exist for drone detection and authentication, there is still limited research focused specifically on detecting RID spoofing in the RF domain. In particular, there is little analysis of how spoofed RID appears in raw I/Q data, or how machine-learning classifiers can distinguish real RID transmissions from spoofed ones based on radio-frequency fingerprints.

In this paper, we present a proof-of-concept framework to explore this problem. We built a Python-based simulator that creates virtual UAVs, generates ASTM-style RID messages, applies realistic hardware imperfections based on device class, and models wireless-channel effects including path loss, fading, and noise. Each device type, DJI-style consumer UAVs, cheap Generic clones, and HackRF-style SDR attackers, has its own hardware profile with characteristic oscillator stability, I/Q imbalance, DC offset, and power amplifier behavior. These hardware differences produce distinct RF fingerprints in the transmitted I/Q signal. Attackers copy the RID message content (including the victim's ID) but transmit using their own hardware, producing a detectably different signal. We label each received signal by its true source class and train machine-learning classifiers to distinguish legitimate transmissions from spoofed ones based solely on the raw I/Q data.

II. Methodology and Procedures

The goal of our method is to answer a straightforward question: can radio-frequency fingerprints be used to detect spoofed RID messages? To keep the project focused, we aim for a proof-of-concept using simulated data instead of real UAVs. Our approach has two main parts: a data-generation pipeline that produces labeled I/Q signals from virtual UAVs, and a machine-learning stage that classifies signals as legitimate or spoofed.

A. Data Generation Pipeline

Our pipeline models the signal chain from UAV transmission to ground reception. The process follows a systematic approach: for each scenario, we create UAVs with random positions and velocities, where Citizens use DJI hardware, flying attackers use Generic hardware, and ground attackers use HackRF hardware. Attackers are assigned a spoofed ID matching a random Citizen's ID. For each UAV, we generate a 25-byte RID message following the ASTM F3411-19 format, generate an RF fingerprint based on the hardware profile, modulate using BPSK at 1 Mbps with 20 MHz sampling, apply RFF impairments to the I/Q signal, apply channel effects including path loss, fading, and AWGN, then normalize and store the signal with its label.

1) Device Hardware Profiles: Each UAV is assigned a hardware profile based on its device type. DJI UAVs represent high-quality consumer hardware and serve as legitimate "Citizen" UAVs. Generic UAVs represent cheap clones that act as flying attackers. HackRF-style transmitters represent ground-based SDR attackers. Table I shows the parameter ranges for each device type. These ranges reflect typical hardware quality differences: consumer UAVs use temperature-compensated crystal oscillators (TCXO) with tight tolerances of ±0.5–2 ppm [8], while cheap clones use standard crystal oscillators with much larger frequency variations of 30–50 ppm. The I/Q imbalance and DC offset ranges are based on typical values observed in direct-conversion receivers [9], [10].

2) RID Message Generation: We generate 25-byte messages following the ASTM F3411-19 format. Byte 0 contains the message type header (0x10). Bytes 1–8 contain the UAS ID as an 8-character ASCII string. Bytes 9–16 encode latitude and longitude as degrees multiplied by 10^7 in signed 32-bit format. Bytes 17–18 encode altitude as meters multiplied by 2 in unsigned 16-bit format. Bytes 19–20 encode speed as m/s multiplied by 4 in unsigned 16-bit format. Bytes 21–22 contain heading in degrees as unsigned 16-bit, and bytes 23–24 contain a timestamp with 0.1s precision. Attackers transmit messages with a Citizen's ID but using their own hardware, producing a different RF fingerprint.

