TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science Institute of System Architecture, Chair of Privacy and Data Security

Master Thesis

Physical layer authentication based on wireless channel fingerprinting

MD Shamsul Arefin Shad

Matriculation number: 4874145

18th February 2025

First referee

Prof. Dr.-Ing. Stefan Köpsell

Second referee

Ms Dr.-Ing. Elke Franz

Supervisor

Ms M.Sc. Ghazal Bagheri

TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science Institute of System Architecture, Chair of Privacy and Data Security

Task for the preparation of a Master Thesis

Course:	Distributed Systems Engineering
Name:	MD Shamsul Arefin Shad
Matriculation number:	4874145
Matriculation year:	2020
Title:	Physical layer authentication based on wireless channel fingerprinting

Objectives of work

This research explores using machine learning for Physical Layer Authentication (PLA), leveraging Channel Impulse Response (CIR) to authenticate legitimate senders in wireless networks. By utilizing Passive PLA, it aims to overcome the inefficiencies of traditional cryptographic methods. The study involves investigating CIR-based authentication techniques, developing machine learning models for classification, and evaluating their performance on real-world wireless data. Through this approach, the research seeks to enhance the security and efficiency of wireless authentication and make it robust against common threats.

Focus of work

- Conduct a thorough literature review on physical layer attributes relevant to wireless communication and existing PLA techniques.
- Investigate various machine learning algorithms for their suitability in identifying and learning the unique patterns of wireless channel attributes.
- Develop and implement a prototype model that applies these ML techniques to authenticate senders based on physical layer data.
- Evaluate the prototype's effectiveness in authenticating legitimate senders and its resilience against common security threats.

First referee:	Prof. Dr.-Ing. Stefan Köpsell
Second referee:	Ms Dr.-Ing. Elke Franz
Supervisor:	Ms M.Sc. Ghazal Bagheri
Issued on:	29th September 2024
Due date for submission:	2nd March 2025

Prof. Dr.-Ing. Stefan Köpsell
Supervising professor

Statement of authorship

I hereby certify that I have authored this document entitled *Physical layer authentication based on wireless channel fingerprinting* independently and without undue assistance from third parties. No other than the resources and references indicated in this document have been used. I have marked both literal and accordingly adopted quotations as such. There were no additional persons involved in the intellectual preparation of the present document. I am aware that violations of this declaration may lead to subsequent withdrawal of the academic degree.

Dresden, 18th February 2025

MD Shamsul Arefin Shad

Abstract

Secure authentication in wireless communication is crucial, especially for resource-constrained devices in Internet of Things (IoT). Traditional cryptographic methods impose high computational costs, making them impractical. This thesis explores CIR-based authentication, a passive PLA approach that leverages wireless channel characteristics for lightweight and secure authentication. We propose four CIR-based methods: (1) Principal Component Analysis (PCA) with Support Vector Machine (SVM), (2) Sparse Residual Classifier, (3) PCA with Sparse classifier, and (4) Sparse Dictionary Learning with SVM. These methods are evaluated using real-world Ultra-Wideband (UWB) channel data under various conditions and our results are compared to those of a reference work. Performance metrics include Authentication Rate (AR), Missed Detection Rate (MDR), and False Alarm Rate (FAR). Results show that all proposed methods outperform the reference work, with the Lasso-based dictionary learning approach achieving the best accuracy and robustness. This study demonstrates the effectiveness of CIR-based authentication and its potential for enhancing wireless security.

Contents

Introduction

Mobile devices and wireless connectivity have become indispensable in various aspects of daily life, extending far beyond personal devices like smartphones. Modern households now include integrated lighting, heating systems, and appliances connected within home networks, while the automotive industry increasingly incorporates internet-connected vehicles that expand their functions and capabilities. This expansion is reflected in industries such as manufacturing, healthcare, and logistics, where IoT and wireless devices play a critical role in real-time data exchange and operational efficiency [40]. However, as the IoT enables seamless integration of devices, it introduces new security challenges, particularly in verifying the identity of communicating entities within these networks.

Authentication is essential to ensure that data is exchanged only between verified and legitimate devices, preventing malicious actors from accessing or manipulating sensitive information. Traditional methods of authentication, such as upper-layer cryptographic protocols, are commonly used. These methods impose significant computational overhead on IoT devices, which often have limited processing power and memory, making them unsuitable for many IoT environments [18]. In resource-constrained IoT systems designed to be low-cost and energy-efficient, complex cryptographic algorithms become impractical. Furthermore, the advent of quantum computing threatens to undermine traditional cryptographic methods by exploiting vulnerabilities in key-based systems, potentially compromising even the most advanced protocols [30].

Therefore, there is a pressing need for new methods of authenticating devices in wireless communication systems that are both computationally efficient and robust against future threats, especially in resource-constrained and large-scale environments [32]. One promising approach involves leveraging physical layer properties, such as PLA, to authenticate devices based on the unique characteristics of their communication channels without relying on complex key exchanges or computationally intensive encryption algorithms [28]. PLA offers a lightweight, scalable alternative to traditional cryptographic methods, providing effective security without the overhead of managing cryptographic keys, making it well-suited for IoT and other distributed wireless systems.

PLA can be broadly classified into two categories: *Active* and *Passive* [32]. Active PLA modifies the transmitted signal by embedding authentication tags, which is effective against impersonation but may alert adversaries to the presence of security measures. In contrast, Passive PLA operates without altering the signal, leveraging inherent channel characteristics to authenticate devices. This offers a more covert form of security, aligning well with environments where resources are constrained and discretion is essential.

Within Passive PLA, channel-based authentication techniques utilize characteristics of the communication channel such as the CIR to distinguish between legitimate and illegitimate transmitters. CIR-based authentication holds particular promise due to its ability to leverage the unique propagation environment of the wireless channel, providing a robust method of authentication even in complex environments [38]. This thesis seeks to explore an alternative approach to wireless communication security by leveraging the physical layer property called CIR for authentication purposes, investigating its effectiveness in providing secure, reliable, and lightweight authentication for wireless communication systems.

Research Objectives

The primary research question guiding this study is:

How can CIR be utilized for effective authentication in wireless communication systems to enhance security and reliability?

To tackle this issue, this research aims to:

- Examine and evaluate existing literature on CIR-based authentication techniques.
- Develop a framework for channel authentication that utilizes CIR measurements to identify legitimate transmitters.
- Evaluate the performance of the proposed CIR-based methods using various classification techniques and compare them against the reference paper to assess improvements in accuracy, robustness, and computational efficiency.
- Identify and address potential obstacles while applying the proposed PLA techniques.

To support these objectives, the thesis is organized as follows:
In Chapter 2, the background of wireless authentication is established, detailing the limitations of traditional methods and introducing the concepts of PLA and CIR. Chapter 3 reviews related literature, contrasting Received Signal Strength (RSS)-based, CIR-based, and machine learning approaches. In Chapter 4, the proposed methodologies including the PCA-SVM, SRC, PCA-SRC, and Sparse-DL-SVM techniques are described in detail. Chapter 5 outlines the experimental setup, dataset, and evaluation metrics, followed by a performance analysis of each method. Finally, Chapters 6 and 7 discuss the findings, address challenges, and conclude the study with insights and suggestions for future work.

Background Information

In this section, the limitations of traditional Upper Layer Authentication (ULA) methods in wireless communication are discussed, followed by an introduction to PLA and its advantages. We then delve into the distinctions between *Active* and *Passive* PLA, highlighting the benefits of Passive PLA for resource-constrained environments. Finally, we explore the concept of CIR, its underlying principles, and its specific application as a robust feature for authentication in wireless systems. This foundational overview establishes the context and rationale for using CIR-based Passive PLA, setting the stage for the methodologies and analyses that follow.

2.1 Limitations of Traditional Authentication Methods

In the context of modern wireless communication, especially within the IoT, reliable and efficient authentication is a crucial requirement. However, traditional methods based on ULA present significant limitations. Given the limited computational and energy resources of many IoT devices, cryptographic methods, which require substantial computational resources for secure key management and encryption, are often impractical [25]. Moreover, the increasing capabilities of quantum computing pose a significant threat to conventional cryptographic methods, potentially compromising their security in the near future [35]. Consequently, alternative methods are necessary to ensure secure authentication in IoT and other wireless communication networks.

2.2 Physical Layer Authentication (PLA)

PLA has emerged as a promising solution to these challenges. Unlike ULA, which relies on computationally intensive cryptographic operations, PLA leverages the unique characteristics of the wireless channel itself to verify the identity of communicating devices [24]. The idea of using physical layer attributes for authentication was introduced in a 2009 study [12]

by *Liang Xiao* and his colleagues. They proposed a system that employs channel probing and hypothesis testing to identify legitimate users while detecting intruders. Their study confirmed the practicality of this approach in static multipath environments, achieving dependable performance.

PLA offers a lightweight and scalable approach, making it particularly suitable for resource-constrained environments. PLA can operate efficiently in environments with diverse devices and supports seamless integration, as it does not impose significant communication overhead or processing requirements. PLA techniques are generally divided into two main categories: *Active PLA* and *Passive PLA*.

Active PLA

In Active PLA, the transmitter embeds an authentication tag within the source message. This tag is typically generated based on a shared secret key between the transmitter and receiver [32], enabling the receiver to verify the authenticity of the sender. The Active PLA generally consists of two stages: *a key-establishment stage* and *a message-transmission stage* [32].

Algorithm: Active PLA [32]

Key-establishment stage:

1: Alice requests communication with Bob.
2: Bob receives the request.
3: Bob verifies the request. If valid, a shared secret key is created using a key establishment protocol; otherwise, the request is ignored.
4: Bob sends an ACK to Alice for message preparation.

Message Transmission Phase:

1: Alice creates a tag using the secret key and embeds it in the message. She then sends the tagged message to Bob.
2: Bob receives the tagged message.
3: Bob regenerates the tag using the secret key and checks for its presence in the message. If it matches, the message is accepted and decoded; otherwise, it is rejected.

While Active PLA is robust against direct impersonation attacks, it has certain limitations. Embedding a tag can make the signal more detectable to adversaries, which could compromise the security and covertness of the communication in certain scenarios.

Passive PLA

In contrast, Passive PLA does not modify the original signal. Instead, it relies on intrinsic characteristics of the signal, such as the signal's physical layer attributes, to authenticate the transmitter. The Passive PLA generally consists of two stages: *a training stage* and *a message-transmission stage*[32].

This approach is advantageous in scenarios where covert operation is essential, as it does not introduce any detectable changes to the signal.

Algorithm: Passive PLA [32]

Training stage:

1: Alice requests communication with Bob over the wireless channel.
2: Bob receives the request at time t_1.
3: Bob authenticates the request; if valid, physical-layer features are extracted to build a whitelist. Otherwise, the request is ignored.
4: Bob sends an ACK to Alice for message preparation.

Message-transmission stage:

1: Alice sends a valid message using the same channel.
2: Bob receives a signal from an unknown source at time t_2.
3: Bob compares extracted features with the whitelist. If they match, the signal is accepted; if not, it is rejected.

And additionally, Passive PLA is computationally efficient and imposes minimal overhead, making it well-suited for IoT devices and other resource-constrained applications.

Given these benefits, Passive PLA was chosen as the focus of this study, particularly due to its efficiency, covert nature, and suitability for environments where low power consumption and computational simplicity are essential.

2.3 Channel-Based Authentication in Passive PLA

Passive PLA can further be divided into subcategories based on the features it utilizes. In this thesis, Channel-Based Authentication is selected due to its ability to leverage the unique and unrepeatable characteristics of the communication channel. These channel-based features are strongly influenced by the surrounding environment, enabling effective differentiation between legitimate and illegitimate devices. Unlike device-based features, which may be influenced by hardware conditions over time, channel-based features are inherently dynamic and less susceptible to hardware variability [32].

One of the most powerful channel-based features for Passive PLA is the **Channel Impulse Response** (CIR).

2.4 Channel Impulse Response (CIR)

CIR describes the propagation of a wireless signal from the transmitter to the receiver through the communication channel [27]. It captures the unique effects of the environment on the signal, including reflections, diffractions, and scattering from objects in the vicinity (see Figure 2.1). These effects create a distinct signature for the channel, which can be used to authenticate a device based on its physical environment.

By applying a known signal to the wireless communication system, the resulting received signal can be used to estimate the CIR. This is achieved by subtracting the known input signal

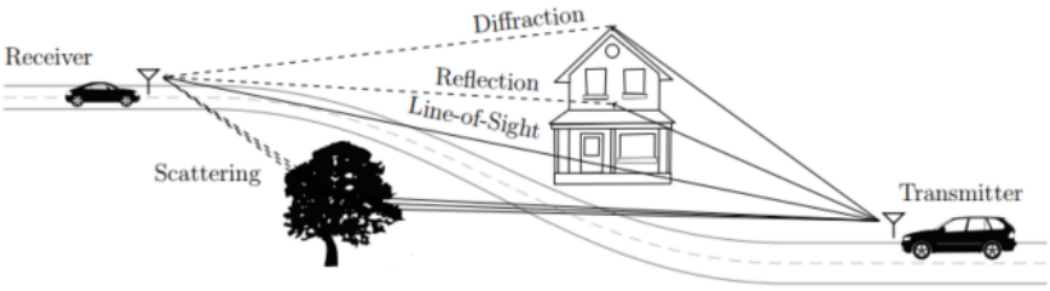

Figure 2.1: Overview of an Impulse in a Wireless Channel [27]

from the received output. The estimated channel impulse response $h(t)$ can be represented as:

$$h(t) = \sum_{n=0}^{N} \alpha_n e^{j\phi_n} \delta(t - \tau_n) \tag{2.1}$$

This formulation assumes a time-invariant channel, implying that the number of multipath components (N), as well as their respective amplitudes (α_n), phases (ϕ_n), and delays (τ_n), remain constant over time [36].

