Robust Device Authentication in Multi-Node Networks: ML-Assisted Hybrid PLA Exploiting Hardware Impairments

Ildi Alla, Selma Yahia, Valeria Loscri, Hossien Eldeeb

Robust Device Authentication in Multi-Node Networks: ML-Assisted Hybrid PLA Exploiting Hardware Impairments

Ildi Alla*, Selma Yahia*, Valeria Loscri*, Hossien Eldeeb†
*Inria Lille-Nord Europe, Lille, France
{ildi.alla, selma.yahia, valeria.loscri}@inria.fr
†6G Research Center, Khalifa University, Abu Dhabi, UAE
hossieneldeeb@ieee.org

***Abstract*—This paper introduces a novel hybrid physical layer authentication (PLA) method designed to enhance security in multi-node networks by leveraging inherent hardware impairments. The approach specifically exploits carrier frequency offset (CFO), direct current offset (DCO), and phase offset (PO) as multi-attribute features, improving the verification process for authorized users and enhancing the detection of unauthorized devices. Machine learning (ML) models are developed to authenticate devices without prior knowledge of malicious characteristics, resulting in robust and reliable device authentication capabilities. Experimental evaluations conducted on a commercial software-defined radio (SDR) platform demonstrate the effectiveness of the proposed approach under varying signal-to-noise ratio (SNR) conditions. The hybrid PLA scheme integrates advanced feature extraction methods with finely-tuned ML models, optimized through controlled experiments to ensure high performance across diverse network conditions and attack scenarios. Real experimental tests validate the efficacy of the proposed scheme, achieving high authentication rates exceeding 96% and reliable detection rates for malicious device attacks surpassing 95%. Additionally, the approach is highly efficient, with a mean inference time of less than 3.75 milliseconds (ms) and power consumption below 25.5 millijoules (mJ), confirming its suitability for real-time applications in energy-constrained environments.**

***Index Terms*—device authentication, hardware impairments, machine learning, multi-node networks.**

1. Introduction

Wireless communication networks are highly vulnerable to interception and spoofing attacks due to the inherent properties of radio signal propagation, intermittent communication, and standardized transmission schemes [1]–[3]. To secure these communications, authentication schemes play a crucial role by verifying the identities of connected devices [4]. Traditionally, Upper Layer Authentication (ULA) methods, which rely on cryptographic protocols [5], [6], have been pivotal in securing wireless networks due to their robustness. However, these techniques face significant challenges, particularly in heterogeneous and resource-constrained environments such as IoT networks.

One of the primary challenges with cryptographic-based authentication is the potential for compromised security during the key generation, distribution, and management processes [7]. Although cryptography is a strong defense against unauthorized access, adversaries may still intercept keys during distribution, potentially undermining their confidentiality [8]. Furthermore, the security of cryptographic methods often hinges on the assumption that computational tools have limited capabilities—a notion increasingly challenged by the rapid advancement in computational power and cryptanalysis techniques. Additionally, the dynamic nature of device participation in decentralized networks complicates the management and distribution of cryptographic keys, further complicating the authentication process [9].

Given these challenges, it is clear that while cryptographic methods remain essential, additional security measures are necessary, particularly in resource-constrained environments. Physical Layer Authentication (PLA) emerges as a promising solution that enhances security by leveraging the unique characteristics of the wireless communication's physical layer, such as radio-frequency (RF) signals, device-specific features, and channel state information, which are inherently difficult to replicate [10], [11]. By integrating these attributes into the authentication process, PLA provides a robust defense against prevalent security threats, including spoofing and replay attacks [12].

Unlike ULA, PLA does not solely depend on cryptographic keys, thereby reducing vulnerabilities associated with key distribution and management. This added layer of security is especially advantageous in dynamic, decentralized, and multi-node network environments, where traditional authentication methods might falter due to the fluid nature of device participation. Integrating PLA enhances protection, especially in situations where cryptographic methods alone may not suffice.

However, developing a PLA scheme that can effectively address the challenges of multi-node networks is a complex task. The presence of multiple nodes transmitting signals to an authenticating entity introduces intricacies in the verification process. Malicious nodes further complicate matters, necessitating the adoption of enhanced security measures. The significance of PLA lies in its ability to leverage the channel characteristics, such as received signal strength

(RSS), channel impulse response (CIR), and channel frequency response (CFR), as well as hardware impairments like carrier frequency offset (CFO), direct current offset (DCO), and phase offset (PO), to enhance device authentication and security.

Several studies have utilized channel-based features for PLA purposes. For instance, the works in [13]–[15] focused on utilizing CIR to design PLA mechanisms to effectively differentiate between authorized and unauthorized devices under specific channel conditions. Similarly, the authors in [16], [17] have exploited the unique properties of the CFR to develop PLA schemes. On the other hand, some studies [18]–[20] have explored the use of RSS for node authentication. However, it is important to note that channel-based PLA strategies may encounter challenges in mobile and dynamic conditions. In such scenarios, the channel characteristics can rapidly change, affecting the reliability and effectiveness of the authentication process.

Unlike channel-based PLA strategies, hardware impairments-based features offer more reliable authentication solutions, particularly in dynamic scenarios. By engineering device-specific features such as CFO, DCO, and PO, authentication schemes can leverage consistent and unique hardware-induced signatures that are inherently tied to each device. These features, arising from manufacturing variations, are difficult for adversaries to replicate or manipulate and remain stable despite external factors like multipath fading or noise. This ensures robust security, supports low-complexity implementation, and maintains strong resistance against spoofing attacks.

The literature has already shown attention towards exploiting hardware impairments-based features for designing authentication frameworks. Many existing PLA schemes focus on a single attribute, such as CFO, to authenticate devices. For instance, [21]–[24] discusses a PLA framework where authentication is based on the analysis of CFO. Specifically, [21] examines authentication for mobile systems by analyzing time-varying CFOs. In [22], a method for orthogonal frequency-division multiplexing (OFDM) systems is presented that uses hypothesis testing of CFO estimates to differentiate between legitimate and illegitimate devices. The work in [23] delves into fingerprinting Wi-Fi devices, utilizing software-defined radios to leverage CFO as a key differentiator. Finally, [24] investigates a novel approach to authentication by combining CFO analysis with visibility graphs, aiming to improve the reliability and robustness of authentication mechanisms. While these schemes benefit from simplicity and reduced computational requirements, they often fail to provide robust security in diverse and dynamic environments due to the overlapping characteristics of this attribute among different devices [25].

Recognizing the limitations of single-attribute-based PLA, some researchers have proposed the use of multiple attributes to enhance security. For example, [26]–[28] propose a hybrid approach that combines CFO with other features for authentication. However, such approaches often rely on predefined thresholds to make authentication decisions, which introduces challenges in terms of precise calibration and

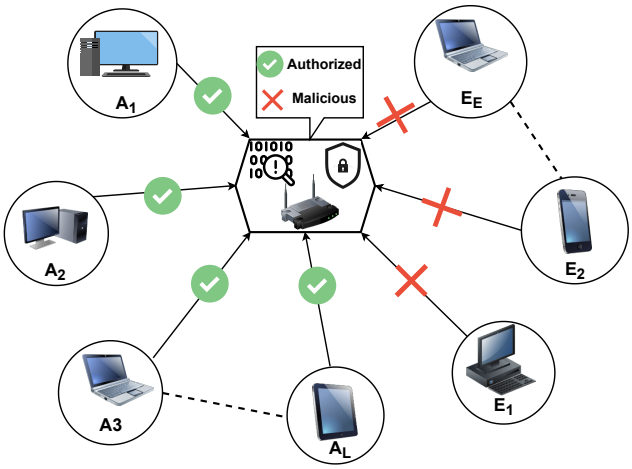


Figure 1: Multi-Node System Model.

optimization for different deployment scenarios. Notably, the research in [29] employs a hybrid approach based on CFO that does not require predefined thresholds, offering a more flexible solution. Nevertheless, these approaches lack experimental validation, which is critical for proving their efficacy in real-world conditions.