TABLE I
Hardware Profile Parameters by Device Type

Parameter	**DJI**	**HackRF**	**Generic**
Oscillator Type	TCXO	TCXO	Crystal
Freq. Stability (ppm)	2–10	0.5–2	30–50
Phase Noise Std (rad)	0.01–0.03	0.02–0.04	0.03–0.06
I/Q Imbalance (dB)	0.5–2.0	1.0–3.0	2.0–4.0
DC Offset (norm.)	0.005–0.015	0.01–0.03	0.02–0.04
PA Compression (dBm)	-35 to -30	-25 to -20	-28 to -22

3) RF Fingerprint Generation: Based on prior literature [2], [11], [12], we model six RFF features that arise from hardware imperfections:

Carrier Frequency Offset (CFO): Crystal oscillator tolerance causes frequency drift. For TCXO devices, temperature drift is ±2.5 ppm/°C; for standard crystals, it is ±50 ppm/°C. The CFO in Hz is computed as:

$$\text{CFO}_{\text{Hz}} = \text{CFO}_{\text{ppm}} \times 10^{-6} \times f_c \tag{1}$$

where $f_c = 2.437$ GHz is the carrier frequency.

Phase Noise: Oscillator jitter introduces random phase variations, modeled as cumulative Gaussian noise with standard deviation based on the hardware profile.

I/Q Gain Imbalance: Imperfect mixer calibration causes different gains on I and Q channels, typically 0.5–4 dB depending on hardware quality [10].

I/Q Phase Imbalance: Quadrature error from mixer imperfections, modeled as 1–5 degrees of phase offset.

DC Offset: Local oscillator leakage adds DC bias to both I and Q channels, a well-known impairment in direct-conversion receivers [9].

Power Amplifier Compression: High-power samples experience nonlinear compression when exceeding the PA's linear operating range.

4) Signal Transmission: The RID message is modulated using Binary Phase Shift Keying (BPSK) at a symbol rate of 1 Mbps and sampled at 20 MHz, yielding 20 samples per symbol. The 25-byte message produces 200 bits, resulting in 4,000 samples of useful signal. After BPSK modulation, the RFF impairments are applied sequentially: CFO shifts the carrier frequency, phase noise adds cumulative random phase, I/Q imbalance distorts the quadrature components with gain and phase errors, DC offset adds bias to both channels, and PA compression reduces amplitude of high-power samples.

5) Channel Model: The transmitted signal passes through a wireless channel with three effects. Free-space path loss provides attenuation based on 3D distance at 2.437 GHz (WiFi channel 6):

$$\text{FSPL(dB)} = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) \quad (2)$$

where d is distance in meters, f is frequency in Hz, and c is the speed of light.

Rician fading models multipath effects with K-factor of 10, representing a strong line-of-sight component:

$$h = \sqrt{\frac{K}{K+1}} + \sqrt{\frac{1}{K+1}} \cdot \frac{\mathcal{CN}(0,1)}{\sqrt{2}} \quad (3)$$

Finally, additive white Gaussian noise (AWGN) is applied based on SNR, which is randomized between 10–30 dB per scenario.

6) Dataset Generation: We generated 1,000 randomized scenarios. Each scenario includes random geographic locations (latitude 30–45°, longitude -120 to $-70°$), 1–2 Citizen UAVs, 0–2 flying attackers, 0–1 ground attackers, random UAV positions (altitude 80–150 m) and velocities (5–15 m/s), a receiver at ground level (2 m altitude) at the environment center, and random SNR between 10–30 dB.

For each UAV transmission, we extract the first 4,000 I/Q samples corresponding to the 25-byte RID message, normalize by RMS power, and flatten to a vector of 8,000 values (alternating I and Q). The final dataset contains approximately 3,000 samples across three classes: Citizen (label 0), UAV_Attack (label 1), and Ground_Attack (label 2).

B. Machine Learning Classification

1) Preprocessing: The dataset is split 70/15/15 into training, validation, and test sets using stratified sampling to maintain class proportions. Features are standardized using z-score normalization fitted on training data. For the 1D-CNN, data is reshaped to (samples, 4000, 2) to preserve I/Q pair structure.

2) Models: We train three classifiers with different characteristics:

1D Convolutional Neural Network: Three convolutional blocks with increasing filters (32→64→128), kernel sizes (7→5→3), batch normalization, and max pooling. Global average pooling feeds a dense layer (64 units, L2 regularization λ=0.001) with 40% dropout, followed by softmax output. Training uses Adam optimizer (initial learning rate 0.001), sparse categorical cross-entropy loss, class weights for imbalance, early stopping (patience=10), and learning rate reduction on plateau.