2.5 Application of CIR in Authentication

CIR is particularly useful in environments with rich multipath propagation, where multiple signal reflections from various surfaces create unique patterns in the received signal. These patterns are challenging for adversaries to replicate, making CIR an effective feature for authentication. In a typical CIR-based authentication process, the receiver compares the observed CIR of an incoming signal to a stored profile associated with a legitimate transmitter. If the CIR matches, the signal is considered authentic; otherwise, it is rejected [22].

In this research, CIR is used as the primary feature for authentication within the Passive PLA framework. This choice is motivated by CIR's inherent resilience to environmental changes, as it reflects the unique multipath characteristics that are difficult for adversaries to duplicate. CIR is sampled and processed to extract relevant features, which serve as the basis for classification and authentication, ultimately enhancing the security of wireless communication systems.

2.6 System Model

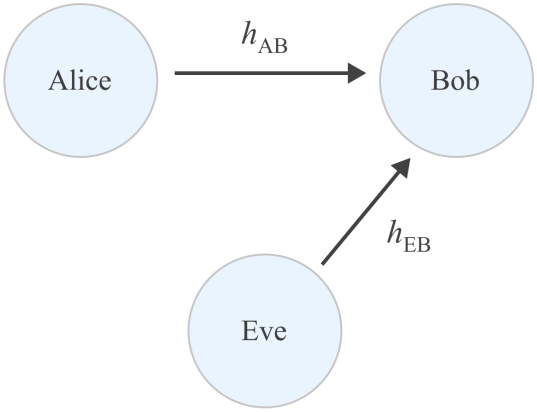

Figure 2.2: System and Attack Model

The system model in this thesis involves three key participants: Alice (A), Bob (B), and Eve (E). Alice and Bob represent legitimate communication partners, while Eve acts as an adversary attempting to compromise the communication link. Alice transmits signals to Bob over a legitimate wireless channel, which is characterized by the CIR h_{AB}. This CIR uniquely represents the physical properties of the communication path between Alice and Bob, making it a useful feature for authentication. Unlike traditional passive eavesdropping scenarios, Eve in this model also transmits signals to Bob, creating a separate channel h_{EB}. Since Eve does not share Alice's exact location or propagation environment, the channel h_{EB} differs from h_{AB} in terms of multipath characteristics, fading behavior, and spatial dependencies. This distinction ensures that Eve cannot accurately replicate h_{AB}, which is fundamental to securing physical layer authentication. By leveraging these unique physical-layer properties of the wireless channel, Alice and Bob can establish a secure and authenticated communication link, ensuring robustness against impersonation attacks and unauthorized access attempts by Eve.

Related Works

Passive PLA methods can be categorized into two main types: *Statistical channel information* and *Instantaneous channel information*. *Statistical channel information* is primarily determined by path loss and shadowing effects, providing a coarse-grained overview of the wireless channel (e.g., RSS). Conversely, *Instantaneous channel information* is affected by path loss, shadowing, and small-scale fading, providing fine-grained insights into the channel's state (e.g., CIR). While statistical features are easier to extract from received signals, they offer less detailed information compared to instantaneous features, which, despite being more informative, are more complex to obtain.

In this chapter, we group related works into three categories based on the primary features or methods they use for PLA: (1) **RSS-based**, (2) **CIR-based**, and (3) **CIR-based ML** approaches.

3.1 RSS-based approaches

Several studies have focused on using **RSS** as a statistical feature for detecting *spoofing attacks*. *Spoofing attacks* involve an adversary masquerading as a legitimate device by falsifying data, thereby gaining unauthorized access to systems[43].

Chen *et al.* explore how to spot spoofing attacks in wireless networks without relying on traditional cryptographic methods [14]. Instead, they focus on using RSS as a physical layer feature, which can capture unique patterns in signal behavior. Their solution uses K-means clustering to identify unusual changes in these patterns, even when an attacker tries to confuse the system by changing their transmission power. The authors also built a real-time system that helps pinpoint the location of these attacks, reporting impressive results with a high success rate and minimal false alarms in tests on Wireless Fidelity (Wifi) and ZigBee networks. On the downside, this approach depends heavily on the stability of RSS, which can be tricky in environments with significant interference or multipath issues where signals bounce unpredictably. The method also assumes that network devices stay in one place, which might limit its use in scenarios where devices are moving. While their technique

seems promising, they didn't fully compare it against other modern methods, leaving some questions about its performance in broader contexts.

Building on the use of RSS, Liang Xiao *et al.* introduce a method [21] to detect spoofing attacks in wireless networks using Received Signal Strength Indicators (RSSI), focusing on physical-layer authentication. They employ a reinforcement learning approach, specifically Q-learning, to dynamically adjust the threshold for a binary hypothesis test that distinguishes legitimate packets from spoofed ones. By framing the problem as a zero-sum game between the receiver and the attacker, they optimize the test threshold based on Bayesian risk to maximize detection accuracy [20]. Implemented on Universal Software Radio Peripherals (USRP), the method showed improved detection performance compared to fixed-threshold strategies. However, the reliance on RSSI, which can be influenced by environmental noise and multipath effects, may limit the robustness of the method. Additionally, the convergence time of the Q-learning algorithm might hinder its real-time applicability in rapidly changing environments.

Further extending this line of research, Xiao *et al.* propose a method [20] for PHY-layer spoofing detection using a reinforcement learning approach tailored for wireless networks. They utilize RSSI and Channel Frequency Responses (CFR) as key features to identify spoofing attempts [41]. The method frames the problem as a zero-sum game [20] between the receiver and the spoofers, where the receiver adjusts its detection threshold using Q-learning and Dyna-Q techniques. This dynamic approach allows the system to learn and adapt in real time, even without prior knowledge of channel conditions. Experimental evaluations conducted using USRP devices in indoor environments demonstrate that the proposed methods yield improved detection rates and reduced false alarm occurrences compared to conventional fixed-threshold approaches. However, the method's reliance on RSSI can be problematic in environments with significant multipath interference, and the convergence time of Q-learning may hinder its practical use in highly dynamic scenarios.

3.2 CIR-based approaches

In contrast to purely statistical methods based on RSS, other works leverage fine-grained instantaneous channel information such as CIR. Tugnait and Kim propose a channel-based hypothesis testing method [15] for user authentication in wireless networks, utilizing the unique Channel State Information (CSI) as a distinguishing characteristic. Their method formulates two hypothesis tests: one based on comparing the time-domain CSI of the current and previous transmissions, and another using whiteness testing of residuals generated from the estimated channel. By comparing the CSI estimates, the approach effectively identifies discrepancies caused by spoofing attempts. Simulations show that the proposed methods achieve strong detection rates, particularly with the CSI comparison outperforming the residual whiteness test. However, the reliance on time-invariant channel assumptions can be problematic in rapidly changing environments, and the method's sensitivity to noise may affect its robustness. The evaluation could have been enhanced with more extensive comparisons against alternative physical-layer authentication techniques.

Liu *et al.* present a robust method [17] for physical-layer authentication using the inherent properties of the CIR. The approach involves monitoring variations in CIR between consecutive transmissions to identify spoofing attempts, leveraging a hypothesis testing framework. To reduce noise impact, the authors introduce an Signal-to-noise ratio (SNR)-dependent threshold that adapts based on the observed CIR differences [17]. This adaptive method is implemented in an Orthogonal Frequency Division Multiplexing (OFDM) system and validated through simulations, showing high detection rates with low false alarms. However, the reliance on accurate CIR estimation in noisy environments and the assumption of a stationary channel could limit its effectiveness in highly dynamic scenarios. Additionally, the paper would benefit from a broader evaluation against other existing physical-layer authentication techniques.

3.3 CIR-based Machine learning approaches

While some methods rely solely on the statistical properties of the wireless channel or basic feature comparisons, an emerging trend incorporates Machine Learning (ML) to better utilize the fine-grained CIR/CSI data.

Wang *et al*. propose a novel approach [23] for physical-layer authentication using an Extreme Learning Machine (ELM), a type of feedforward neural network. The method leverages the multi-dimensional features of the radio channel, including Euclidean distance and Pearson correlation coefficients, to enhance the identification of spoofing attacks [29]. The authors introduce a pseudo-adversary model to generate training data, addressing the challenge of obtaining labeled data in real-world scenarios. The ELM's fast learning capability allows for efficient and accurate detection without requiring iterative training, making it suitable for low-complexity environments. Simulation results demonstrate significant improvements in detection accuracy compared to traditional threshold-based methods. However, the reliance on accurate feature extraction and the pseudo-adversary model's assumptions may affect performance in highly dynamic and noisy environments. The study could be strengthened with more real-world tests and comparisons against other machine learning techniques.

Similarly, Yoon *et al*. propose a machine learning-based PLA scheme [26] for Multiple-Input Multiple-Output (MIMO) wireless communication, leveraging Neighborhood Component Analysis (NCA) for feature selection. The method focuses on reducing high-dimensional CSI features by selecting the most discriminative ones to distinguish between legitimate users and attackers. An Radial Basis Function (RBF) kernel-based SVM is used for classification, achieving high performance by training on optimized features. The scheme demonstrates strong authentication results across 24 test scenarios, achieving an average Area Under The Curve (AUC) score of 0.9965, even under worst-case conditions where an attacker closely mimics legitimate signals[26]. However, the reliance on accurate feature extraction and the static channel assumptions may limit its applicability in dynamic environments. The study could benefit from more extensive real-world testing and comparisons with other feature selection methods to validate its robustness.

Beyond these, Abdrabou and Gulliver propose an adaptive physical layer authentication scheme [33] using machine learning and antenna diversity for 5G networks. The method utilizes a One-Class Classifier Support Vector Machine (OCC-SVM), leveraging the magnitude and real and imaginary parts of the received signal as features extracted from the Sounding Reference Signal (SRS) in the 5G uplink frame [33]. By incorporating antenna diversity, the approach increases the number of features, significantly boosting the authentication rate. The evaluation in urban scenarios demonstrated a high authentication rate exceeding 99.9 with multiple antennas, even under varying mobility conditions [33]. However, the reliance on accurate feature extraction from SRS signals may limit its performance in environments with severe interference. Additionally, the diversity combining techniques tested showed mixed results, occasionally degrading the classification performance due to reduced feature distinctiveness. The study could benefit from broader real-world testing and comparisons with deep learning-based methods to validate the practical advantages of the proposed scheme.

Methodology

This chapter outlines the methods developed for PLA based on CIR data. The first method utilizes PCA with Singular Value Decomposition (SVD) for dimensionality reduction, followed by classification using an SVM. The second method employs a sparse preprocessing technique, classifying signals based on residual calculations to distinguish between legitimate and illegitimate transmitters. The third method combines PCA preprocessing with the same sparse classifier used in method SRC to improve classification accuracy. Finally, the fourth method leverages Lasso-based dictionary learning to extract sparse features, followed by classification using an SVM, providing an optimized balance between feature selection and classification performance. Each method is explained in detail, highlighting its preprocessing steps, feature extraction, and classification approach.

4.0.1 Dimensionality Reduction

The dataset with high-dimensional data often contains redundant and correlated features, which can negatively impact classification efficiency and model performance. In this study, dimensionality reduction is applied as to remove redundancy, improve computational efficiency, and enhance classification accuracy in PLA.

Figure 4.1 shows a CIR signal and in figure 4.2 shows the patterns that indicate the redundant information of a CIR. This redundancy suggests that the dataset contains correlated features, which can be reduced without significant information loss.

To address this redundancy, two different dimensionality reduction techniques were employed across different methods:

- Principal Component Analysis (PCA): PCA is applied in one method to transform CIR data by projecting it onto principal components that capture the most variance. This ensures that the most informative variations in the data are retained while eliminating redundant features. PCA is particularly effective for datasets where correlation among features is high.