To address this research gap, this paper presents a robust device PLA scheme that leverages the power of machine learning (ML) models and hybridization of hardware impairments. The proposed scheme aims to authenticate devices effectively, even without prior knowledge of malicious characteristics. It utilizes ML models trained with advanced feature extraction techniques, enabling them to differentiate between authorized and malicious entities. The development of these ML models emphasizes fine-tuning through a series of controlled experiments, optimizing their performance under diverse network conditions and various attack scenarios. To evaluate the effectiveness of the proposed hybrid PLA approach, experimental validations are conducted on a commercial software-defined radio (SDR) platform. By subjecting the system to varying signal-to-noise ratio (SNR) conditions, the performance of the proposed approach is assessed. The experimental results demonstrate high authentication rates for the legitimate nodes and reliable detection rates for malicious device attacks. These findings validate the efficacy of the hybrid PLA scheme in bolstering device authentication and enhancing overall network security. The paper's significant contributions can be summed up as follows:

- Introduction of a novel hybrid PLA scheme, leveraging CFO, DCO, and PO to enhance authentication in multi-node networks.
- Implementation of advanced feature extraction methods to differentiate authorized devices requiring authentication from other devices, including malicious ones.
- Development of device authentication approaches based on ML models, capable of recognizing and

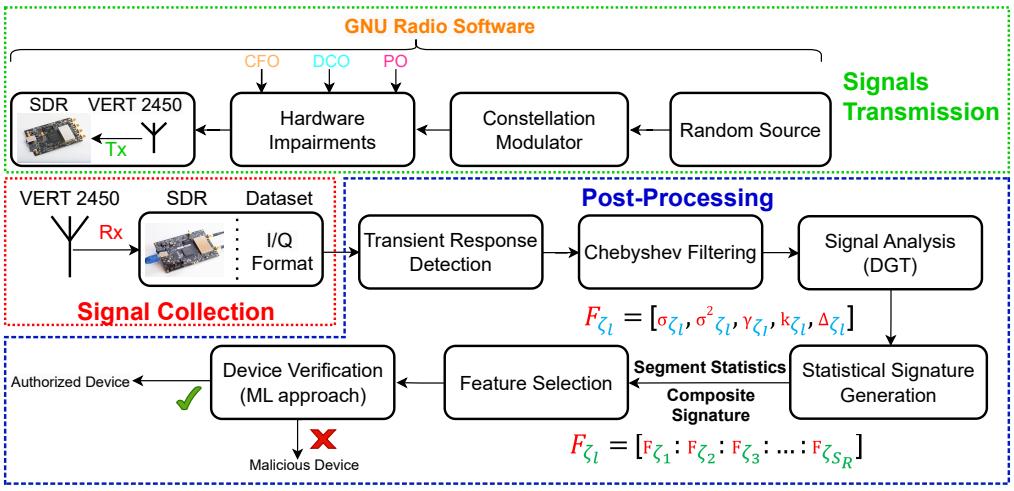


Figure 2: PHY authentication framework.

authenticating devices without prior knowledge of potential malicious nodes' signals or characteristics. These ML-based methods operate effectively without predetermined thresholds, striking a balance between authentication accuracy and attack detection sensitivity.

- Fine-tuning of the ML models through controlled experiments to optimize performance across different network conditions and attack scenarios.
- Validation of the proposed approach through experimental testing, demonstrating a true authorized detection rate exceeding 95%, a false authorized detection rate below 5%, and a true malicious detection rate exceeding 95%. Furthermore, the scheme achieves a mean inference time of less than 3.75 milliseconds (ms) and power consumption below 25.5 millijoules (mJ), confirming its suitability for real-time and energy-constrained applications.

The rest of this paper is organized as follows. Section 2 presents the considered multi-node network model, highlighting the scenario of multiple nodes transmit signals to an authenticating entity. The detailed description of the proposed PLA scheme and the deployed physical features are provided in Section 3. Section 4 presents the ML approaches adopted to identify the specific features in the RF signals. Section 5 is devoted to the evaluation and validation of our approaches through experimental analysis. Finally, the paper is concluded in Section 6.

2. Multi-Node Network Model

In this multi-node network model, depicted in Figure 1, the network consists of N devices, with a subset of L devices identified as legitimate nodes, referred to as A_i ("Alice"), where $i \in \{1, 2, \ldots, L\}$. These legitimate nodes are reliable entities that engage in normal communication, participating in data transmission and reception to fulfill the network's intended functions. The remaining devices, $E = (N - L)$, are categorized as malicious nodes, represented as E_j ("Eve"), where $j \in \{1, 2, \ldots, E\}$. These malicious nodes act as adversaries within the network, attempting to undermine it through activities such as unauthorized access, eavesdropping, data manipulation, or disrupting communication processes.

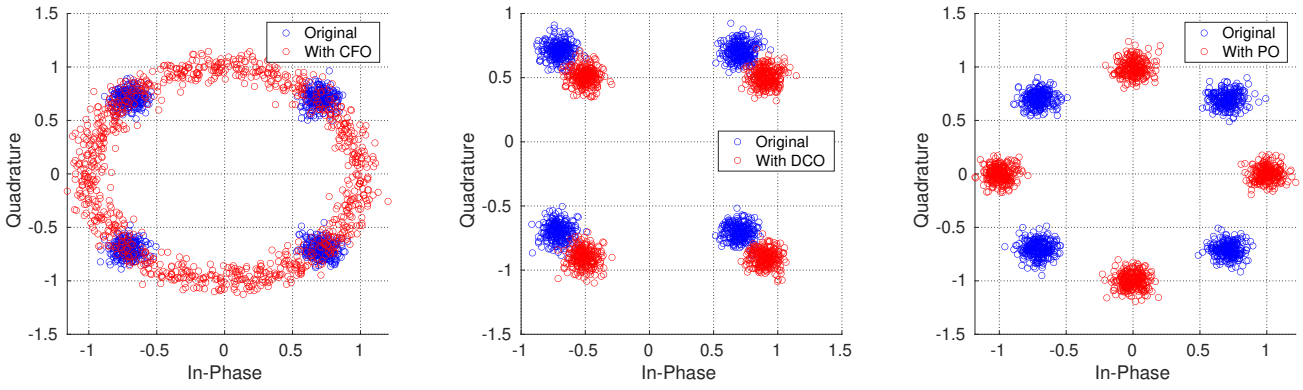
All nodes—whether Alice or Eve—must pass through an authenticator to access network resources. The authenticator is a critical component, responsible for identifying and authenticating legitimate nodes while detecting and denying access to malicious ones. This process ensures that only trusted devices can participate in the network's communication, thereby safeguarding the network's integrity and functionality.

However, the sophistication of malicious nodes poses a formidable challenge as they can bypass existing security protocols by exploiting weak encryption methods or flaws in the authentication process. For example, Eve might impersonate a legitimate node by presenting compromised credentials (e.g., MAC address, password, or device ID) to the network's authenticator, effectively masquerading as an authorized device, "Alice".

Given the potential threats posed by malicious nodes, it is crucial to implement enhanced security measures. The next section introduces a new PLA approach designed to protect the network from these threats. This advanced PLA utilizes distinctive device-based features such as CFO, DCO, and PO to create unique, unreplicable signatures for each device. These signatures ensure that each device's identity is distinct and verifiable, significantly enhancing network security and data integrity.

3. Proposed Authentication Scheme

In this section, we detail the PLA scheme designed to authenticate both authorized and malicious devices within



(a) (b) (c)

Figure 3: Effect of hardware impairment on RF data (a) CFO effect (b) DCO effect (c) PO effect.

the network. Our proposed method leverages a combination of three distinct device imperfections: CFO, DCO, and PO, to establish a robust authentication process. This process is executed through several key phases: data collection, data pre-processing, feature extraction, feature selection methods, ML model development and selection under malicious device attacks, and finally, device authentication, as illustrated in Figure 2. Each of these phases is comprehensively detailed in the following sections.

3.1. RF Data Impairments Characteristics

In our study, the signals of interest are represented by in-phase and quadrature (I/Q) components, which play a critical role in defining a device's communication characteristics. These I/Q data streams contain distinct hardware imperfections that can be exploited for authentication purposes. We focus on three primary types of hardware-induced variations: CFO, DCO, and PO. These three impairments were selected because they provide a comprehensive and reliable representation of a device's unique hardware characteristics, which are vital for effective authentication. Unlike channel-based features such as CIR and RSS, which are heavily influenced by environmental factors like multipath fading and noise, CFO, DCO, and PO are intrinsic to the device and remain stable under varying conditions. This makes them more consistent and dependable indicators of a device's identity. By integrating these hardware-based impairments, we capture a wide range of device-specific distortions, thereby enhancing the distinctiveness of signal signatures. This approach ensures that the authentication process is resilient against various attack scenarios, even when malicious nodes possess similar or identical hardware, significantly improving both accuracy and security in dynamic wireless environments.