Random Forest: 100 decision trees with balanced class weights to handle class imbalance.

Logistic Regression: L2 regularization with balanced class weights, maximum 1000 iterations.

For Random Forest and Logistic Regression, the I/Q data is flattened to 8,000 features per sample.

III. Tests and Results

A. Visual Analysis

Before training classifiers, we examined both averaged and individual I/Q signals to understand the RFF characteristics of each device class. Fig. 1 shows the average received signal amplitude across all samples per class. Despite all devices transmitting identical RID message content, the averaged waveforms exhibit distinct characteristics. The Ground_Attack signals (light purple) show a notably different decay pattern with a gradual amplitude decline over the first 1,000 samples. This characteristic shape arises from the higher DC offset of SDR hardware; when the signal is normalized by RMS power, the elevated DC component creates this distinctive slow decay that differentiates it from the sharper transient response of the drone hardware. The Citizen and UAV_Attack signals both show a sharp initial peak followed by rapid decay, but the UAV_Attack signal (dark red) exhibits greater amplitude variation and more pronounced oscillations throughout the signal, consistent with the poorer I/Q balance and higher phase noise of cheap Generic hardware. The Citizen signal (green) maintains the most stable amplitude profile after the initial transient.

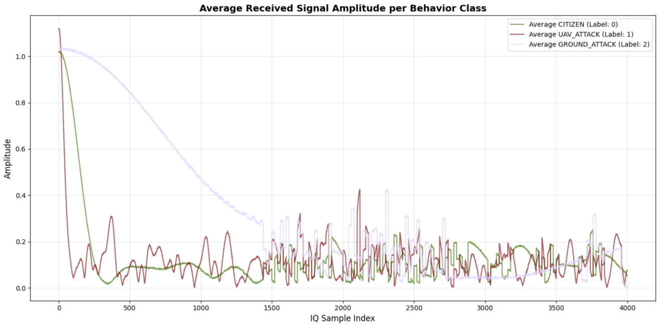

Fig. 1. Average received signal amplitude per behavior class. Ground_Attack (SDR) shows a distinct slow decay pattern, while Citizen (DJI) and UAV_Attack (Generic) differ in amplitude stability and oscillation patterns.

Fig. 2 shows individual received signals after channel effects, with distances noted in the legend. The BPSK modulation pattern is clearly visible as periodic amplitude variations. Importantly, signal amplitude scales with distance due to path loss—the DJI-CITIZEN-003 at 1294m shows lower amplitude than DJI-CITIZEN-001 at 713m. However, the waveform shape characteristics that encode the RFF remain distinguishable regardless of distance. The Generic hardware (GENERIC-PHANTOM, red traces) produces visibly noisier waveforms with less consistent peak amplitudes compared to the cleaner DJI signals. The HackRF ground attacker (light blue) shows the smoothest waveform but with a distinct DC offset visible as an elevated baseline.

These visual differences confirm that hardware fingerprints persist through the channel model and can potentially distinguish device types, even when the same RID message content is transmitted.

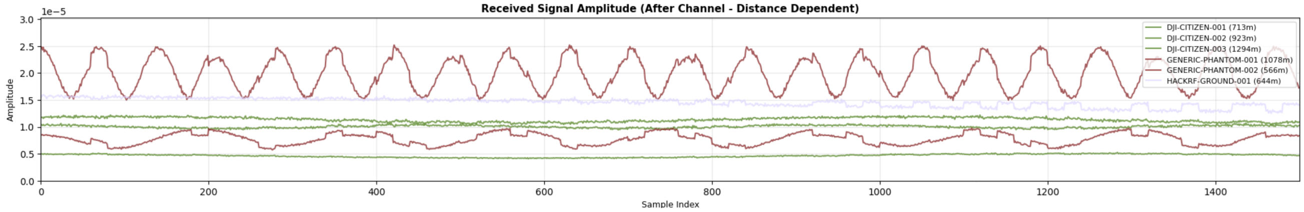

Fig. 2. Individual received signal amplitudes after channel effects. Distance-dependent path loss affects amplitude, but RFF-induced waveform characteristics remain distinguishable across device types.