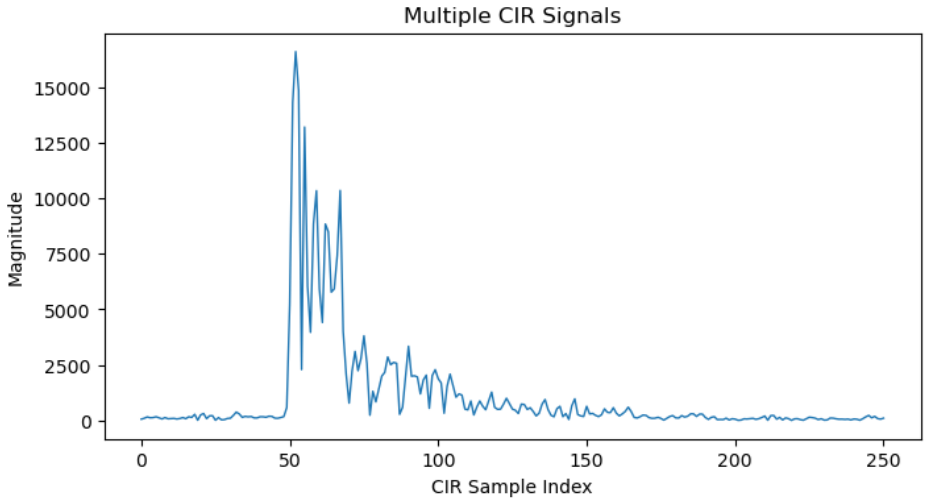

Figure 4.1: A Single CIR Signal

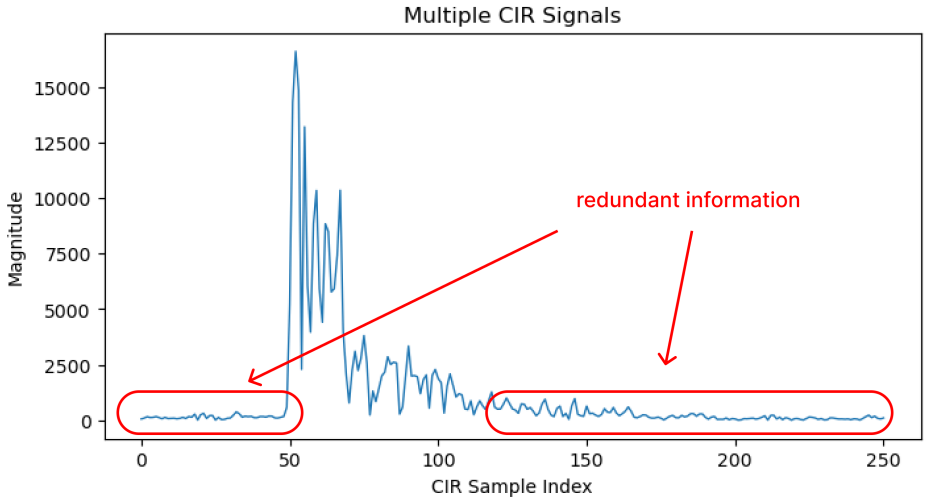

Figure 4.2: Demonstrates the Redundant Information of a CIR

- Sparse Representation via Dictionary Learning: In another method, we use sparse representation to achieve dimensionality reduction. Specifically, we apply dictionary learning to extract a set of basis functions (or atoms) from the data. Each CIR sample is then represented as a sparse linear combination of these learned atoms. The resulting sparse codes are typically much lower in dimensionality compared to the original data, capturing only the most discriminative features essential for classification. This method not only reduces dimensionality but also improves interpretability and enhances classification performance.

4.0.2 Initial Data Preprocessing

In our research, we conducted several initial preprocessing steps prior to applying dimensionality reduction techniques. Initially, the dataset was partitioned into three

subsets: training, testing, and evaluation. Subsequently, for each CIR signal, we computed the magnitude from its real and imaginary components. This process involved forming magnitude vectors corresponding to both legitimate and illegitimate CIRs. The data was then appropriately labeled and organized. These preprocessing steps are elaborated upon in the subsequent sections.

Dataset Splitting

To ensure a fair and unbiased evaluation of the method, the dataset is divided into three subsets:

- **Training Set (X_{train})**: Used to train the SVM classifier.
- **Testing Set (X_{test})**: Used to validate model performance on unseen data.
- **Evaluation Set (X_{eval})**: Used to compute final classification metrics such as Accuracy, FAR, MDR, and AR.

Data Representation

The dataset we have, has N channel observations, each containing measurements across several samples of the channel (e.g., 251 samples). Each sample is complex $h(t)$, composed of real and imaginary parts:

$$h(t) = h_{\text{real}}(t) + j \cdot h_{\text{imag}}(t), \quad t = 1, 2, \ldots, D \tag{4.1}$$

where $h_{\text{real}}(t)$ is the real part of the CIR, $h_{\text{imag}}(t)$ is the imaginary part of the CIR, and j is the imaginary unit ($j^2 = -1$) that is used to combine the real and imaginary parts into a single complex number, and D is the number of samples in each CIR (for instance, $D = 251$).

In this stage of preprocessing, we perform two key steps: first, we compute the magnitude of the signals, and second, we stack the feature vectors before assigning the corresponding labels.

Magnitude Computation

Each observation's complex CIR is first converted into a magnitude vector. For a single sample $h(t)$, the magnitude is:

$$|h(t)| = \sqrt{(h_{\text{real}}(t))^2 + (h_{\text{imag}}(t))^2} \tag{4.2}$$

This step consolidates each sample's real and imaginary parts into one non-negative real value, reflecting the signal strength at sample t. Hence, for each CIR with D samples, we obtain a real-valued vector of length D.

Stacking and Labeling

After computing the magnitude vectors, we stack all legitimate CIRs (Alice) into one group and all illegitimate CIRs (Eve) into another. Each sample is now of the form:

$$\mathbf{x}_i = (|h(1)|, |h(2)|, \ldots, |h(D)|), \quad x_i \in \mathbb{R}^F. \tag{4.3}$$

Here, $\mathbb{R}^F$ means a F-dimensional vector where each element is a real number. Thus, our dataset looks like:

$$\{(x_1, y_1), (x_2, y_2), \ldots, (x_N, y_N)\}, \quad x_i \in \mathbb{R}^F, \quad y_i \in \{0, 1\}. \tag{4.4}$$

where $y_i = 0$ (legitimate) or $y_i = 1$ (illegitimate).

These are the initial preprocessing steps which we have performed across all the methods we've proposed.

4.1 Method: Principle Component Analysis with Support Vector Machine Classification (PCA-SVM)

This method aims to classify CIR data by first simplifying its representation through dimensionality reduction and then applying a machine learning algorithm for accurate classification. PCA is employed to transform the high-dimensional CIR data into a lower-dimensional representation while retaining the most significant variance. It was originally introduced by *Pearson* [1] and later developed in its modern form by *Hotelling* [2]. After reducing the feature space, SVM is applied to classify the reduced data efficiently, distinguishing between legitimate and illegitimate signals. SVM first introduced by *Vapnik* and *Chervonenkis* [4] and later formalized by *Cortes* and *Vapnik* [7]. The method is explained below in each subsection.

4.1.1 Data Preprocessing

Prior to implementing the subsequent steps, we conducted some initial preprocessing steps. See the section Data preprocessing for further details.

Standardization

To ensure that all features contribute equally to the classification process, each dataset (eg. training, testing, and evaluation) is standardized before applying PCA. Standardization transforms each dimension (i.e., each of the D samples) to have zero mean and unit variance across the data, preventing any single feature from dominating the model due to its scale:

$$\mathbf{z}_i = \frac{\mathbf{x}_i - \mu}{\sigma}, \tag{4.5}$$

where $\boldsymbol{\mu}$ and $\boldsymbol{\sigma}$ are the mean and standard deviation vectors of the dataset.

After the training dataset is scaled, we use PCA to reduce the dimension of our high-dimensional dataset.

Why PCA for dimensionality reduction?

PCA is widely used for reducing the number of features in high-dimensional datasets while preserving their most important variations. It identifies and retains the most informative variations in the dataset and it ensures that the essential signal characteristics are preserved while eliminating redundant information. Compared to other non-linear techniques such as t-distributed Stochastic Neighbor Embedding (t-SNE) or Uniform Manifold Approximation and Projection (UMAP), PCA is computationally fast and less expensive. Unlike Linear Discriminant

Analysis (LDA), which requires class labels, PCA is unsupervised and does not rely on predefined categories. This makes it more generalizable to different datasets without requiring additional labeled data. PCA is also easier to implement than Sparce Coding and Dictionary Learning.

In practical implementations, PCA is often computed using SVD, a mathematical technique formally developed by *Eckart* and *Young* for matrix approximation [3].

Principle Component Analysis (PCA) using Singular value decomposition (SVD)

Each vector $\mathbf{x}_i \in \mathbb{R}^F$, where x_i is a data sample represented as a vector of F features (dimensions), $\mathbb{R}^F$ is the F-dimensional space of real numbers, and F denotes the number of features or dimension in the dataset. Many dimensions in $\mathbf{x}_i$ may be noisy or redundant. PCA is used to reduce the number of dimensions while preserving the main variance in the data. This helps to make the data easier to analyze and improves computational efficiency [3].

Singular Value Decomposition (SVD)

We form a data matrix $\mathbf{Z} \in \mathbb{R}^{N_{\text{train}} \times F}$, where each row is a standardized sample $\mathbf{z}_i^\top$. PCA can be obtained by taking the SVD of $\mathbf{Z}$ [3]:

$$\mathbf{Z} = \mathbf{U}\,\mathbf{\Sigma}\,\mathbf{V}^\top, \tag{4.6}$$

where

- $\mathbf{U}$ is an $(N_{\text{train}} \times F)$ matrix with orthonormal columns.
- $\mathbf{\Sigma}$ is a diagonal matrix whose entries $\sigma_1 \geq \sigma_2 \geq \cdots \geq 0$ are the singular values.
- $\mathbf{V}$ is a $(F \times F)$ matrix whose columns (the right-singular vectors) are orthonormal directions of maximal variance.

Principal Components

The columns of $\mathbf{V}$ (the right-singular vectors) represent the principal components in the original feature space. By selecting the top n_{comp} columns of $\mathbf{V}$, a projection matrix $\mathbf{P}$ is obtained. The singular vectors associated with the highest singular values encapsulate the most variance in the data, rendering them the most informative for dimensionality reduction.

For this method, we experimented with different values of n_{comp}, ranging from 2 to 6, to analyze the impact of dimensionality reduction on classification performance. Thus, the projection matrix is given by:

$$P = [v_1, v_2, \ldots, v_{n_{\text{comp}}}] \tag{4.7}$$

where $v_1, v_2, \ldots, v_{n_{\text{comp}}}$ are the right-singular vectors, corresponding to the largest singular values $\sigma_1, \sigma_2, \ldots, \sigma_{n_{\text{comp}}}$.

Projection

Each standardized sample $\mathbf{z}_i$ is then projected onto these principal components:

$$\mathbf{z}'_i = \mathbf{z}_i \mathbf{P}. \tag{4.8}$$

Here, $\mathbf{z}_i$ is a row vector, and $\mathbf{P}$ is a matrix whose columns are the principal directions.

4.1.2 Model Training

After dimensionality reduction, each sample is represented by only a few principal components. We then train a SVM model to distinguish legitimate (Alice) from illegitimate (Eve) samples [4] [7]. Below subsections explain it in details.

SVM Model

SVM is a discriminative classifier that finds the optimal hyperplane separating two classes in a transformed feature space. Given a training set of labeled samples $(\mathbf{z}'_i, y_i)$, SVM determines a decision boundary that maximizes the margin between the classes [7]. In high-dimensional spaces, SVM effectively identifies a linear decision boundary. However, when the data is not linearly separable, a kernel function is utilized to map the input space into a higher-dimensional space where linear separation becomes feasible. For this purpose, we adopt an RBF kernel, allowing SVM to capture non-linear patterns in the CIR data, thereby making it well-suited for wireless channel authentication tasks.

Training the SVM Classifier

During training, the SVM is provided with the PCA transformed feature vectors $\mathbf{z}'_i$ along with their corresponding labels y_i. SVM solves a constrained optimization problem to maximize the margin between the two classes [7]. The RBF kernel is applied to map the input data into a higher-dimensional space, enabling effective classification of CIR signals with complex decision boundaries.

4.1.3 Testing and Classification

Once the SVM model is trained, new CIR samples undergo the same preprocessing steps. They are standardized using the mean and standard deviation from the training set. Then, the standardized features are projected onto the PCA transformation matrix P to maintain consistency. Finally, the transformed features are classified by the trained SVM, which predicts whether a sample belongs to Alice (label = 0) or Eve (label = 1) based on the decision boundary.

Algorithm of *Method PCA-SVM*

1: **Train-Test Split:** Split dataset into training (X_{train}), testing (X_{test}), and evaluation (X_{eval}) sets.
2: **Data Preprocessing:** Extract CIR magnitudes from X_{train} and stack into dataset (X_{train}, y_{train})
3: **Standardization:** Normalize features to have zero mean and unit variance
4: **Dimensionality Reduction:**
5: Compute PCA using SVD: $\mathbf{Z} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T$
6: Select top n_{comp} principal components to form projection matrix $\mathbf{P}$
7: Project data: $\mathbf{z'}_i = \mathbf{z}_i\mathbf{P}$
8: **Train SVM:** Fit SVM classifier using projected training data
9: **Testing:** Transform and classify X_{test} using trained SVM.
10: **Evaluation:** Compute classification metrics (Accuracy, FAR, MDR, AR) on X_{eval}.