The baseband complex signal $x_b(t)$ at time t can be decomposed into its in-phase (I) component $x_{b,I}(t)$ and quadrature (Q) component $x_{b,Q}(t)$:

$$x_b(t) = x_{b,I}(t) + jx_{b,Q}(t) = r(t)e^{j\phi(t)}, \tag{1}$$

where $r(t)$ is the amplitude, and $\phi(t)$ is the phase. Assuming no hardware impairments, the ideal RF signal $x(t)$ is given by the real-valued combination of the in-phase and quadrature components modulated onto a carrier frequency f_c:

$$x(t) = x_{b,I}(t)\cos(2\pi f_c t) + x_{b,Q}(t)\sin(2\pi f_c t). \tag{2}$$

However, practical RF signals often experience distortions due to hardware imperfections, including DCO, CFO, and PO.

3.1.1. Carrier Frequency Offset (CFO). The carrier frequencies for up-conversion and down-conversion are generated by the transmitter and receiver using their respective Local Oscillators (LOs), which may not oscillate at exactly the same frequency. Let $y(t)$ denote the ideal signal received at the antenna. The baseband signal $y_b(t)$, obtained after down-conversion, is given by:

$$y_b(t) = y(t)e^{-j2\pi f_{c,r}t}, \tag{3}$$

where $f_{c,r}$ represents the receiver's local carrier frequency. The carrier frequency offset ϵ_f is defined as the difference between the transmitter's carrier frequency $f_{c,t}$ and the receiver's carrier frequency $f_{c,r}$, i.e., $f_{c,r} = f_{c,t} + \epsilon_f$. Therefore, Eq (3) is rewritten as:

$$y_b(t) = y(t)e^{-j2\pi(f_{c,t}+\epsilon_f)t}. \tag{4}$$

The carrier waves at the receiver, affected by CFO, is modeled as:

$$\cos(2\pi(f_{c,t}+\epsilon_f)t) \quad \text{and} \quad \sin(2\pi(f_{c,t}+\epsilon_f)t). \tag{5}$$

3.1.2. Direct Current Offset (DCO). DC Offset is an undesirable characteristic in RF communication systems where a DC component is superimposed on the desired AC signal. It originates from imbalances and leakage currents in the mixers or imperfections in the analog-to-digital converters. If $y(t)$ represents the ideal AC component of the received

signal, the presence of DCO alters the baseband signal $y_b(t)$ as follows:

$$y_b(t) = y(t) + DC_I + jDC_Q, \tag{6}$$

where DC_I is the in-phase component and DC_Q is the quadrature component of the DC offset. The in-phase and quadrature components of the received signal, including the DCO, can be separately modeled as:

$$y_{b,I}(t) = \Re\{y_b(t)\} = \Re\{y(t)\} + DC_I, \tag{7}$$

$$y_{b,Q}(t) = \Im\{y_b(t)\} = \Im\{y(t)\} + DC_Q, \tag{8}$$

here, $\Re\{\}$ and $\Im\{\}$ denote the real and imaginary parts of the baseband signal, respectively.

3.1.3. Phase Offset (PO). Similar to CFO, Phase Offset (PO) is another form of imperfection that affects the integrity of the transmitted RF signal. It is a deviation from the expected phase and occurs due to inconsistencies in the phase response of the RF chain in the transmitter and receiver. The PO can be modeled as an additional phase term in the received signal:

$$y_b(t) = y(t)e^{j(\phi_t + \Delta_\phi)}, \tag{9}$$

where Δ_ϕ is the constant phase error introduced by the phase offset. This phase error can result from various sources, such as mismatches in the phase-locked loop (PLL) and temperature variations affecting the circuitry.

The presence of CFO, DCO, and PO shifts the signal's constellation points, creating distinct patterns that can be leveraged for authentication purposes. As illustrated in Figure 3, each of these imperfections introduces unique distortions that generate identifiable patterns specific to each device, making them useful for developing hardware-based authentication systems.

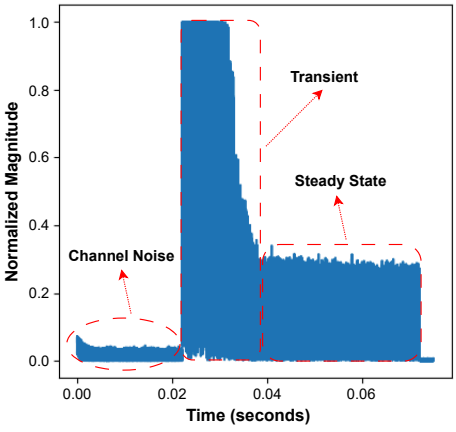


Figure 4: Signal Response Phases.

3.2. Data Pre-processing

3.2.1. Transient Detection and Filtering. In our methodology, we focus on the transient part of the signal, commonly known as the "burst transient." This particular region occurs when a transmitter transitions from an idle state to an active transmission mode (see Figure 4). The burst transient exhibits distinct characteristics unique to each transmitting device, making it highly suitable for authentication purposes [30]. Accurate separation of the transient signal from noise and the steady-state portion of the received signal is essential to extract reliable signatures. To achieve this, we adopted the amplitude-based Variance Trajectory (VT) burst detection technique described in [31] to identify the onset of each transmission burst. This approach allows for precise extraction of the transient signal from the overall signal collection before generating the RF signature. The methodology in [31] is particularly advantageous because it focuses on the time-invariant aspects of signature generation and addresses the impact of sample registration (both cross-burst and cross-collection alignment) using emissions from the same devices. The extracted signal segment is then filtered using a low-pass Chebyshev filter of order 4. This filter is designed with a sharp roll-off to reduce high-frequency noise and emphasize the unique features of the transient burst. The filter effectively mitigates interference and background noise that could obscure the burst's distinctive characteristics, ultimately enhancing the quality of the RF signature.

3.2.2. Features Generation. The generation of robust RF signal signatures is crucial for the authentication and verification of RF devices. This section explores computational strategies and mathematical formulations to identify distinctive features in RF signals, essential for creating these signatures. Our feature extraction process consists of two main phases: **(1)** initial transformation and **(2)** feature extraction through statistical analysis. The initial transformation utilizes the Discrete Gabor Transform (DGT), a two-dimensional analytical approach designed to simultaneously capture momentary and localized time-frequency variations. This process reveals hidden patterns and nuances that contribute to the statistical signature features, offering an accurate representation of the RF signal characteristics. The DGT is defined as [32]:

$$G_{mn} = \sum_{k=0}^{RS-1} x(k)W^*(k - mS)\exp\left(-i2\pi\frac{nk}{T}\right), \tag{10}$$

where G_{mn} are Gabor coefficients, $x(k) = x(k + vRS)$ is the input signal, and $W(k) = W(k + vRS)$ is the analysis window. RS is the product of the number of samples shifted (S) and the oversampling factor (R). The indices m (where $m = 1, 2, \ldots, R$) correspond to the time shifts, and n (where $n = 0, 1, \ldots, T-1$) correspond to the frequency bins, while T represents the number of frequency bins. The DGT is implemented using a Gaussian analysis window [32].

The extraction of the RF signature is based on the normalized, magnitude-squared Gabor coefficients $|G_{mn}|^2$.

The normalization process is critical for ensuring uniformity across signals with varying strengths and is performed using the following equation:

$$|Z_{xx}|^2 = \frac{|G_{mn}|^2 - \min(|G_{mn}|^2)}{\max(|G_{mn}|^2) - \min(|G_{mn}|^2)}, \tag{11}$$

where $\min(G_{mn})$ and $\max(G_{mn})$ are the minimum and maximum values of the Gabor coefficients, respectively.

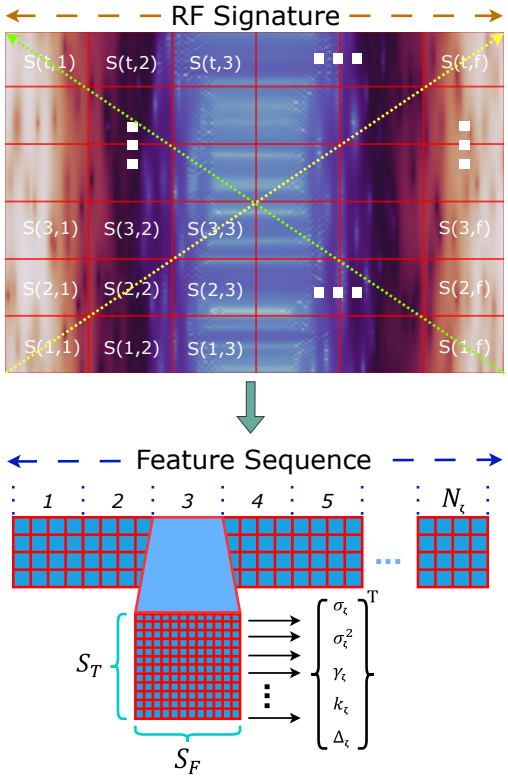


Figure 5: Feature generation using DGT approach.