B. *Classification Results*

Table II summarizes classifier performance on the held-out test set of 448 samples.

TABLE II
CLASSIFICATION RESULTS

Model	**Accuracy**	**Weighted F1**
1D-CNN	93.97%	0.9415
Random Forest	89.29%	0.8923
Logistic Regression	82.14%	0.8274

Table III shows the per-class performance for the best-performing 1D-CNN model.

TABLE III
PER-CLASS PERFORMANCE (1D-CNN)

Class	**Precision**	**Recall**	**F1**	**Support**
Citizen	0.9903	0.9031	0.9447	227
UAV_Attack	0.9790	0.9655	0.9722	145
Ground_Attack	0.7755	1.0000	0.8736	76

The 1D-CNN achieved the highest accuracy (93.97%) by learning spatial patterns in the I/Q sequences. Random Forest performed competitively (89.29%), demonstrating that even simpler models can leverage RFF differences. Logistic Regression's lower performance (82.14%) suggests the class boundaries are not linearly separable in the raw feature space.

The per-class results reveal that the 1D-CNN achieves near-perfect precision on Citizen signals (99.03%) and high recall on UAV_Attack (96.55%). Ground_Attack detection shows perfect recall (100%) but lower precision (77.55%), indicating some Citizen signals are misclassified as ground attacks. This is likely due to two factors: the smaller sample size for this class, and the fact that HackRF SDR hardware uses TCXO oscillators similar to DJI consumer UAVs, resulting in more similar RFF characteristics between these two classes compared to the Generic hardware used by flying attackers. This inter-class similarity presents an interesting challenge for future work, where finer-grained device-specific fingerprinting could improve discrimination—though such approaches would require enrolling known devices, which may not be practical for large-scale deployment.

C. *Key Observations*

Our results support several important findings. First, RFF differences persist through the channel: despite path loss, fading, and noise, the hardware-induced signal characteristics remain distinguishable across classes. Second, attackers cannot forge RFF: even when attackers copy the exact RID message content (same ID, position, speed), their different hardware produces detectably different I/Q patterns. Third, class imbalance affects Ground_Attack performance: the smaller number of ground attacker samples (76 vs. 227 Citizen) contributes to lower precision for this class. Fourth, deep learning outperforms traditional ML: the 1D-CNN's ability to learn hierarchical features from raw I/Q data provides a 4.7 percentage point accuracy improvement over Random Forest.

IV. CONCLUSION AND FUTURE WORKS

In this work, we showed a simple but effective way to detect spoofed RID messages using only radio-frequency fingerprints. The main novel part of our approach is that we do not rely on GPS data, message fields, or cryptography. Instead, we use the small hardware imperfections inside each device, which still appear in the raw I/Q signal even after the attacker copies the digital RID message. This makes our method useful in cases where traditional message-based checks may fail.

Our simulator allowed us to generate large amounts of realistic I/Q data from different types of devices, including a DJI-like Citizen drone, a cheap clone drone, and a HackRF-style SDR attacker. One of the key results we demonstrated is that these different devices create clearly different average I/Q waveforms. Even after adding path loss, fading, and noise, the hardware differences remained visible. This shows that spoofers can imitate the message but not the hardware, which supports the idea that RF fingerprints can help detect false RID signals.

Table IV summarizes the main differences we observed between the three device classes, derived from the averaged I/Q signals showing that the simulator produces useful variation for machine learning.