The evaluation dataset is used to evaluate the model and this dataset is also preprocessed the same way as the testing dataset. Evaluation of this method and the comparison with the reference paper, are briefly explained in the evaluation chapter.

4.2 Method: Sparse Residual Classifier (SRC)

This method classifies CIR signals using sparse representation-based classification, unlike Method PCA-SVM, which relies on PCA and SVM. It constructs a dictionary from training data and applies OMP to represent test samples as a sparse combination of dictionary elements. Classification is performed by computing reconstruction residuals, and assigning the test sample to the class with the smallest residual. The concept of sparse representation was first introduced by *Bruno A. Olshausen* and *David J. Field* in their paper [8] published in 1996.

In this section, we briefly explain the method we propose using sparse representation.

4.2.1 Data Preprocessing

Prior to implementing the subsequent steps, we conduct some preprocessing steps here. The CIR data is structured and preprocessed identically to ensure consistency across all methods. This setup allows us for a fair comparison of classification performance across different methods.

See the section *Data preprocessing* for further details.

4.2.2 Dictionary Formation

In this method, we directly form the dictionary $\mathbf{D}$ from the training data.
Let, $\mathbf{X} \in \mathbb{R}^{N_{\text{train}} \times F}$ represent all the training samples (each row is a CIR magnitude vector). The dictionary $\mathbf{D}$ is given by:

$$\mathbf{D} = \mathbf{X}^T \in \mathbb{R}^{F \times N_{\text{train}}}, \tag{4.9}$$

so that each column of $\mathbf{D}$ corresponds to one training sample. Since the training set contains samples from both Alice and Eve, $\mathbf{D}$ effectively combines all their representative magnitudes into a single matrix.

4.2.3 Sparse Coding with Orthogonal Matching Pursuit (OMP)

Orthogonal Matching Pursuit (OMP) is a greedy algorithm used to find sparse representations of signals in terms of an overcomplete dictionary. It was first introduced by *Mallat, S.G.* and *Zhifeng Zhang* in 1993 [5]. We are going to use it in this method to extract sparse representation.

In the context of sparse representation-based classification, given a test sample $\mathbf{x}_{\text{test}} \in \mathbb{R}^F$, we seek a sparse representation β such that:

$$\beta = \arg\min_{\beta} \|\mathbf{x}_{\text{test}} - \mathbf{D}\beta\|_2^2 \quad \text{subject to} \quad \|\beta\|_0 \leq K, \tag{4.10}$$

where $\|\cdot\|_0$ denotes the number of nonzero entries, and K is the maximum allowed number of nonzero coefficients (i.e.sparsity level) [19].

OMP algorithm finds an approximate solution efficiently by greedily selecting columns in $\mathbf{D}$ that best reduce the residual $\mathbf{x}_{\text{test}} - \mathbf{D}\beta$ at each step. This process continues until K atoms (columns) have been selected or the error reduction becomes negligible.

4.2.4 Testing and Classification

Once β is obtained, the overall reconstruction of $\mathbf{x}_{\text{test}}$ is simply:

$$\widehat{\mathbf{x}}_{\text{test}} = \mathbf{D}_c\beta_c. \tag{4.11}$$

However, for classification, we aim to measure how well $\mathbf{x}_{\text{test}}$ can be reconstructed using only the atoms corresponding to each class. Suppose $\mathbf{D}_0$ contains only the columns from Alice's training samples, and $\mathbf{D}_1$ those from Eve's training samples. We similarly define β_0 and β_1 by zeroing out the entries in β that do not belong to each respective class.

1. Residual for Alice (Class 0)
$$r_0 = \|\mathbf{x}_{\text{test}} - \mathbf{D}_0\beta_0\|_2 .$$
2. Residual for Eve (Class 1)
$$r_1 = \|\mathbf{x}_{\text{test}} - \mathbf{D}_1\beta_1\|_2 .$$

These two quantities, r_0 and r_1, represent the reconstruction errors when only dictionary atoms from Alice or Eve, respectively, are used.

Algorithm of *Method SRC*

1: **Train-Test Split:** Split dataset into training (X_{train}), testing (X_{test}), and evaluation (X_{eval}) sets.
2: **Data Preprocessing:** Extract CIR magnitudes from $X_{train}$and stack into dataset (X_{train}, y_{train})
3: **Dictionary Formation:** Construct dictionary $\mathbf{D}$ from training data.
4: **Sparse Representation:** Compute sparse coefficients $\boldsymbol{\beta}$ for each test sample x_{test} using OMP.
5: **Residual Computation:** Compute residuals $r_c = \|x_{\text{test}} - D_c\beta_c\|_2$ for each class $c \in \{0, 1\}$.
6: **Classification:** Assign class label based on minimum residual:

$$\hat{y} = \arg\min_{c \in \{0,1\}} r_c$$

7: **Evaluation:** Preprocess and classify X_{eval} using the trained model.
8: Compute classification metrics: Accuracy, FAR, MDR, AR.

Decision Rule

The final classification decision $\hat{y}$ assigns $\mathbf{x}_{\text{test}}$ to the class that yields the lowest reconstruction error:

$$\hat{y} = \arg\min_{c \in \{0,1\}} r_c. \tag{4.12}$$

Accordingly, if $\mathbf{x}_{\text{test}}$ is more accurately reconstructed by Alice's atoms, $\hat{y} = 0$; if it is better reconstructed by Eve's atoms, $\hat{y} = 1$.

The evaluation dataset is used to evaluate the model and this dataset is also preprocessed the same way as the testing dataset. Evaluation of this method and the comparison with the reference paper, are briefly explained in the evaluation chapter.

4.3 Method: Principal Component Analysis (PCA) with Sparse classifier (PCA-SRC)

This method extends the method SRC by incorporating dimensionality reduction before sparse coding. In the previous method SRC, no dimensionality reduction was applied, whereas in this method, PCA is applied to reduce the feature space before performing sparse representation-based classification. After PCA transformation, dictionary is formed, OMP extracts sparse coefficients, and classification is performed based on residual minimization. The following subsections detail each step.

4.3.1 Data Preprocessing

Prior to implementing the subsequent steps, we conducted some preprocessing steps. The CIR data is structured and preprocessed identically to ensure consistency across all methods.

See the section *Data preprocessing* for further details.

Additionally, we apply PCA for dimensionality reduction, following the same way we applied PCA outlined in method *PCA-SVM*.

4.3.2 Dictionary Formation and Sparse Coding

After preprocessing the CIR dataset, form the dictionary and set up the OMP algorithm which can extract sparse representation using the formed dictionary. This method leverages a sparse representation-based classification approach using OMP like method *SRC*. The classification is performed based on reconstruction residuals.

The first step is to construct a dictionary D using the PCA-transformed training data. Let the training set be:

$$X_{\text{train}} = \{z'_1, z'_2, \ldots, z'_{N_{\text{train}}}\} \tag{4.13}$$

where each z'_i is a PCA-reduced CIR sample obtained from the preprocessing step. The dictionary $\mathbf{D}$ is then formed by stacking all training samples together, ensuring that it contains both Alice's (legitimate) and Eve's (illegitimate) CIR signals.

To classify a new test sample, we represent it using a small number of dictionary elements instead of the entire dictionary. The OMP algorithm selects the most relevant features, ensuring a compact and efficient representation. This helps capture the essential characteristics of the CIR signal while reducing noise.

4.3.3 Testing and Classification

After training the model, the next step is to classify new CIR samples using the trained dictionary and assign labels based on reconstruction accuracy. The test dataset is preprocessed in the same way as the training dataset, ensuring consistency in feature extraction, standardization, and PCA transformation before classification.

Sparse Representation Using OMP

Each test sample is represented as a sparse combination of dictionary elements using the OMP algorithm. The goal is to approximate the test sample using only a small subset of dictionary atoms, ensuring efficient and accurate classification.

Residual-Based Classification

Once the sparse representation is obtained, the classification is performed using a residual-based decision rule:

1. The test sample is **reconstructed** using only the dictionary atoms corresponding to **Alice's** training data, and the reconstruction error (**residual**) is computed.
2. The same process is repeated using **Eve's** training data.
3. The test sample is assigned to the **class with the smallest residual**, meaning it is best represented by that class's dictionary atoms.

The final predicted label for a test sample z'_{test} is:

$$y = \arg \min_{c \in \{0,1\}} \|z'_{\text{test}} - D_c \beta_c\|_2 \tag{4.14}$$

where D_0 and D_1 are the dictionary components corresponding to **Alice (legitimate)** and **Eve (illegitimate)**, respectively.

Algorithm of *Method PCA-SRC*

1: **Train-Test Split:** Split dataset into training (X_{train}), testing (X_{test}), and evaluation (X_{eval}) sets.
2: **Data Preprocessing:** Extract CIR magnitudes from $X_{train}$and stack into dataset (X_{train}, y_{train})
3: **Standardization:** Normalize the dataset.
4: **Dimensionality Reduction:** Apply PCA to reduce the feature space.
5: **Dictionary Formation:** Construct dictionary $\mathbf{D}$ from PCA-transformed training data.
6: **Sparse Representation:** Compute sparse coefficients $\boldsymbol{\beta}$ for each test sample x_{test} using OMP.
7: **Residual Computation:** Compute residuals $r_c = \|x_{\text{test}} - D_c\beta_c\|_2$ for each class $c \in \{0, 1\}$.
8: **Classification:** Assign class label based on minimum residual:

$$\hat{y} = \arg\min_{c \in \{0,1\}} r_c$$

9: **Evaluation:** Preprocess and classify X_{eval} using the trained model.
10: Compute classification metrics: Accuracy, FAR, MDR, AR.

The evaluation dataset is used to evaluate the model and this dataset is also preprocessed the same way as the testing dataset. Evaluation of this method and the comparison with the reference paper, are briefly explained in the evaluation chapter.

4.4 Method: Sparse Dictionary Learning with Support Vector Machine (SVM) (Sparse-DL-SVM)

This method leverages Lasso-based dictionary learning to extract sparse features from CIR signals and then employs SVM for classification. In contrast to method *SRC* and method *PCA-SRC*, which uses OMP to obtain sparse representations, the current approach uses Lasso Least Angle Regression (Lasso-LARS). This alternative method enforces an L1 penalty for feature selection and often provides more stable or interpretable coefficients, particularly when there are correlations among features.

4.4.1 Data Preprocessing

Prior to implementing the subsequent steps, we conducted the same preprocessing steps we did for the previous two methods. The CIR data is structured and preprocessed identically to ensure consistency across all methods.

See the section *Data preprocessing* for more details.

Dictionary Learning for Sparse Feature Extraction

Dictionary learning serves our goal in this method for sparse feature extraction and also the dimension reduction of the dataset. It was first introduced by *Mairal*, *Julien* and *Bach* in 2009 [13]. In this method, we learn a dictionary $\mathbf{D} \in \mathbb{R}^{F \times K}$ from the training data $\mathbf{X} \in \mathbb{R}^{N_{\text{train}} \times F}$ by solving the following optimization problem [32]:

$$\min_{\mathbf{D}, \{\boldsymbol{\alpha}_i\}} \sum_{i=1}^{N_{\text{train}}} \left(\|\mathbf{x}_i - \mathbf{D}\boldsymbol{\alpha}_i\|_2^2 + \lambda \|\boldsymbol{\alpha}_i\|_1 \right)$$

where:

- K is the number of dictionary atoms (set by the parameter $n\_components$, which is experimentally tested for different values (e.g., 5, 10, 15, 20) to find the best-performing model.)
- $\boldsymbol{\alpha}_i \in \mathbb{R}^K$ denotes the sparse representation of the i-th training sample, and
- λ serves as a regularization parameter that balances reconstruction accuracy and sparsity.

Unlike method SRC, where the dictionary was directly formed as $\mathbf{D} = \mathbf{X}^T$, here the dictionary is learned iteratively using a Lasso-based approach (specifically, Lasso-LARS)[9][11][10]. This procedure not only yields a compact dictionary but also provides sparse representations that capture the essential features of the CIR signals.

Lasso-Based Dictionary Learning

The optimization described above is carried out using a Lasso-LARS algorithm [9][11], which is well-suited for high-dimensional data where features may be correlated. The algorithm minimizes the reconstruction error while enforcing sparsity via an L1 penalty [9]. Once the dictionary $\mathbf{D}$ is learned from the training data, new (test) samples can be encoded into sparse feature vectors by solving:

$$\boldsymbol{\alpha}_{\text{test}} = \arg\min_{\boldsymbol{\alpha}} \left(\|\mathbf{x}_{\text{test}} - \mathbf{D}\boldsymbol{\alpha}\|_2^2 + \lambda \|\boldsymbol{\alpha}\|_1 \right),$$

with $\mathbf{D}$ held fixed.

Why Lasso-LARS?

Because of its automatic feature selection ability and its handling of correlated features, Lasso can set some coefficients to zero, effectively selecting the most informative components. In addition, Lasso-LARS provides robust performance when dictionary atoms exhibit interdependencies, making it a suitable choice for extracting sparse representations from CIR signals [9][11].