As shown in Figure 5, the resulting time-frequency (T-F) surface is subdivided into S_R 2-D segments. Each segment contains $S_T \times S_F$ values, where $S_T = 15$ and $S_F = 15$ represent the length of the segment along the time and frequency dimensions, respectively. Initially, segments are extracted diagonally from the first two diagonals of the T-F matrix to quickly converge on features that significantly enhance the distinguishing capability (see Figure 5). Subsequent segments are extracted horizontally, ensuring comprehensive coverage and analysis of the signal spectrum. Each segment is then reshaped into a 1-D vector for feature calculation. A total of five features are then calculated for each segment: standard deviation (σ_ζ), variance (σ_ζ^2), skewness (γ_ζ), kurtosis (k_ζ), and entropy (Δ_ζ). The calculated features are arranged as follows for each segment l (where $l = 1, 2, \ldots, S_R$):

$$F_{\zeta_l} = [\sigma_{\zeta_l}, \sigma^2_{\zeta_l}, \gamma_{\zeta_l}, k_{\zeta_l}, \Delta_{\zeta_l}]_{1\times 5}, \tag{12}$$

The composite feature vector for a given segment is formed by concatenating F_{ζ_l} from all segments, resulting in the final RF signature:

$$\mathbf{F} = \left[F_{\zeta_1} : F_{\zeta_2} : F_{\zeta_3} : \cdots : F_{\zeta_{S_R}}\right]_{1\times 5S_R}, \tag{13}$$

Algorithm 1 Feature Generation Process

Require: RF signal $x(k)$
Ensure: RF signature $\mathbf{F}$
procedure GENERATERFSIGNATURE
  Phase 1: Initial Transformation
  Calculate Gabor coefficients G_{mn} via eq. (10).
  Normalize the magnitude-squared Gabor coefficients $|G_{mn}|^2$ via eq. (11).
  Phase 2: Feature Extraction using Statistical Analysis
  Divide the T-F surface into S_R 2-D segments.
  for each segment l (where $l = 1, 2, \ldots, S_R$) **do**
    Reshape segment into a 1-D vector.
    Calculate statistical features for each segment: σ_{ζ_l}, $\sigma^2_{\zeta_l}$, γ_{ζ_l}, k_{ζ_l}, and Δ_{ζ_l}.
    Form feature vector for segment l as eq. (12).
  end for
  Concatenate feature vectors from all segments to form the final RF signature as eq. (13).
end procedure

The entire procedure for extracting features to create the RF signature is illustrated in Algorithm 1.

3.3. Feature Selection Approaches (FSs)

From an authentication perspective, input signature sets often contain non-salient features that can diminish the accuracy. As the number of features increases, the computation time and the number of required training samples grow exponentially [33]. Thus, feature selection (FS) plays a crucial role in this context, as it significantly impacts model performance by reducing redundancy and enhancing predictive accuracy. In this paper, we employ four FS approaches to evaluate our proposed method: Mutual Information (MI), Analysis of Variance (ANOVA), Principal Component Analysis (PCA), and Recursive Feature Elimination (RFE).

3.3.1. Mutual Information (MI). MI measures the dependency between features and the target variable, selecting features that provide the most information about the target. It is calculated as [34]:

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\left(\frac{p(x,y)}{p(x)p(y)}\right), \tag{14}$$

where $p(x, y)$ is the joint probability distribution, and $p(x)$ and $p(y)$ are the marginal distributions. Features with higher MI values are prioritized for model inclusion.

3.3.2. Analysis of Variance (ANOVA). ANOVA F-test assesses the impact of each feature on the target variable

by comparing the variance between groups to the variance within groups [35]:

$$F_v = \frac{\text{Between-group variability}}{\text{Within-group variability}}, \tag{15}$$

This metric indicates feature importance based on their ability to differentiate between groups defined by the target variable. Higher F-values suggest that the feature has a greater ability to distinguish between different target groups, making it a valuable feature for model inclusion.

3.3.3. Recursive Feature Elimination (RFE). RFE uses Logistic Regression to rank features based on the absolute values of their coefficients, iteratively removing the least significant features [36]:

$$\text{importance}_\zeta = |\beta_\zeta|, \tag{16}$$

where β_ζ is the coefficient of feature ζ. This process continues until the optimal subset of features is determined.

3.3.4. Principal Component Analysis (PCA). PCA reduces dimensionality by transforming features into a new set of variables, called principal components, which capture most of the data variance [37].

$$\text{Variance Retained} = \frac{\sum_{u=1}^{r} \lambda_u}{\sum_{v=1}^{s} \lambda_v}, \tag{17}$$

where λ_u are the eigenvalues, r is the number of components retained, and s is the total number of features. This method is beneficial in settings with high feature correlation.

4. Machine Learning (ML) Modules

In our authentication approach, we employ a binary classification framework to train and evaluate multiple machine learning models for device authentication. To formalize, consider a set of devices $\mathcal{D} = \{D_1, D_2, \ldots, D_N\}$. Each device D_i generates a set of RF features, forming a feature vector $\mathbf{F}_i$. These individual vectors contribute to the overall feature matrix $\mathbf{X} \in \mathbb{R}^{n_s \times d}$, where n_s represents the number of samples and d denotes the number of features. Feature selection identifies then the most relevant subsets $\{\mathbf{X}'_1, \mathbf{X}'_2, \ldots, \mathbf{X}'_{k_s}\} \subset \mathbf{X}$. The goal is to authenticate a target device $D_t \in \mathcal{D}$. For binary classification, the target device D_t under verification is labeled as class 1, while the remaining devices are labeled as class 0. This labeling is represented by the vector $\mathbf{y} \in \{0,1\}^{n_s}$. This method ensures our models are trained without malicious device data, reflecting the real-world scenario where information about potential attackers is unavailable.

Our model selection algorithm iterates over the selected feature subset $\{\mathbf{X}'_1, \mathbf{X}'_2, \ldots, \mathbf{X}'_{k_s}\}$ to train different ML models. Let M_q represent the q-th ML model, and for each M_q, we train the model and evaluate its performance using key metrics. Specifically, the performance metrics include the true authorized detection rate (TDR_A), false authorized detection rate (FDR_A), and true malicious detection rate (TDR_M).

To determine how well each model meets the predefined performance criteria, we compute a closeness score CS. This score provides a balanced evaluation of the model's ability to authenticate legitimate devices and detect malicious ones. The score is defined based on the differences between the model's performance metrics and their respective thresholds. Specifically, Let TDR_{th} be the threshold for the true detection rate and FDR_{th} be the threshold for the false detection rate. Let $A = \text{TDR}_A - \text{TDR}_{\text{th}}$, $B = \text{FDR}_A - \text{FDR}_{\text{th}}$, and $C = \text{TDR}_M - \text{TDR}_{\text{th}}$. Consequently, the closeness score is calculated as:

$$\text{CS} = |A| + |B| + |C|. \tag{18}$$

The decision to select a model is based on its ability to achieve a TDR_{th} of at least 95% and maintain an FDR_{th} below 5% for both authorized and malicious devices. If a model meets these criteria, i.e., $\text{TDR}_A \geq \text{TDR}_{\text{th}}, \text{FDR}_A \leq \text{FDR}_{\text{th}}, \text{TDR}_M \geq \text{TDR}_{\text{th}}$, it is selected directly. Otherwise, the model with the lowest closeness score is selected, indicating its proximity to the desired performance benchmarks, as follows:

$$\text{best\_model} = \arg\min_{M_q} \text{CS}_q. \tag{19}$$

We conduct experiments with various robust ML models to compare their effectiveness across different scenarios. Each model is carefully chosen for its specific strengths in handling different aspects of classification tasks, from managing high-dimensional spaces to efficiently modeling non-linear decision boundaries. The models include:

- M_1: **Random Forest (RnF)** and M_2: **XGBoost (XGB)** are particularly effective in environments where the decision boundaries are complex and the data may contain nonlinear relationships [38], [39].
- M_3: **Support Vector Machines (SVM)** are utilized for their capability to find the optimal hyperplane in high-dimensional spaces, which is crucial for achieving fine-grained separation between classes [40].
- M_4: **Logistic Regression (LR)** provides robust probabilistic outputs, essential for making threshold-based decisions in authentication tasks [41].
- M_5: **K-Nearest Neighbors (KNN)** offers a straightforward implementation that excels in scenarios where the relationship between features is more intuitive or geometrically interpretable [42].

These models are integrated into our PLA process, where they are trained and fine-tuned as outlined in Algorithm 2. To ensure reproducibility, we evaluate the techniques on our dataset and release all the code used to run the experiments presented in the paper[1].