While these results are promising, this project is still a proof of concept. In future work, we plan to gather real I/Q data from actual UAVs and SDR devices to validate how closely our simulated data matches real-world conditions. We also want to add more realism to the simulator, including fingerprint drift that changes with distance, more types of drone hardware, and a richer channel model with multipath

TABLE IV
SIGNAL FEATURE COMPARISON BETWEEN DEVICE TYPES

Class	Osc. Stability	DC Offset	IQ Imbal.	Waveform Noise
Citizen (DJI)	High	Low	Low	Low
UAV_Attack (Generic)	Low	Medium	High	High
Ground_Attack (HackRF)	High	High	Medium	Low

and Doppler effects. Additionally, investigating the robustness of our approach against adversarial attacks where attackers attempt to mimic legitimate hardware characteristics would strengthen the practical applicability of this method.

Another promising direction is combining RF fingerprinting with cryptographic authentication methods. While cryptographic approaches like A2RID [1] provide strong message-level authentication, they require protocol modifications and key management infrastructure. RF fingerprinting operates at the physical layer and requires no changes to the RID message format, making it complementary to cryptographic solutions. A hybrid approach could use cryptographic signatures for primary authentication while employing RF fingerprinting as a secondary verification layer to detect sophisticated attacks where an adversary might have compromised cryptographic keys but cannot replicate the legitimate transmitter's hardware characteristics. Such defense-in-depth strategies would significantly raise the bar for successful RID spoofing attacks.

Overall, these results suggest that RF fingerprints could be a solid way to spot spoofed RID signals. Even though we used a fairly simple Python simulation, the hardware differences still showed clearly in the I/Q data, and attackers cannot easily fake those imperfections. With more testing and real-world experiments, this approach could end up being a helpful extra layer of security for the RID system.

REFERENCES

[1] E. Wisse, P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "A2RID Anonymous Direct Authentication and Remote Identification of Commercial Drones," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10587–10604, Jun. 2023.

[2] C. Xu, F. He, B. Chen, Y. Jiang, and H. Song, "Adaptive RF Fingerprint Decomposition in Micro UAV Detection based on Machine Learning," in *Proc. IEEE ICASSP*, pp. 7968–7972, Jun. 2021.

[3] M. S. Allahham, T. Khattab, and A. Mohamed, "Deep Learning for RF-Based Drone Detection and Identification: A Multi-Channel 1-D Convolutional Neural Networks Approach," in *Proc. IEEE Int. Conf. Informatics, IoT, Enabling Technol.*, 2020.

[4] 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 J. Commun. Soc.*, vol. 1, pp. 60–79, Nov. 2019.

[5] B. Pardhasaradhi and L. R. Cenkeramaddi, "GPS Spoofing Detection and Mitigation for Drones Using Distributed Radar Tracking and Fusion," *IEEE Sensors Journal*, vol. 22, no. 11, pp. 11122–11134, Jun. 2022.

[6] M. Ogab, S. Zaidi, A. Bourouis, and C. T. Calafate, "Machine Learning-Based Intrusion Detection Systems for the Internet of Drones: A Systematic Literature Review," *IEEE Access*, vol. 13, pp. 96681–96714, 2025.

[7] K. Belwafi, R. Alkadi, S. A. Alameri, H. A. Hamadi, and A. Shoufan, "Unmanned Aerial Vehicles' Remote Identification: A Tutorial and Survey," *IEEE Access*, vol. 10, pp. 87577–87601, 2022.

[8] J. R. Vig, "Introduction to Quartz Frequency Standards," *IEEE Int. Frequency Control Symp. Tutorial*, 1999.

[9] M. Windisch and G. Fettweis, "On the Estimation and Compensation of IQ Impairments in Direct Conversion Transmitters," in *Proc. IEEE APCCAS*, pp. 1078–1081, 2008.

[10] J. Tubbax, B. Come, L. Van der Perre, S. Donnay, M. Engels, H. De Man, and M. Moonen, "Compensation of IQ Imbalance and Phase Noise in OFDM Systems," *IEEE Trans. Wireless Commun.*, vol. 4, no. 3, pp. 872–877, May 2005.

[11] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau, "Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach," in *Proc. IEEE VTC*, pp. 1–5, 2008.

[12] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in *Proc. ACM MobiCom*, pp. 116–127, 2008.