Standardization and Feature Scaling

Many machine learning models, including SVMs, are sensitive to the scale of input features. Therefore, after obtaining the sparse representations $\boldsymbol{\alpha}_i$, each dimension is standardized:

$$\tilde{\boldsymbol{\alpha}}_i = \frac{\boldsymbol{\alpha}_i - \mu}{\sigma},$$

where μ and σ denote the mean and standard deviation computed across the dataset set for each feature, respectively [37]. We do this scaling for each of the datasets - training, testing, and evaluation.

4.4.2 Model training

After dictionary learning and sparse feature extraction, we train an SVM model to distinguish between Alice's signals and Eve's signals based on their sparse codes.

Training the SVM Classifier

Let $\tilde{\boldsymbol{\alpha}}_i$ denote the standardized sparse representation for the i-th sample and let $y_i \in \{0, 1\}$ be its corresponding label. The SVM seeks a decision boundary in the sparse feature space $\mathbb{R}^K$ [6]:

$$f(\tilde{\boldsymbol{\alpha}}) = w^T \tilde{\boldsymbol{\alpha}} + b,$$

where $w \in \mathbb{R}^K$ is the weight vector and $b \in \mathbb{R}$ is the bias term. The classifier is trained to maximize the margin between samples labeled $y = 0$ (Alice) and $y = 1$ (Eve) using an RBF kernel [16]:

$$\kappa(\mathbf{u}, \mathbf{v}) = \exp\left(-\gamma \|\mathbf{u} - \mathbf{v}\|^2\right).$$

4.4.3 Testing and Classification

When a new test sample $\mathbf{x}_{\text{test}}$ is presented, the following steps are performed:

1. **Sparse Representation via Lasso:** The test sample is encoded using the learned dictionary:
$$\boldsymbol{\alpha}_{\text{test}} = \arg\min_{\boldsymbol{\alpha}} \left(\|\mathbf{x}_{\text{test}} - \mathbf{D}\boldsymbol{\alpha}\|_2^2 + \lambda \|\boldsymbol{\alpha}\|_1\right).$$
2. **Standardization:** The sparse code is then standardized using the mean μ and standard deviation σ from the training set:
$$\tilde{\boldsymbol{\alpha}}_{\text{test}} = \frac{\boldsymbol{\alpha}_{\text{test}} - \mu}{\sigma}.$$
3. **SVM Inference:** Finally, the standardized sparse representation is input to the SVM classifier:
$$\hat{y} = \text{SVM}(\tilde{\boldsymbol{\alpha}}_{\text{test}}),$$
where $\hat{y} \in \{0, 1\}$ is the predicted label, classifying the test sample as either Alice ($\hat{y} = 0$) or Eve ($\hat{y} = 1$).

Algorithm of *Method Sparse-DL-SVM*

1: **Train-Test Split:** Split dataset into training (X_{train}), testing (X_{test}), and evaluation (X_{eval}) sets.
2: **Data Preprocessing:** Extract CIR magnitudes from X_{train} and stack into dataset (X_{train}, y_{train})
3: **Dictionary Learning:** Learn dictionary $\mathbf{D}$ using Lasso-based approach on X_{train}.
4: **Sparse Encoding:** Encode training samples into sparse representations $\boldsymbol{\alpha}$.
5: **Standardization:** Normalize sparse representations.
6: **Train SVM:** Fit SVM classifier on standardized sparse representations of X_{train}.
7: **Testing:** Transform and classify X_{test} using trained SVM.
8: **Evaluation:** Compute classification metrics (Accuracy, FAR, MDR, AR) on X_{eval}.

The evaluation dataset is used to evaluate the model and this dataset is also preprocessed the same way as the testing dataset. Evaluation of this method and the comparison with the review paper, are briefly explained in the evaluation chapter.

Evaluation

5.1 Dataset

This section introduces the dataset [31] used throughout this thesis to explore PLA techniques. The dataset comprises real-world UWB channel measurements providing a valuable resource for analyzing signal characteristics in a realistic indoor setting.

Measurement Environment

All measurements were taken in a typical office space measuring approximately 5.9 m in length and 3.05 m in width [31]. The environment includes standard office furnishings and several sources of signal reflections: a radiator, cable channels running along the walls, and an inset doorway. The experimental setup consisted of three fixed anchor nodes (A0, A1, and A2) placed at a height of 1.15 m, with an additional position (A1') introduced to create asymmetry in certain scenarios [31]. These anchors help capture multipath effects, fading, and spatial diversity by providing stable reception points for CIR measurements. The transmitter was positioned at different predefined locations within the environment to simulate various channel conditions. This setup offers a variety of line-of-sight and non-line-of-sight propagation paths, which helps capture the nuanced effects of multipath fading and shadowing that are crucial for wireless security research.

Measurement Scenarios

Five key scenarios are provided within this dataset, each contributing to a comprehensive assessment of channel variability:

- Symmetric - Anchors A0, A1, and A2 maintain a symmetric layout. This scenario reflects a nominal indoor environment with moderate mobility of the transmitter.

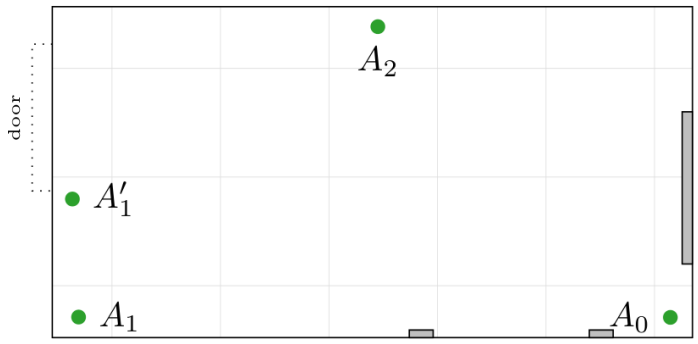

Figure 5.1: Schematic Floor Plan of the Measurement Room [31]

- **Asymmetric** - One anchor is replaced by A1', breaking the symmetry in the anchor placement. This scenario highlights how minor changes in anchor positions affect signal propagation and channel diversity.
- **Reflector** - A lightweight reflector was introduced, rotating at a fixed rate near the ceiling. By adding time-varying reflections, this scenario tests the robustness of authentication algorithms against complex, dynamic multipath conditions.
- **Varying speed** - The transmitter (mounted on a mobile platform) moves at changing speeds, ranging from 0.15 m/s down to 0.05 m/s. This scenario helps isolate how different motion velocities influence channel coherence and the feasibility of real-time authentication.
- **No movement** – The transmitter remains stationary at predefined 1m × 1m grid points within the environment, where it is manually placed and does not move. This scenario ensures that only small-scale fading effects influence the signal variations and serves as a baseline for comparison with mobility-based scenarios.

For our research, we excluded the *No Movement* scenario, as our focus is on authentication performance under mobility.

Communication and Measurement Collection

From the original dataset, for our authentication problem, we only consider the CIR observed at Bob, meaning we focus on one-way transmission from Alice to Bob while treating only one attacker or Eve as an active adversary who also transmits to Bob.

Each recorded CIR measurement in the dataset contains 15 channel observations, reflecting different multipath components. According to the dataset description and to adapt this dataset for our authentication problem, we:

- Selected **Channel 3** as the communication channel between Alice and Bob.
- Selected **Channel 6** as the adversarial channel between Eve and Bob.
- Disregarded bidirectional measurements as our authentication model only requires Bob's received CIR.

During each transmission, CIR data was recorded in its complex form, consisting of *real* and *imaginary* components. For our research, we computed the *magnitude* from the *real* and *imaginary* components and used this transformed data as input for our authentication methods. This preprocessing ensures a controlled differentiation between legitimate and adversarial signals, making it suitable for evaluating authentication techniques based on channel characteristics. In subsequent chapters, we elaborate on how these preprocessed CIR observations are used for training and evaluating our proposed authentication methods.

5.2 Reference paper

This section reviews the foundational work by *Abdrabou* and *Gulliver*, titled *Adaptive Physical Layer Authentication Using Machine Learning With Antenna Diversity* [33]. We will discuss the reason for choosing this paper as the reference paper, their system model, authentication approach, and the performance metrics they use. The goal is to provide a clear understanding of their approach before outlining how our proposed methods build upon their framework.

Why this paper?

In our research, we selected this paper as the reference paper for comparison with our proposed methods. There are several key reasons:

- Focus on Passive Authentication: Our research aim was to develop passive PLA methods, and this paper aligns with that goal by leveraging channel characteristics without modifying the transmitted signal.
- High-Performance Claims: The paper reports strong authentication performance with their simulated dataset. So we wanted to see with our real-world dataset if it performs the same way. That also makes it a relevant reference to assess the effectiveness of our proposed methods.
- ML-Based Approach: Since our work incorporates machine learning, this paper's use of OCC-SVM provides a relevant comparison to evaluate different classification strategies.

These factors make it a strong reference paper for evaluating and contextualizing our contributions to PLA in wireless communication systems.

System model

The system model presented in [33] differs from our research setup. Their model considers a multi-antenna base station (Bob) receiving signals from a legitimate transmitter (Alice) while multiple eavesdroppers (Eve) attempt to intercept the communication. This setup was simulated rather than derived from a real-world dataset, focusing on evaluating authentication performance in an idealized scenario. In contrast, our research employs a real-world dataset with Alice transmitting signals to Bob, where Eve also transmits signals to Bob over a separate channel and Bob estimates each channel. This difference ensures that our authentication evaluations consider practical environmental variations and real-world multipath effects, making our results more representative of actual wireless deployments.

Features

Bob employs multiple receive antennas to exploit antenna diversity. From each antenna, the following features are extracted - the *real (R)* , *imaginary (I)*, and the *magnitude (M)* components of the received signal.
For *N* antennas, this results in a total of *3N* features.

$$(R_1, I_1, M_1, \ldots, R_N, I_N, M_N)$$

Scaling These features are scaled using *min-max* scaling before being fed into the OCC-SVM to ensure equal contribution from all feature types (magnitude, real, and imaginary components) [33]. Since these features have different numerical ranges, scaling prevents high-magnitude features from dominating the classification process. *Min-max* normalization maps values to a fixed range (e.g., [0,1]), preserving feature distribution and maintaining consistency across training, testing, and evaluation data. This improves the SVM's ability to separate legitimate and adversarial signals effectively.

One-Class Classifier Support Vector Machine (OCC-SVM)

OCC-SVM is utilized to define a decision boundary that encapsulates most of the legitimate user's training data while distinguishing it from potential adversarial signals. The decision function is derived by solving the following optimization problem:

$$\min_{w,s,\rho} \quad \frac{1}{2}\|w\|^2 + \frac{1}{\nu\ell}\sum_{i=1}^{\ell} s_i - \rho$$

subject to

$$\big(w \cdot \Phi(g_i)\big) \geq \rho - s_i, \quad s_i \geq 0, \quad i = 1, \ldots, \ell, \tag{5.1}$$

where $\mathbf{w}$ is the weight vector in the transformed feature space, $\Phi(\cdot)$ is the mapping function from the input space to the high-dimensional feature space, $\mathbf{g}_i$ is the feature vector of the i-th training sample (in our case, the $3N$ features from each SRS snapshot, s_i (slack variable) measures how far a sample falls outside the learned boundary, ρ is a parameter representing the offset or bias of the boundary, ν (ν) is the regularization parameter controlling the fraction of outliers and hence the trade-off between the volume enclosed and the misclassified points, and ℓ is the number of training samples [34][42].

Conceptually, ν dictates how "loose" or "strict" the boundary is. A larger ν allows more outliers but can capture complex distributions, while a smaller ν creates a tighter boundary around the training data. The parameter ρ helps position the decision boundary in the transformed feature space.

Authentication Phases

There are two phases in the authentication - **Initial phase** (T_1) and **Subsequent phases** (T_2,T_3, ..., T_n).

In the **Initial phase (T_1)**, ULA is performed. During this phase, Bob collects training data from Alice using SRS in the 5G uplink radio frame. This data is used to train the OCC-SVM with features derived from the received signals.

And in the **Subsequent phases (T_2,T_3, ..., T_n)**, Testing and retraining are conducted. The received signals are tested against the OCC-SVM boundary. If the test passes, the features are updated and used to retrain the classifier. If it fails, the connection is terminated.
As illustrated in Figure 5.2.