5. Experimental Evaluation

In this section, we present the experimental validation of our PLA approach. First, we describe the experimental setup and the specific scenarios used for evaluation. Then, we analyze and discuss the authentication performance results.

1. https://github.com/PLA-AP/PLA

Algorithm 2 ML Model Selection and Evaluation for Device Authentication

Require: $\mathcal{D}$, $\mathbf{X}$, TDR_{th}, FDR_{th}
Ensure: best_model, best_feature_subset
Apply feature selection approach on $\mathbf{X}$ to obtain subsets $\{\mathbf{X}'_1, \mathbf{X}'_2, \ldots, \mathbf{X}'_{k_s}\}$
Models $\leftarrow$ {RnF, XGB, SVM, LR, KNN}
for each device D_t in $\mathcal{D}$ **do**
  for each model M_q in Models **do**
    for each feature subset $\mathbf{X}'_i$ in $\{\mathbf{X}'_1, \mathbf{X}'_2, \ldots, \mathbf{X}'_{k_s}\}$ **do**
      Prepare training and test sets for D_t
      Train M_q on training set
      Evaluate M_q on test set to compute performance metrics: TDR_A, FDR_A, TDR_M
      if $\text{TDR}_A \geq \text{TDR}_{\text{th}}$ **and** $\text{FDR}_A \leq \text{FDR}_{\text{th}}$ **and** $\text{TDR}_M \geq \text{TDR}_{\text{th}}$ **then**
        best_model $\leftarrow M_q$
        best_feature_subset $\leftarrow \mathbf{X}'_i$
        return best_model, best_feature_subset
      else
        Compute CS via (18)
        if CS $<$ best_CS **then**
          best_model $\leftarrow M_q$
          best_CS $\leftarrow$ CS
          best_feature_subset $\leftarrow \mathbf{X}'_i$
        end if
      end if
    end for
  end for
end for
  return best_model, best_feature_subset

5.1. Experimental Setup and Scenarios

The experimental setup for transmitting and receiving wireless signals is depicted in Figure 6. Our experiment was designed to accurately replicate a real-world RF communication environment, specifically tailored for evaluating our hybrid PLA scheme. The setup is detailed in three subsections: Hardware and Software Implementation, Experimental Procedure, and Dataset Description.

5.1.1. Hardware and Software Implementation. The system operates on Windows 11 with a 12th Gen Intel® Core™ i7-12800H processor. This processor has 14 cores and features a base clock speed of 2.4 GHz. The system is equipped with 32 GB of RAM. For the transmission and reception of RF signals, we utilized two BladeRF 2.0 Micro xA4 Software-Defined Radios (SDRs). These SDRs operate within a frequency range of 47 MHz to 6 GHz and feature a high sampling rate of 61.44 MHz. Each SDR was paired with a VERT 2450 antenna to facilitate effective signal transmission and reception. The SDRs were connected to laptops via USB 3.0 SuperSpeed connections, ensuring high-speed data transfer necessary for real-time signal processing. On the software side, GNURadio, a versatile real-time signal processing tool, was employed to configure the SDRs for transmitting and receiving RF signals. GNURadio also played a crucial role in performing real-time visual analysis in both time and frequency domains, applying initial signal preprocessing steps, and storing I/Q samples for subsequent analysis.

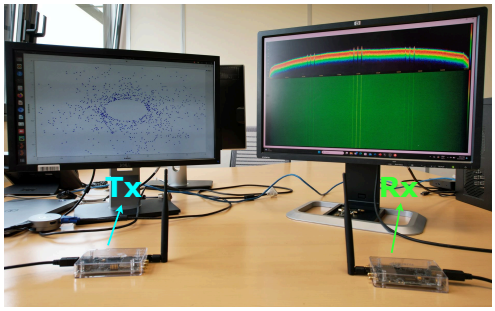


Figure 6: Experiment Setup.

5.1.2. Experimental Procedure. In this experiment, the procedure begins with configuring the transmitting SDR (Tx) to generate and broadcast a signal, with the parameters such as frequency, amplitude, and modulation being meticulously set using GNURadio. Predefined imperfection parameters are then introduced to embed unique hardware-induced characteristics that are essential for device authentication. The transmitted signal is visualized in real-time, ensuring accurate setup before broadcasting it via the VERT 2450 antenna. On the receiving side, the receiving SDR (Rx) captures the transmitted signal using its corresponding VERT 2450 antenna. The captured signal is simultaneously processed and visualized in real-time using GNURadio blocks, displaying both the time-domain signal and frequency spectrum, which allows for immediate evaluation of the signal quality and integrity. After capturing, the I/Q samples of the received signal are stored for further detailed analysis. The specifics of the captured dataset are described in the subsequent subsection.

5.1.3. Dataset Description. Our RF data consists of I/Q samples collected using Blade RF 2.0 Micro xA4 SDR devices. These devices operate at a center frequency of f = 5 GHz, and the received signals are recorded with a sampling frequency of F_s = 20 Msps, and a bandwidth of B = 10 MHz. To simulate real-world scenarios and evaluate the robustness of our proposed authentication scheme, we introduced specific imperfections into the RF signals. These imperfections were carefully calibrated to reflect typical distortions encountered in wireless communications environments. We applied three distinct types of hardware impairments: CFO, DCO, and PO. Each type of impairment was varied across three predetermined levels—labeled as V1, V2, and V3—to create a series of 12 different combinations, each representing a distinct device scenario as shown in Table 1.

The specific values for each type of impairment were chosen based on experimental measurements conducted on real devices. Specifically, for CFO, the levels were set at 50 KHz (V1), 100 KHz (V2), and 200 KHz (V3) to capture typical frequency drifts [43]. For DCO, the levels were defined as 10 mV (V1), 50 mV (V2), and 100 mV (V3),

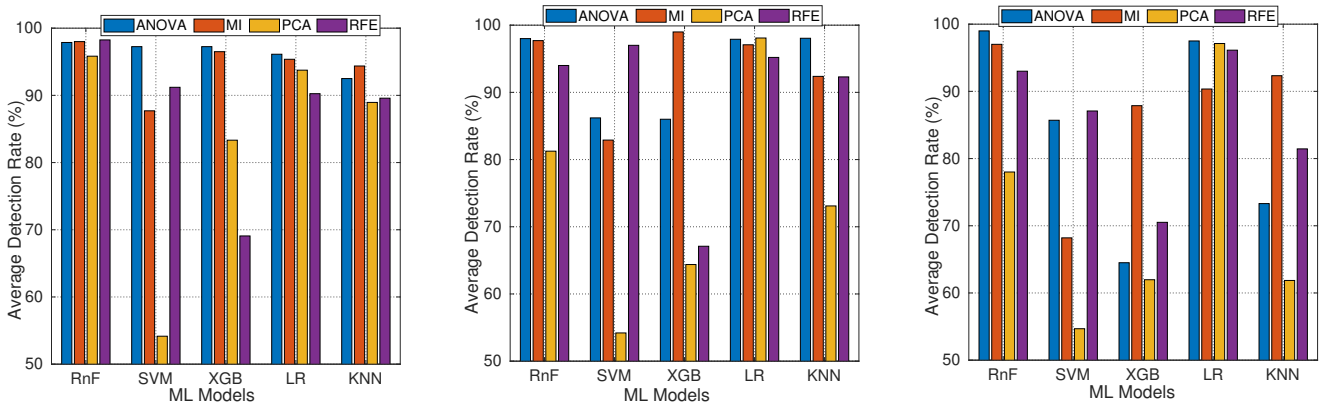


Figure 7: Average detection rate for different ML and FS models for (a) Scenario 1 (b) Scenario 2 (c) Scenario 3.

TABLE 1: Devices and their configurations across different parameters.

Devices	CFO	DCO	PO	Devices	CFO	DCO	PO
device 1	V1	V1	V1	**device 7**	V3	V3	V1
device 2	V1	V1	V2	**device 8**	V3	V3	V2
device 3	V1	V1	V3	**device 9**	V3	V3	V3
device 4	V2	V2	V1	**device 10**	V1	V2	V1
device 5	V2	V2	V2	**device 11**	V1	V2	V2
device 6	V2	V2	V3	**device 12**	V1	V2	V3

reflecting common hardware offsets [44]. Lastly, for PO, the levels were set at 11.5°(V1), 17.2°(V2), and 45°(V3) to account for usual phase misalignments during transmission and reception [45]. The SNR of the collected signal is 20 dB. To simulate different SNR levels and evaluate the noise effects, we added varying levels of Additive White Gaussian Noise (AWGN) to the received I/Q samples, ranging from 1 to 15 dB.