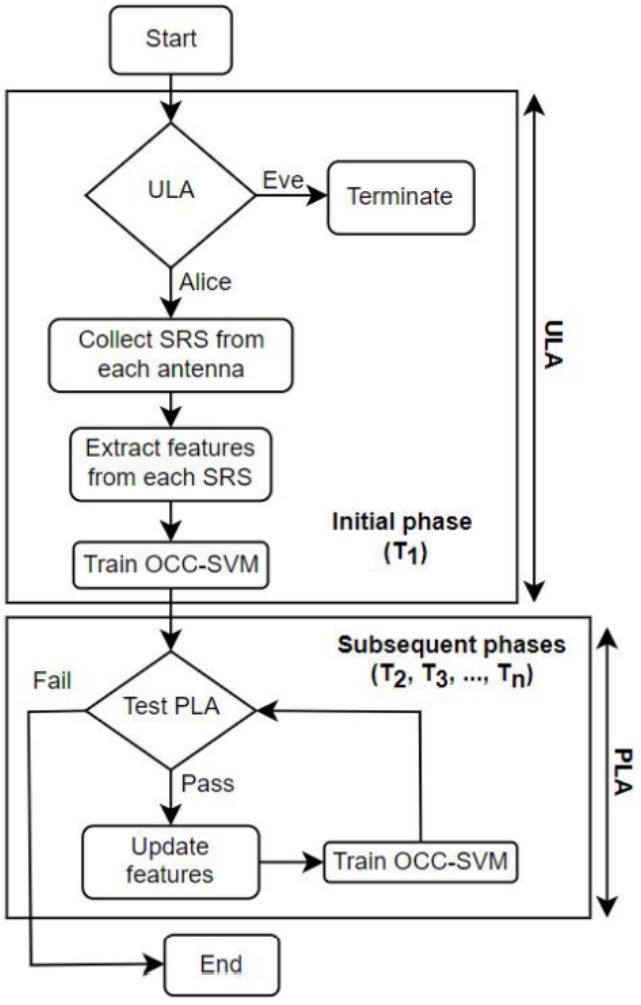

Figure 5.2: ALPLA Authentication Scheme Flowchart [33]

5.3 Metrics for Evaluation

Evaluating the efficacy of a PLA system involves measuring how often it correctly recognizes legitimate users and rejects adversaries. In this thesis, we adopt the confusion matrix framework shown in figure 5.3, which is standard in binary classification tasks. The confusion matrix helps us to compute the evaluation metrics - MDR, FAR, and AR for our methodologies to evaluate. The confusion matrix contrasts the actual label (legitimate user vs. illegitimate user) with the predicted label (accepted vs. rejected), generating four possible outcomes:

Confusion Matrix	Predict Negative	Predict Positive
Actual Negative	TN $\mathcal{H}_1$	FP Type II error
Actual Positive	FN Type I error	TP $\mathcal{H}_0$

Figure 5.3: Confusion Matrix [33]

- **True Positive (TP)**: The system correctly accepts a legitimate user.
- **True Negative (TN)**: The system correctly rejects an illegitimate user.
- **False Positive (FP)**: The system incorrectly accepts an illegitimate user.
- **False Negative (FN)**: The system incorrectly rejects a legitimate user.

From this confusion matrix, three key metrics are derived - *Missed Detection Rate (MDR)*, *False Alarm Rate (FAR)*, and *Authentication Rate (AR)*. These metrics are commonly used in PLA to assess the system's effectiveness in distinguishing legitimate users from adversaries [33] [39]. The desired values of these key metrics are typically derived from the reference paper. Based on the reference paper [33], the following values were achieved using our dataset:

- **MDR**: A lower MDR ensures fewer legitimate users are mistakenly rejected. In the reference paper, MDR values varied across scenarios, with 0.17 in the Asymmetric scenario and up to 0.51 in Symmetric Varyingspeed, indicating performance variations due to mobility.
- **FAR**: Lower FAR reduces the risk of an adversary being misclassified as a legitimate user. From the reference paper, we observed that FAR values between 0.41 (Symmetric) and 0.48 (Asymmetric).
- **AR**: Higher AR reflects improved authentication reliability. From the reference paper, we observed AR values ranging from 0.530 (Symmetric VarSpeed) to 0.677 (Asymmetric).

Using the dataset, our methodologies aim to improve upon these baseline values, ensuring better authentication performance while addressing system robustness across different mobility and environmental conditions.

Missed Detection Rate (MDR)

MDR measures the proportion of illegitimate attempts that are mistakenly accepted by the system. A lower MDR indicates that attackers are more consistently detected and blocked. In PLA contexts, this metric is particularly important because a high MDR means the system is failing to detect adversaries which is a critical weakness in any authentication scheme. The equation for MDR is:

$$MDR = \frac{FP}{FP + TN} \tag{5.2}$$

False Alarm Rate (FAR)

FAR tracks how frequently the system rejects legitimate users. In other words, among all genuine authentication requests, FAR is the fraction that is misclassified as illegitimate. Keeping FAR low is crucial for user satisfaction since legitimate clients should not be regularly denied access to the system. FAR is defined as:

$$FAR = \frac{FN}{FN + TP} \tag{5.3}$$

Authentication Rate (AR)

AR offers a single-value measure that balances the correct acceptance of legitimate users (TP) and the correct rejection of illegitimate users (TN). AR is defined as:

$$AR = \frac{TP + \gamma \times TN}{(TP + FN) + \gamma \times (TN + FP)} \tag{5.4}$$

The parameter γ adjusts the relative importance of legitimate vs. illegitimate user classification. It is often defined as:

$$\gamma = \frac{TP + FN}{TN + FP} \tag{5.5}$$

By tuning γ, one can emphasize either higher accuracy for genuine users or stricter screening of potential attackers, depending on the security requirements of the application.

In practice, there is often a trade-off between lowering MDR (strict measures against attackers) and lowering FAR (convenience for legitimate users). Deciding the right operating point depends on the security needs and tolerance for user inconvenience. For instance, critical infrastructure may prioritize reducing missed detections (MDR) even if it slightly increases the false alarm rate (FAR).

By analyzing these metrics together, we gain comprehensive insights into the performance of our PLA methods. The final choice of γ or decision thresholds can be guided by the specific application requirements, ensuring that we achieve an acceptable balance between usability and security.

5.4 Implementation Setup and Parameters

This section outlines the technical setup and parameters used in the implementation and evaluation of all the proposed methods. It includes details on the software tools, dataset configuration, feature extraction settings, and classifier hyperparameters.

Software and Development Environment

The implementation was carried out using Python 3.12.3 as the language, Jupyter Notebook as the environment and VS Code as the code editor. The following libraries were used:

- Scikit-learn: For PCA, SVM, Dictionary Learning, OMP, Standard Scaler, Confusion Matrix, and Train-Test Split.
- NumPy: For numerical computations.
- Matplotlib: For plotting CIR signals and performance metrics.

All experiments were conducted on a system equipped with a 32-core CPU with L3 cache (512 MB) and 31 GB RAM. No additional GPU acceleration was used.

Dataset Configuration

The dataset consisted of 2000 CIR samples, which were split as follows:

- Training Set: 1200 CIRs (60%)
- Testing Set: 400 CIRs (20%)
- Evaluation Set: 400 CIRs (20%)

Preprocessing included PCA for dimensionality reduction and Sparse Representation for feature extraction.

Method-Specific Parameters

Table 5.1 explains the parameter used for PCA-SVM,

Table 5.1: Implementation Parameters for PCA-SVM Method

Parameter	Value
Scaling	StandardScaler()
PCA component	2,3,4,5,6
Model	SVM
Kernel	RBF

Table 5.2 explains SRC configuration,

Table 5.2: Implementation Parameters for SRC Method

Parameter	Value
Feature Extraction	Sparse representation
Non zero coefficient no.	2,4,8,10
Model	OMP

Table 5.3 explains PCA-SRC configuration,

Table 5.3: Implementation Parameters for PCA-SRC Method

Parameter	Value
Scaling	StandardScaler()
Dimension Reduction	PCA
PCA component	2,3,4,5,6
Feature Extraction	Sparse representation
Non zero coefficient no.	2,3,4,5
Model	OMP

And table 5.4 explains Sparse-DL-SVM configurations,

Table 5.4: Implementation Parameters for Sparse-DL-SVM Method

Parameter	Value
Dictionary Atoms	2, 4, 8, 10
Feature Extraction	Lasso-based Dictionary Learning
Scaling	StandardScaler()
SVM Kernel	RBF

These tables summarize the key parameters and configurations used in each method. The experimental results and findings based on these configurations will be discussed in the following chapters.

Code availability

Codes can be found here - https://github.com/mdarefinsaad/Thesis-CRKG/

5.5 Evaluation Results and Analysis

In this section, we present and discuss the performance results of our four proposed methods compared to the reference paper Adaptive lightweight physical layer authentication (ALPLA). Our evaluation encompasses four indoor scenarios - Symmetric, Symmetric with Varying Speed, Asymmetric, and Asymmetric with Reflector to ensure coverage of both standard and challenging channel conditions. We use multiple metrics, including classification accuracy, false alarm rate (FAR), missed detection rate (MDR), and authentication rate (AR), to provide a comprehensive assessment of each method's strengths and weaknesses.

5.5.1 Performance Evaluation of Individual Methods

In this section, we evaluate the performance of each proposed authentication method. Each method is assessed under different experimental scenarios to understand its classification accuracy, robustness to channel variations, and overall effectiveness in distinguishing legitimate transmitters from adversaries. The results are presented individually for each method, highlighting key observations and trends in their performance.

Evaluation of Method PCA-SVM

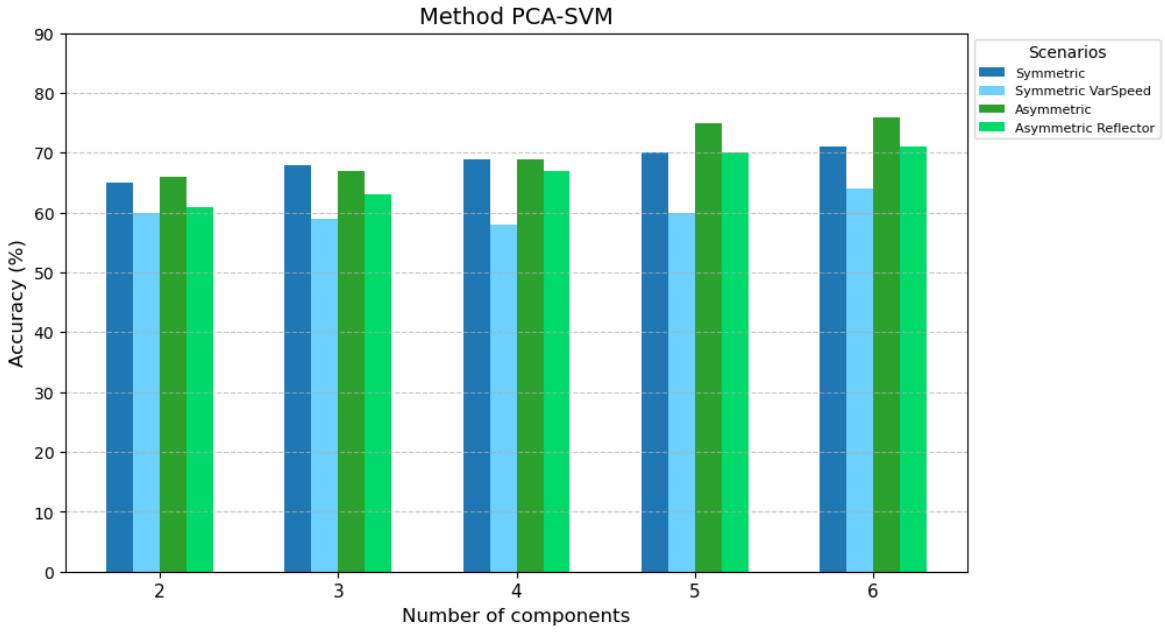

Figure 5.4: Method PCA-SVM - Accuracy Comparison with Different PCA Components in Different Scenarios

In Figure 5.4, we examine how classification accuracy varies with the number of principal components (ranging from 2 to 6) for method PCA-SVM, which applies PCA followed by an SVM classifier. Each bar group corresponds to one of four measurement scenarios - *Symmetric*, *Symmetric Varying Speed*, *Asymmetric*, and *Asymmetric Reflector*. At the lower

dimensionality (2 components), accuracies range roughly between 58% and 63% across the four scenarios, indicating that a minimal feature space might omit important channel variations. As the number of components increases to 5 or 6, we see a general rise in performance: for instance, the *Symmetric* scenario climbs from about 63% at 2 components to around 73% at 6, while the *Asymmetric* setup sees a similar improvement from about 61% to 74%. Even the *Varying Speed* and *Reflector* scenarios, which introduce additional motion or reflective interference, reach 70%–71% accuracy by 6 components. This progression suggests that incorporating more principal components helps capture richer channel information, ultimately leading to more robust classification.

Evaluation of Method SRC

From figure 5.5, the results indicate that classification accuracy generally improves slightly as the number of non-zero coefficients increases. For example, in the *Symmetric* scenario, accuracy rises from approximately 60% with 2 coefficients to 65% at 10 coefficients, showing a modest improvement. Similarly, in the *Asymmetric* scenario, accuracy increases slightly from 60% to 62%, suggesting that while adding more coefficients helps retain more relevant channel features, the overall gain is limited. The *Asymmetric Reflector* scenario initially achieves 65% accuracy with 2 coefficients but drops slightly to 62% at 10 coefficients, indicating that increasing the number of coefficients does not always yield better performance. Meanwhile, the *Symmetric Varying Speed* scenario improves only marginally from 58% to 60%, showing that under dynamic conditions, sparse reconstruction alone struggles to enhance classification accuracy significantly.

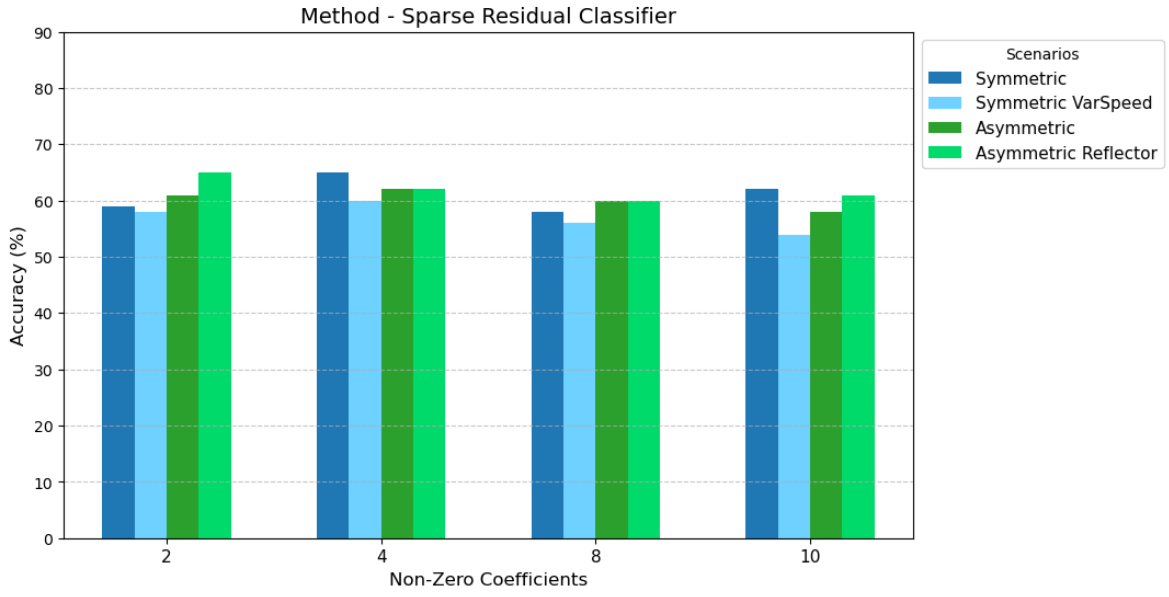

Figure 5.5: Method SRC - Accuracy Comparison with Non-zero Coefficient in Different Scenarios

While increasing the number of non-zero coefficients generally improves classification performance, the overall accuracy remains relatively low, indicating the limitations of

this method. These results highlight a key limitation of the method SRC: while sparse representation helps retain structural features of the channel, it does not provide a strong discriminative capability on its own. The overall low accuracy across all scenarios suggests that additional processing steps such as feature refinement or hybrid approaches may be necessary to achieve more reliable authentication performance.

Evaluation of Method PCA-SRC

In figure 5.6, we can see that, by keeping the non-zero coefficient count fixed, in the *Symmetric* scenario, accuracy starts at approximately 58% with 2 components, briefly peaks around 65% at 4 components, but then declines again, showing instability in feature representation. The *Asymmetric Reflector* scenario exhibits a similar trend, but despite an initial rise above 65%, its accuracy drops to nearly 60%, indicating that increasing the number of components does not provide consistent improvements. The Asymmetric scenario remains within a low range of 60–63%, showing no significant gains. Meanwhile, the *Symmetric Varying Speed* scenario performs the worst, experiencing a steady decline beyond 4 components, highlighting a lack of robustness in dynamic conditions.

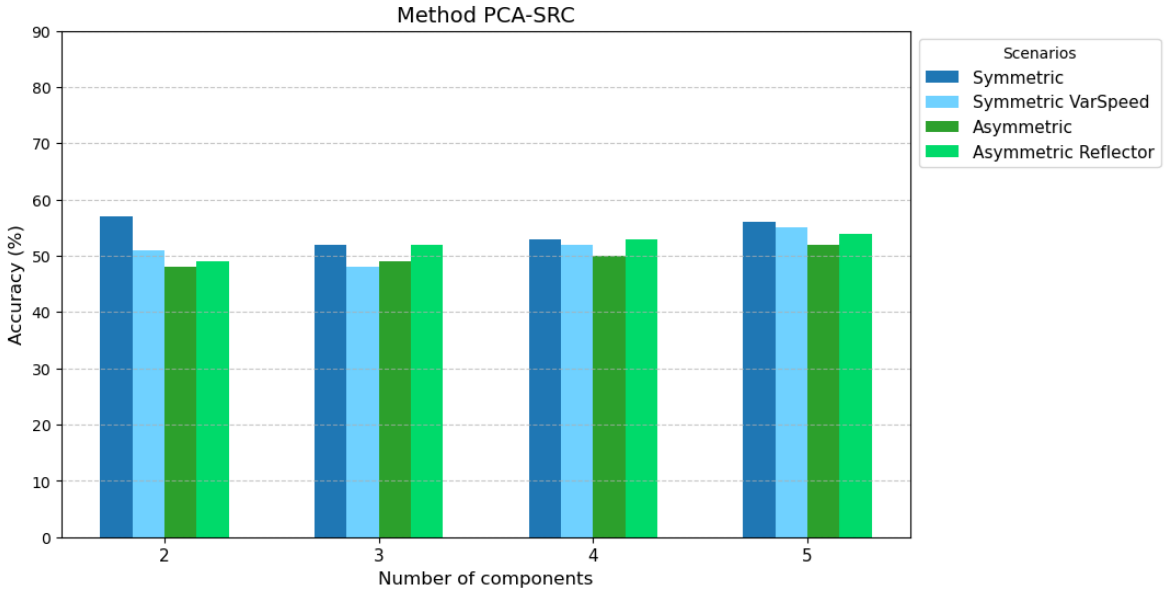

Figure 5.6: Method PCA-SRC - Accuracy Comparison with Different PCA Components in Different Scenarios

These results indicate that method PCA-SRC struggles to extract meaningful features from the CIR dataset, leading to suboptimal classification performance. Unlike method SRC, which at least demonstrated moderate improvements with increased coefficients, method PCA-SRC fails to show any meaningful enhancement beyond a certain point. The method's instability and consistently poor performance across all scenarios suggest that it is not a viable approach for physical layer authentication under the tested conditions.

Evaluation of Method Sparse-DL-SVM

Figure 5.7 illustrates the classification accuracy of Sparse-DL-SVM as the dictionary size (i.e., the number of learned atoms) is varied. Even with only 5 atoms, the *Symmetric* scenario achieves a reasonable accuracy above 70%, while the *Asymmetric* scenario starts slightly lower at 68–69%. As the number of atoms increases to 10, 15, and 20, classification performance consistently improves across all scenarios. Notably, the *Symmetric* scenario reaches approximately 80–82% accuracy at 20 atoms, while the *Asymmetric Reflector* scenario shows a steady improvement, rising from 72% to 78%.

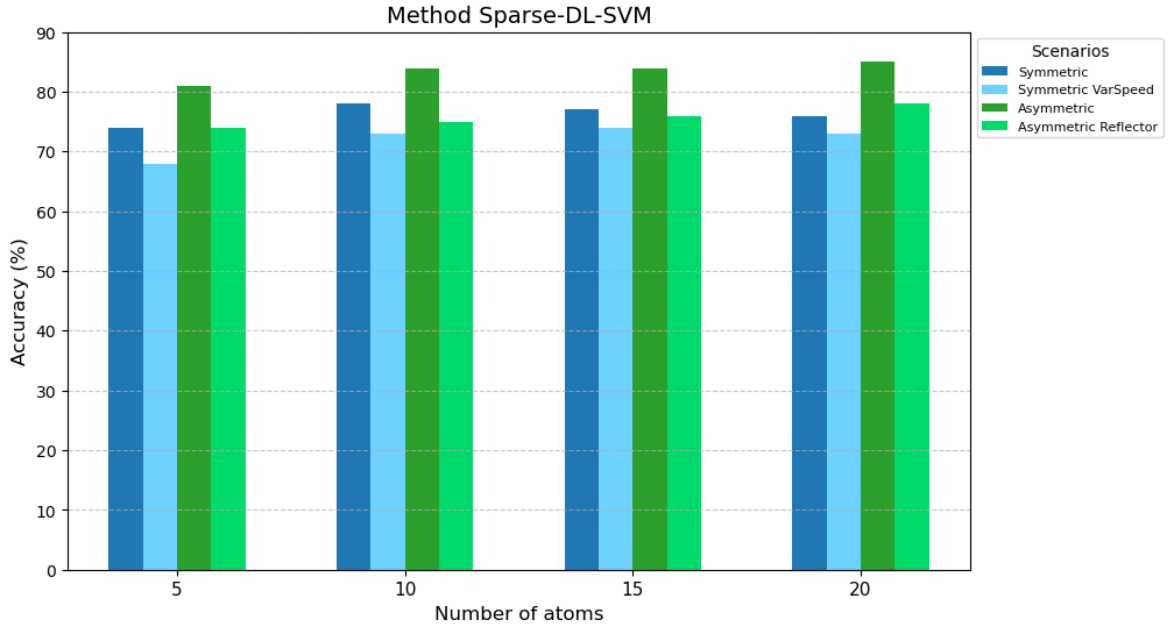

Figure 5.7: Method Sparse-DL-SVM - Accuracy Comparison with No. of Learned Dictionary Atoms in Different Scenarios

The *Symmetric* scenario in particular approaches 80–82% accuracy at 20 atoms, and even the *Asymmetric Reflector* data maintains a consistent rise from roughly 72% up to 78%. This trend suggests that increasing the dictionary size enhances the model's ability to capture fine-grained channel features, leading to better sparse representations. Unlike previous methods, method Sparse-DL-SVM maintains a strong and stable classification performance across different scenarios, reinforcing the effectiveness of dictionary learning in feature extraction for authentication.

5.5.2 Comparative Analysis Based on Evaluation Metrics

MDR Analysis

Figure 5.8 shows the MDR across four scenarios - *Symmetric*, *Symmetric VaryingSpeed*, *Asymmetric*, and *Asymmetric Reflector* for ALPLA (blue) and our four proposed methods: PCA-SVM (orange), SRC (green), PCA-SRC (red), and Sparse-DL-SVM (purple). Overall, Sparse-DL-SVM consistently achieves the lowest MDR, dipping below 0.20 in the *Symmetric* scenario and remaining below 0.30 even in the challenging *Asymmetric Reflector* case. In contrast, PCA-SRC shows the highest MDR in three of the four scenarios, exceeding 0.60 in the *Symmetric VaryingSpeed* and *Asymmetric* conditions. ALPLA and PCA-SVM fall in a middle range, with ALPLA reaching between 0.40 and 0.50 in some conditions and PCA-SVM mostly hovering between 0.25 and 0.35.

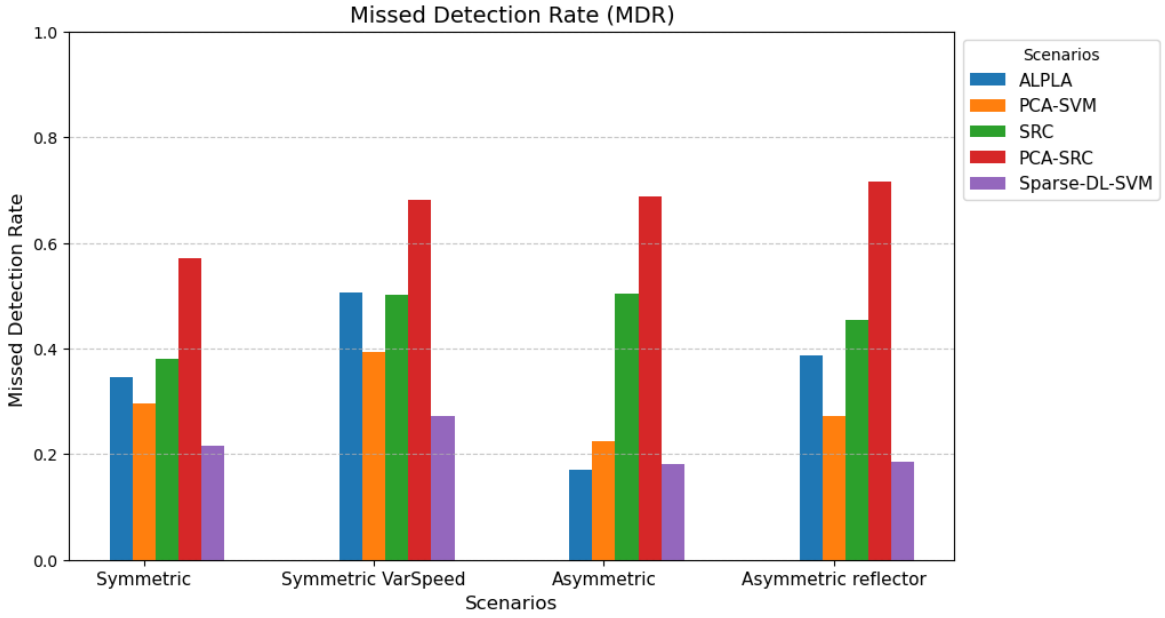

Figure 5.8: MDR Comparison of Different Methods with the Reference Paper

These results suggest that while PCA-SRC struggles to detect illegitimate users reliably, Sparse-DL-SVM offers a more robust approach, consistently outperforming the review paper's ALPLA baseline in terms of lower missed detections.