TABLE 2: Configuration of devices in each Scenario

Scenarios	Auth. Devices	Mal. Devices
Scenario 1	device 3, device 2, device 12, device 9	8 devices
Scenario 2	device 10, device 6, device 12, device 3, device 11, device 1	6 devices
Scenario 3	device 1, device 10, device 9, device 8, device 12, device 11, device 6, device 7	4 devices

To ensure a comprehensive analysis, we designed and implemented three distinct scenarios, each with a specific configuration of authorized and malicious devices. These scenarios were created to evaluate the model's performance under various conditions, considering the number of devices in both categories. The details of these scenarios are summarized in Table 2.

- **Scenario 1:** This scenario focuses on assessing the model's ability to accurately detect malicious devices by exposing it to varied unauthorized patterns.
- **Scenario 2:** This scenario aims to create a balanced testing environment with an equal number of authorized and malicious devices. The objective is to evaluate the model's performance in terms of both detection accuracy and false alarms.
- **Scenario 3:** This scenario examines the model's ability to maintain high detection rates when confronted with a larger and more diverse set of authorized devices.

The RF signature of malicious devices are exclusively used for testing, ensuring they do not influence the training phase or the selection process of the "best" model, but serve to assess the model's effectiveness in malicious detection. Our dataset comprises 84,000 statistical features for 12 devices, with 80% used for training and 20% for testing.

5.2. Experimental Results and Discussions

5.2.1. Performance Analysis. In this section, we present a comparative analysis of our PLA approach utilizing various feature selection methods and ML models. Our objective is to identify the most effective combination of methods for selecting the optimal set of signature features, ultimately enabling node authentication based on the detection rates of both authorized and malicious devices. We consider four different feature selection methods: MI, RFE, PCA, and ANOVA. Additionally, we evaluate the performance of five different machine learning models: RnF, SVM, XGB, LR, and KNN.

Figure 7 illustrates the average detection rates for each combination across three scenarios. In Scenario 1, which focuses on detecting malicious devices, RnF paired with ANOVA and MI achieves detection rates above 97% due to its robustness in identifying unfamiliar patterns. SVM performs well (around 96% with ANOVA) but shows significant sensitivity to feature selection approaches, dropping to 55% with PCA. LR remain stable across different feature selection methods, consistently achieving detection rates $\geq$ 95% using ANOVA, MI, and PCA. XGB and KNN also perform reasonably well with ANOVA and MI, achieving rates of around 94%, but exhibit significant drops with PCA and RFE. In Scenario 2, a balanced environment with equal numbers of authorized and malicious devices, distinguishing between the two classes becomes more challenging,

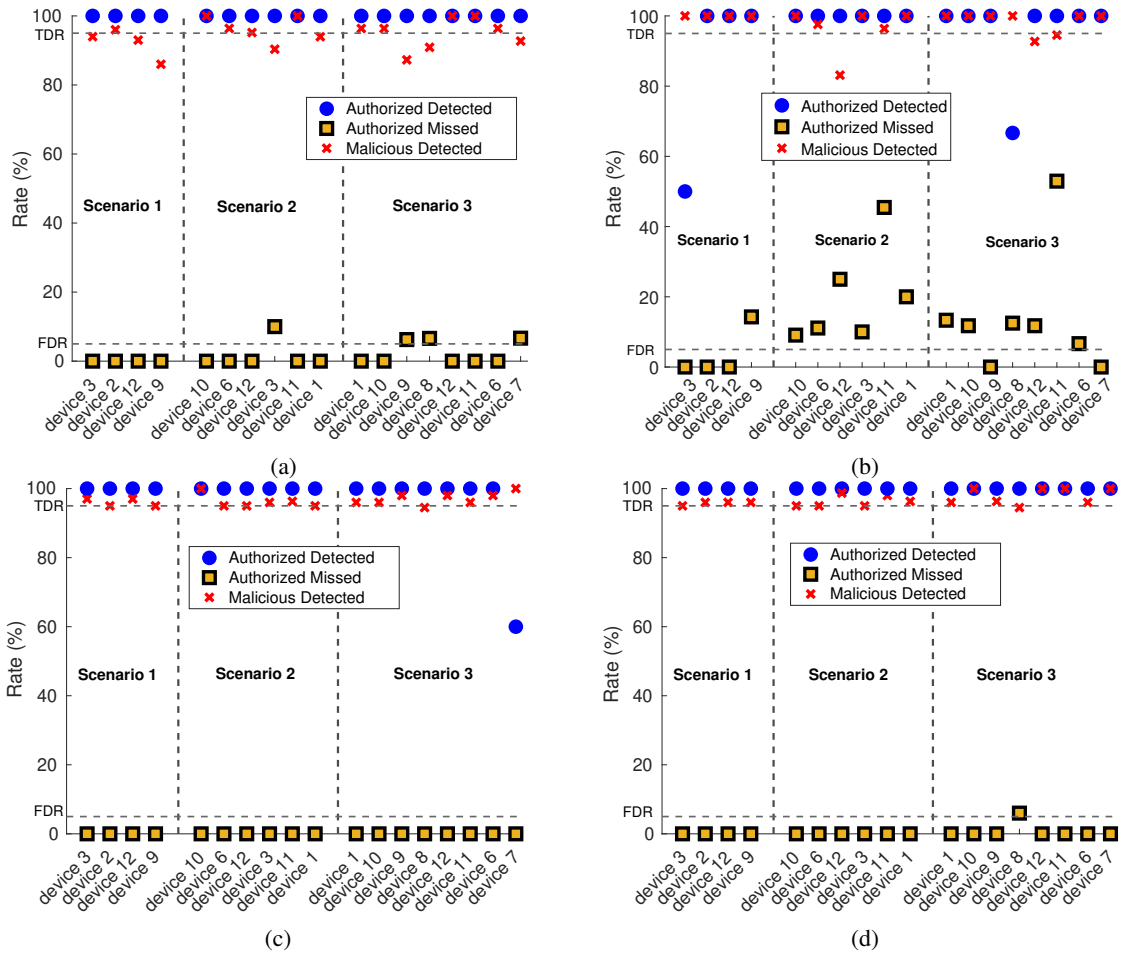
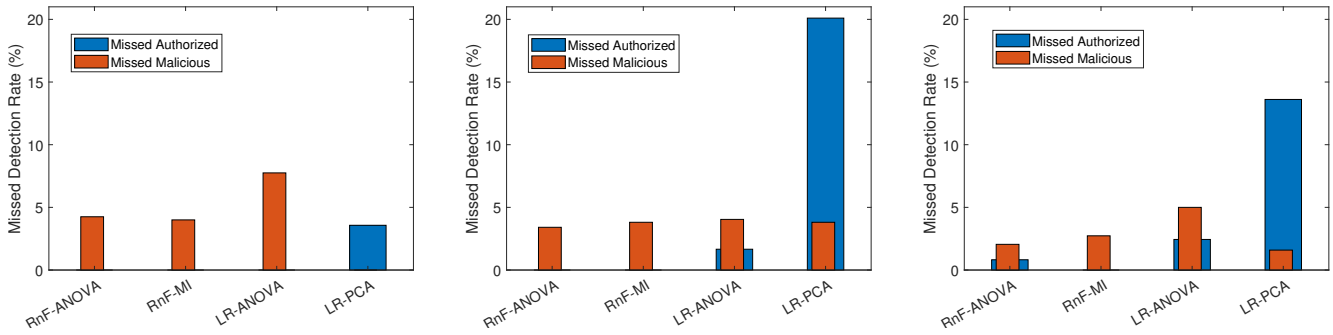


Figure 8: Authentication Rate for different combinations of FS and ML models (a) LR-ANOVA (b) LR-PCA (c) RnF-MI (d) RnF-ANOVA.

affecting false positive rates. Here, SVM shows strong performance with RFE (97%) but drops with PCA. RnF with ANOVA and MI remains robust ($\geq$ 97%), highlighting its adaptability. XGB and KNN perform well with MI ($\geq$ 94%) but experience a significant drop with PCA (69%). In Scenario 3, the model was challenged with more diverse set of authorized device patterns. This scenario led to a decline in the performance of XGB and KNN, as they struggled to adapt to the increased variety of authorized devices. In contrast, RnF with ANOVA and MI, as well as LR with ANOVA and PCA, remained effective ($\geq$ 96%), highlighting their adaptability to diverse authorized device patterns. Overall, RnF with ANOVA and MI, along with LR with ANOVA and PCA, proved consistently reliable across all scenarios, demonstrating their robustness in handling various device patterns.

After conducting a comprehensive analysis of the selected methods' performance, as depicted in Figure 7, we will now delve deeper into the individual performance of each method. Based on the results in Figure 7, the verification of authorized nodes and rejection of malicious ones are evaluated using the top combinations of FS methods and ML models. This includes RnF with ANOVA and MI and LR with ANOVA and PCA. These methods are assessed using three key metrics: detection of authorized devices, misdetection of authorized devices, and detection of malicious devices. For verifying authorized radios, the "best" authentication performance is defined by achieving a TDR of at least 95% and a FDR of no more than 5% for the remaining authorized radios (i.e., those not being verified). Similarly, the "best" performance in rejecting malicious attempts is characterized by a TDR of at least 95% for all malicious radios attempting to gain network access. This ensures robust detection and rejection of malicious devices, thereby safeguarding the network from potential threats.

Figure 8 illustrates the detection and the authentication performance across all scenarios for the four selected approaches. In Scenario 1, RnF-ANOVA and RnF-MI show superior performance with nearly 100% TDR for authorized devices and TDRs $\geq$ 95% for malicious devices, while keeping FDRs below 5%. This highlights their robustness in identifying unauthorized patterns. Conversely, LR-PCA struggles with elevated FDRs above 5% for certain devices and a lower TDR of 55% for device 3, indicating its



(a) (b) (c)

Figure 9: Comparative Analysis of ML Algorithms on Missed Detection Rates for (a) Scenario 1 (b) Scenario 2 (c) Scenario 3.

difficulty in distinguishing authorized devices in high malicious activity environments. In the balanced environment of Scenario 2, RnF-ANOVA and RnF-MI maintain their reliability with TDRs above 95% for all authorized devices and an FDR of 0% for the remaining nodes. They also achieve TDRs $\geq$ 95% for malicious devices, showcasing their adaptability in balanced settings. However, LR-PCA struggles, misclassifying other authorized devices (FDR $\geq$ 5%) and missing some malicious ones, such as in case of device 12 with a TDR of 88%, highlighting its sensitivity to balanced distributions and its inability to retain subtle distinguishing features. LR-ANOVA performs better for detecting authorized devices but sometimes falls short on TDRs for malicious ones. In Scenario 3, which tests the models with a diverse set of authorized device patterns, RnF-ANOVA maintains high TDRs close to 100%, showing strong adaptability. RnF-MI also performs well but inconsistently, particularly with device 7 (TDR = 66%), indicating challenges with high patterns diversity. LR-ANOVA detects authorized nodes reasonably well but struggles with false acceptance of the others authorized and malicious nodes, showing FDRs above 5% and TDRs below 95% for devices 7, 8, and 9. LR-PCA performs poorly, with high misdetection rates for authorized devices like device 8 (TDR = 72%) and fails to detect malicious nodes effectively, with TDRs below 95% for devices 11 and 12. In evaluating different combinations of models and feature selection methods, our analysis highlights the overall superiority of the RnF paired with ANOVA. This combination consistently achieves detection rates above 96% and maintains an FDR of less than 5%, surpassing the approach in [24], which reports a TDR of 63% with an FDR of 5% at an SNR of 20 dB. It also outperforms the study in [46], which achieved a TDR of 85% with an FDR of 5%. Our method not only improves detection accuracy but also significantly reduces false alarms compared to these studies. This robust performance makes RnF with ANOVA a strong candidate for effective and reliable deployment in security-critical environments.

For a more comprehensive understanding of the comparative performance of these approaches, Figure 9 illustrates the missed detection rates for both authorized and malicious devices across all three scenarios. RnF-ANOVA and RnF-MI consistently show low missed detection rates (below 5%) for both authorized and malicious devices across all scenarios, highlighting their robustness and ability to effectively handle new patterns. In contrast, LR-ANOVA and LR-PCA show significant shortcomings. LR-ANOVA often exceeds 5% missed detection rates for malicious devices in Scenario 1 and struggles with higher missed detection rates for authorized devices in Scenario 2 and Scenario 3, indicating difficulty with diverse authorized patterns. LR-PCA performs even worse, with missed detection rates for authorized devices surpassing 12% in Scenarios 2 and 3. This indicates poor adaptability to more diverse device patterns.

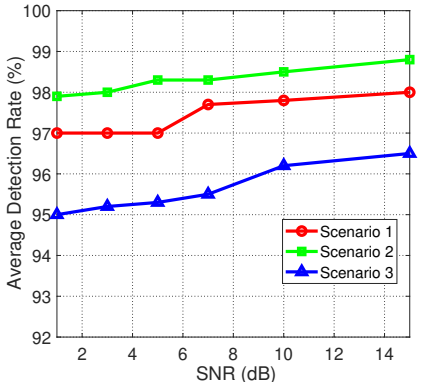


Figure 10: Average detection rate for different SNRs.

Based on the results presented in Figures 7, 8, and 9, RnF with ANOVA consistently demonstrates the best performance for verifying authorized devices and rejecting malicious ones, making it the most suitable choice for our system. Its robust detection capabilities are further reinforced in Figure 10, which illustrates the performance of our approach across varying SNRs in all three scenarios. Notably, in Scenario 2, the detection rate stays above 98% even at the lowest SNRs, demonstrating the model's stability and effectiveness. Scenario 1 starts around 97% at 1 dB and improves to 98% as SNR increases, showing reliable

detection of unauthorized patterns even in noisy conditions. Scenario 3, starting at 95% at 1 dB, improves to over 96.5% at higher SNRs, highlighting the model's ability to manage a diverse set of authorized devices despite significant noise levels. The robustness of our approach against SNR variations is particularly noteworthy when compared to previous works. For instance, [24] reported a significant decrease in detection accuracy from 63% to 42% when SNR fell below 10 dB. Similarly, [46] observed a decline in performance from 85% to 63% when the SNR dropped below 8 dB. These results underscore the reliability of RnF with ANOVA, demonstrating its resilience to varying noise environments and its consistent ability to distinguish between authorized and malicious devices across different scenarios.

5.2.2. Scalability and Energy Efficiency Analysis. Scalability and energy efficiency are vital for the practical deployment of the proposed PLA scheme, particularly in large-scale wireless networks with numerous nodes. These considerations are key to ensuring the approach remains feasible in real-world scenarios, where diverse network sizes and device types can greatly influence overall performance.

Scalability: The proposed PLA scheme is inherently scalable, utilizing the flexibility of ML models to handle a growing number of nodes. Our approach begins with offline model selection, where multiple ML models and feature selection techniques are tested on measured datasets to determine the optimal configuration for the given scenario. During this phase, models are fine-tuned to achieve high detection rates and low false-positive rates under existing network conditions.

As the network size increases, authentication complexity rises due to the larger number of devices that must be accurately identified. To address this, further hyper-parameter tuning should be conducted, adjusting key model parameters such as learning rates, regularization terms, and architecture specifics to accommodate the added complexity. By continuously adapting the models to the expanding network, we ensure that the PLA scheme remains effective in differentiating between authorized and malicious nodes, even as the network scales. Such adaptability is crucial for sustaining high detection rates and minimizing false positives, thereby supporting secure operations in expansive wireless networks.

Energy Efficiency: Another key aspect of the proposed scheme is its energy efficiency, which is particularly important for battery-powered devices in wireless networks. In our design, we consider a centralized network architecture where a single node, typically a server, serves as the authenticating entity responsible for verifying all other nodes. This configuration ensures that only the server node requires significant computational resources, thereby reducing the overall energy demand across the network.

To evaluate the energy efficiency of our approach, we analyzed the power consumption and time complexity of the proposed framework using a Jetson Nano Orin platform. The results show that the mean inference time for the most optimal model, RnF with ANOVA, is approximately 3.714 ms, with an average energy consumption of 25.341 mJ per inference. These metrics demonstrate that our approach is highly suitable for real-time dynamic applications, operating well within the energy constraints typical of wireless devices.

6. Conclusion and Future Work

This paper presented a robust device PLA scheme that leverages the hybridization of hardware impairments with ML models. The proposed scheme aims to authenticate devices effectively, even without prior knowledge of malicious characteristics. The ML models were trained using advanced feature extraction techniques, enabling clear differentiation between authorized and malicious entities. The development process involved fine-tuning the ML models through a series of controlled experiments to optimize their performance under diverse network conditions and various attack scenarios. Experimental validations on a commercial SDR platform confirmed the effectiveness of the proposed hybrid PLA approach, demonstrating high authentication rates for legitimate nodes and reliable detection rates for malicious device attacks. Additionally, the approach is highly efficient, with a mean inference time of less than 3.75 ms and power consumption below 25.5 mJ, confirming its suitability for real-time applications in energy-constrained environments. The method developed in this work can be effectively employed in modern wireless systems, where the rapid detection of malicious nodes, such as jammers or rogue nodes, is crucial. These findings validate the efficacy of the hybrid PLA scheme in bolstering device authentication and enhancing overall network security.

While the current approach relies on a centralized network architecture for authentication, there is growing industry interest in decentralized networks. In such architectures, each node independently authenticates others, which poses significant challenges in managing computational resources. Future research should focus on developing optimization strategies that align the proposed approach with the unique requirements of decentralized environments. We plan to implement this approach using various Raspberry Pi devices to represent the nodes and perform real-time authentication in our future work. Additionally, integrating deep learning techniques presents another promising direction that could further enhance the performance of the hybrid PLA scheme, leading to more advanced and reliable device authentication solutions.

Acknowledgment

This research was made possible with the support of the Horizon Europe research and innovation programme of the European Union, under grant agreement number 101092912 (project MLSysOps). The authors also gratefully acknowledge the support from the Regional STIMULE CORTESE project of the Hauts-de-France Region.

References

[1] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," *Comput. Netw.*, vol. 221, p. 109515, 2023.

[2] Y. Qian, F. Ye, and H.-H. Chen, *Security in Wireless Communication Networks*. John Wiley & Sons, 2021.

[3] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security," *IEEE Commun. Mag.*, vol. 60, no. 4, pp. 65–71, 2022.

[4] S. Boonkrong, *Authentication and Access Control: Practical Cryptography Methods and Tools*. Apress, New York, USA: Springer, 2021.

[5] S. Dey and A. Hossain, "Session-key establishment and authentication in a smart home network using public key cryptography," *IEEE Sensors Lett.*, vol. 3, no. 4, pp. 1–4, 2019.

[6] S. Atiewi *et al.*, "Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography," *IEEE Access*, vol. 8, pp. 113 498–113 511, Jun. 2020.

[7] Y. Zou *et al.*, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.

[8] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2356–2366, 2021.

[9] T. O. Olwal, K. Djouani, and A. M. Kurien, "A survey of resource management toward 5G radio access networks," *IEEE Commun. Surveys & Tuts.*, vol. 18, no. 3, pp. 1656–1686, 2016.

[10] J. Zhang *et al.*, "Physical layer security for the internet of things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.

[11] B. M. ElHalawany *et al.*, "Physical-layer security and privacy for vehicle-to-everything," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 84–90, Oct. 2019.

[12] P. Angueira *et al.*, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Commun. Surveys & Tuts.*, vol. 24, no. 2, pp. 810–838, 2022.

[13] N. Xie *et al.*, "Physical-layer authentication using multiple channel-based features," *IEEE Trans. Inf. Forensics and Security*, vol. 16, pp. 2356–2366, Jan. 2021.

[14] S. Tomasin, "Analysis of channel-based user authentication by key-less and key-based approaches," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 5700–5712, Sept. 2018.

[15] A. Mahmood *et al.*, "Channel impulse response-based distributed physical layer authentication," in *2017 IEEE 85th Veh. Technol. Conf. (VTC Spring)*. IEEE, 2017, pp. 1–5.

[16] S. Van Vaerenbergh *et al.*, "Physical layer authentication based on channel response tracking using gaussian processes," in *2014 IEEE Int. Conf. Acoustics, Speech and Signal Process. (ICASSP)*. IEEE, 2014, pp. 2410–2414.

[17] C. Pei *et al.*, "Channel-based physical layer authentication," in *2014 IEEE Global Commun. Conf.* IEEE, 2014, pp. 4114–4119.

[18] H. B. Eldeeb, A. Pandey, M. Andreoni, and S. Muhaidat, "Experimental evaluation of a lightweight RSS-based PLA scheme in multi-node multi-cell mesh networks," in *2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*. IEEE, 2023, pp. 393–398.

[19] E. Illi *et al.*, "Physical layer continuous authentication for wireless mesh networks: An experimental study," in *2022 IEEE Int. Mediterranean Conf. Commun. Netw. (MeditCom)*. IEEE, 2022, pp. 136–141.

[20] J. Tang *et al.*, "Light-weight physical layer enhanced security schemes for 5G wireless networks," *IEEE Netw.*, vol. 33, no. 5, pp. 126–133, Oct. 2019.

[21] T. D. Vo-Huu *et al.*, "Fingerprinting Wi-Fi devices using software defined radios," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016, pp. 3–14.

[22] W. Hou *et al.*, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[23] W. Hou, X. Wang, and J.-Y. Chouinard, "Physical layer authentication in ofdm systems based on hypothesis testing of cfo estimates," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 3559–3563.

[24] S. Zeng, X. Li, A. Salem, and D. Zhao, "Physical layer authentication based on cfo and visibility graph," in *2018 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2018, pp. 147–152.

[25] Y. Xing, A. Hu, J. Zhang, L. Peng, and X. Wang, "Design of a channel robust radio frequency fingerprint identification scheme," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6946–6959, 2022.

[26] H. B. Eldeeb, A. Pandey, M. Andreoni, and S. Muhaidat, "Exploiting engineered IQ samples for physical layer authentication," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*. IEEE, 2023, pp. 1–6.

[27] P. Hao, X. Wang, and W. Shen, "A collaborative phy-aided technique for end-to-end iot device authentication," *IEEE Access*, vol. 6, pp. 42 279–42 293, 2018.

[28] H. Fang, X. Wang, and L. Xu, "Fuzzy learning for multi-dimensional adaptive physical layer authentication: A compact and robust approach," *IEEE Transactions on Wireless Communications*, vol. 19, no. 8, pp. 5420–5432, 2020.

[29] E. Illi, M. Qaraqe, and F. El Bouanani, "A novel hybrid physical layer authentication scheme for multiuser wireless communication systems," *IEEE Internet of Things Journal*, 2023.

[30] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proceedings of the third ACM conference on Wireless network security*, 2010, pp. 89–98.

[31] R. Klein, M. A. Temple, M. J. Mendenhall, and D. R. Reising, "Sensitivity analysis of burst detection and rf fingerprinting classification performance," in *2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–5.

[32] M. J. Bastiaans and M. C. Geilen, "On the discrete gabor transform and the discrete zak transform," *Signal processing*, vol. 49, no. 3, pp. 151–166, 1996.

[33] K. W. Bauer Jr, S. G. Alsing, and K. A. Greene, "Feature screening using signal-to-noise ratios," *Neurocomputing*, vol. 31, no. 1-4, pp. 29–44, 2000.

[34] T. M. Cover, *Elements of information theory*. John Wiley & Sons, 1999.

[35] H. Ding, P.-M. Feng, W. Chen, and H. Lin, "Identification of bacteriophage virion proteins by the anova feature selection and analysis," *Molecular BioSystems*, vol. 10, no. 8, pp. 2229–2235, 2014.

[36] I. Guyon, J. Weston, S. Barnhill, and V. Vapnik, "Gene selection for cancer classification using support vector machines," *Machine learning*, vol. 46, pp. 389–422, 2002.

[37] M. Ringnér, "What is principal component analysis?" *Nature biotechnology*, vol. 26, no. 3, pp. 303–304, 2008.

[38] L. Breiman, "Random forests," *Machine learning*, vol. 45, pp. 5–32, 2001.

[39] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, 2016, pp. 785–794.

[40] C. Cortes and V. Vapnik, "Support-vector networks," *Machine learning*, vol. 20, pp. 273–297, 1995.

[41] D. R. Cox, "The regression analysis of binary sequences," *Journal of the Royal Statistical Society Series B: Statistical Methodology*, vol. 20, no. 2, pp. 215–232, 1958.

[42] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE transactions on information theory*, vol. 13, no. 1, pp. 21–27, 1967.

[43] T.-D. Chiueh and P.-Y. Tsai, *OFDM baseband receiver design for wireless communications*. John Wiley & Sons, 2008.

[44] Y. Zheng, J. Yan, and Y. P. Xu, "A cmos vga with dc offset cancellation for direct-conversion receivers," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 56, no. 1, pp. 103–113, 2008.

[45] A. Zubow, P. Gawłowicz, and F. Dressler, "On phase offsets of 802.11 ac commodity wifi," in *2021 16th Annual Conference on Wireless On-demand Network Systems and Services Conference (WONS)*. IEEE, 2021, pp. 1–4.

[46] Y. Liu, P. Zhang, J. Liu, Y. Shen, and X. Jiang, "Physical layer authentication in mimo systems: a carrier frequency offset approach," *Wireless Networks*, vol. 28, no. 5, pp. 1909–1921, 2022.