FAR Analysis

From figure 5.9, we can see that in the *Symmetric* setup, ALPLA peaks at around 0.40, while PCA-SRC provides the lowest FAR near 0.20, indicating fewer false alarms. PCA-SVM and SRC fall somewhere in between, hovering between 0.25–0.35, with Sparse-DL-SVM around 0.30. When speed variations are introduced (*Symmetric Varying Speed*), ALPLA climbs further toward 0.45, and PCA-SVM approaches 0.40. By contrast, PCA-SRC dips closer to 0.25, performing

better than the other methods, while SRC and Sparse-DL-SVM remain in the mid-range, around 0.30–0.35.

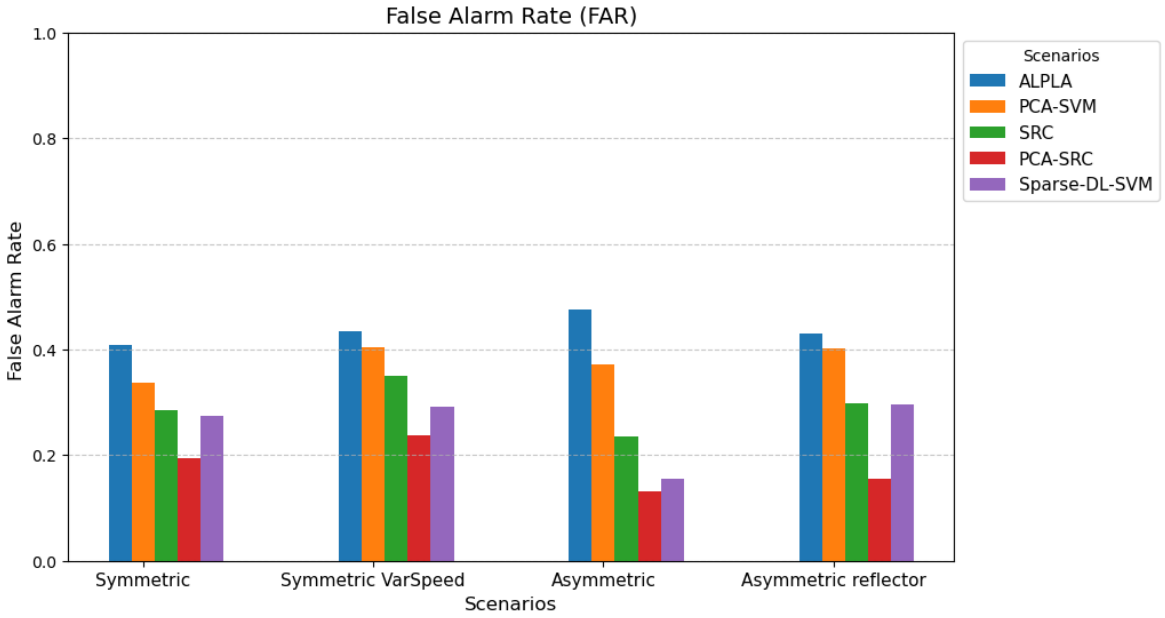

Figure 5.9: FAR Comparison of Different Methods with the Reference Paper

In the *Asymmetric* scenario, ALPLA increases to about 0.50, whereas PCA-SRC stays below 0.20, dramatically reducing FAR. SRC hovers at around 0.25, and Sparse-DL-SVM lands near 0.20–0.25. Under *Asymmetric Reflector* conditions, ALPLA drops to 0.45, PCA-SVM hits 0.30, SRC is roughly 0.25, and PCA-SRC sits around 0.20. Sparse-DL-SVM stands near 0.28, again indicating moderate performance relative to the others. Taken together, these results show PCA-SRC consistently achieving the lowest false alarm rates, outperforming both ALPLA and the other proposed techniques, especially in *Asymmetric* scenarios.

AR Analysis

In figure 5.10, we observe that across all scenarios, Sparse-DL-SVM consistently yields the highest AR, often exceeding 0.80—notably in the Asymmetric case, where it reaches approximately 0.90. By comparison, ALPLA ranges from about 0.50 to 0.65, trailing behind the other approaches, especially in the Symmetric VarSpeed scenario. PCA-SVM and SRC deliver moderate gains, hovering between 0.60 and 0.70, while PCA-SRC tends to dip slightly lower, around 0.55 to 0.65 in most tests. Overall, the strong AR results from Sparse-DL-SVM reinforce its ability to achieve both low false alarms and low missed detections, maintaining a more balanced and effective authentication performance compared to both the baseline (ALPLA) and other proposed methods.

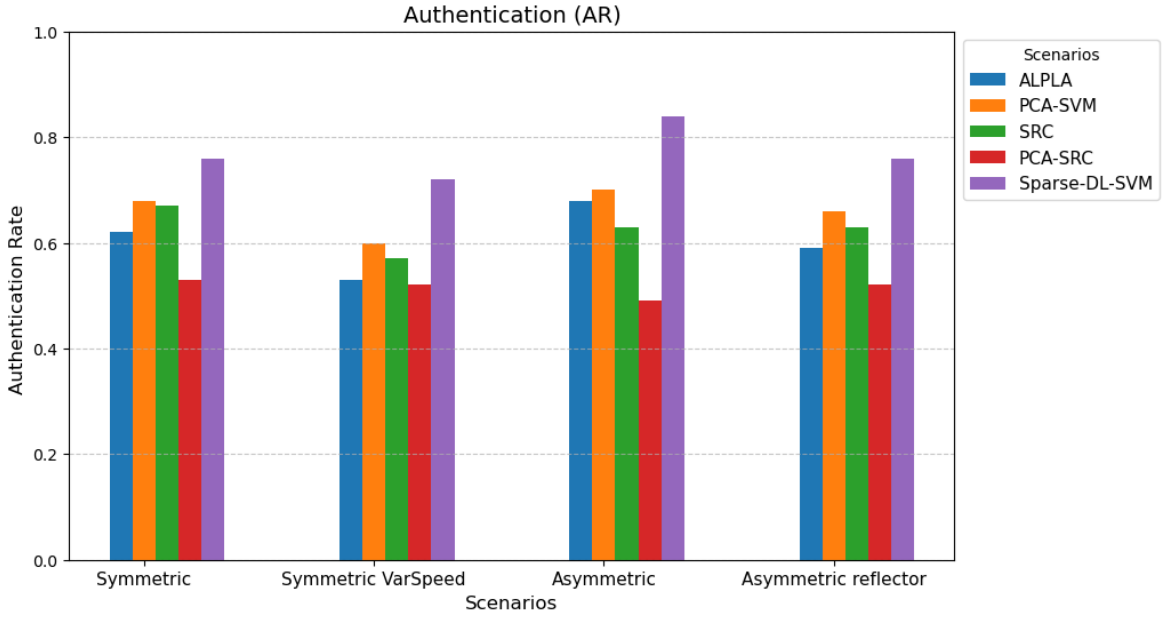

Figure 5.10: AR Comparison of Different Methods with the Reference Paper

Discussion

This chapter provides a comprehensive discussion of the experimental findings, interprets the implications of the results, and reflects on the strengths and limitations of the proposed approaches. In particular, we analyze how the performance of the various methods compares across different indoor scenarios and elaborate on the challenges encountered during the evaluation. Importantly, we also discuss the two methods that did not yield the expected results.

6.0.1 Summary of Key Findings

Our experimental evaluation focused on four authentication methods, which were compared against the baseline approach (ALPLA) using multiple performance metrics such as classification accuracy, MDR, FAR, and AR. Overall, the results reveal that:

- Sparse-DL-SVM consistently achieved the highest accuracy (up to 80–82% in favorable conditions) and the best AR, while maintaining low MDR and FAR across all scenarios.
- PCA-SVM demonstrated moderate yet stable performance, especially in scenarios with less severe channel variations.

However, our evaluation also highlighted that two of the proposed methods did not perform as expected:

- The SRC method, which relies on OMP for channel representation, consistently produced lower accuracy (ranging between 60–65%) and was more sensitive to variations in the number of non-zero coefficients.
- The PCA-SRC approach, intended to combine dimensionality reduction with sparse coding, underperformed relative to our expectations by exhibiting higher MDR and lower AR across several test conditions.

6.0.2 Interpretation of the Results

This section analyzes the performance of different authentication methods, highlighting successful approaches and challenges faced by underperforming techniques. By examining the strengths and limitations of each method, we gain insights into the factors influencing authentication accuracy and potential areas for improvement.

Successful Approaches

The strong performance of the Sparse-DL-SVM method underscores the benefits of leveraging a learned dictionary to capture richer channel representations. By extracting more discriminative features, this approach proved robust against multipath fading and variations introduced by mobility and environmental asymmetry. Likewise, the PCA-SVM method, despite its simplicity, offered competitive performance in scenarios where the channel variations were moderate. These results confirm that when the feature extraction method preserves critical signal characteristics, even conventional classifiers like SVM can yield reliable authentication outcomes.

Challenges with Underperforming Methods

In contrast, the SRC and PCA-SRC methods did not meet our performance expectations. Several factors may have contributed to their shortcomings:

- Information Loss in Dimensionality Reduction: For the PCA-SRC approach, the reduction in dimensionality likely resulted in the loss of critical channel information. Although PCA is effective at capturing the most significant variance in the data, the discarded components may have contained subtle features essential for differentiating between legitimate and adversarial signals.
- Parameter Tuning Limitations: Both SRC-based performed poorly because they rely on sparse reconstruction errors instead of direct classification, are highly sensitive to dictionary quality and parameter selection, and struggle with CIR variability and non-linearity. Despite thorough experimentation, the optimal parameters for robust performance across all scenarios remained elusive.

6.0.3 Limitations and Future Directions

While the evaluation provides valuable insights into the performance of the proposed PLA methods, several limitations must be acknowledged. First, the dataset used in this study was recorded in a controlled indoor office environment. Although this setting allowed for systematic and reproducible data collection, it does not fully capture the complexities of real-world deployments where unpredictable interference and more severe

multipath conditions may significantly affect system performance. Additionally, the SRC-based methods demonstrated a pronounced sensitivity to parameter selection, suggesting that further research is needed to develop more adaptive parameter tuning strategies that can generalize across diverse environments and dynamic channel conditions. Building on these observations, future research should address several promising directions to enhance both the performance and practical deployment of PLA systems:

Deep Learning Architectures

Recent advances in deep learning have shown significant potential for enhancing feature extraction and classification accuracy. Future work should investigate the use of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to automatically learn complex, discriminative features directly from raw CIR data. These architectures may capture non-linear relationships and temporal dynamics more effectively than traditional methods, potentially leading to higher authentication accuracy.

Real-Time Implementation

For PLA systems to be viable in practical wireless networks, real-time performance is essential. Future studies should focus on optimizing computational efficiency for deployment on edge devices by leveraging hardware accelerators such as field-programmable gate arrays (FPGAs) or graphics processing units (GPUs). Developing and fine-tuning algorithms that are both efficient and scalable will be crucial to meet the stringent latency requirements of real-world applications.

Adversarial Robustness

As spoofing and adversarial attacks become increasingly sophisticated, ensuring the robustness of PLA methods is paramount. Future research should evaluate the proposed methods against advanced spoofing techniques, including those that utilize generative adversarial networks (GANs) to simulate realistic but malicious CIR signals. Enhancing adversarial robustness will help safeguard PLA systems against emerging threats, thereby improving overall security.

Multi-Node Authentication

The current study primarily focuses on scenarios with a single legitimate user interacting with potential adversaries. However, the growing prevalence of IoT devices calls for authentication frameworks capable of handling multi-user environments. Extending the PLA framework to support multi-node authentication in dense IoT networks will be an important step toward

developing scalable and robust systems. This extension should address the challenges of distinguishing between multiple legitimate users while simultaneously detecting adversarial behavior.

Conclusion

This thesis explored the potential of CIR-based PLA as a lightweight and robust authentication framework for wireless communication systems. With the increasing adoption of the IoT and the inherent security vulnerabilities in conventional cryptographic authentication schemes, there is a growing demand for efficient authentication mechanisms that do not impose significant computational overhead. By leveraging the unique physical characteristics of wireless channels, CIR-based authentication provides a promising alternative to traditional key-based methods, offering resilience against impersonation attacks while ensuring low computational complexity.

To address the challenges associated with CIR-based authentication, this research introduced and evaluated four distinct methodologies: (1) *Principal Component Analysis with Support Vector Machine* (PCA-SVM), (2) *Sparse Residual Classifier* (SRC), (3) *PCA with Sparse Representation-based Classification* (PCA-SRC), and (4) *Sparse Dictionary Learning with SVM* (Sparse-DL-SVM). Each method was designed to extract and utilize unique CIR features for authentication, with varying approaches to dimensionality reduction, feature extraction, and classification. Experimental evaluations using real-world UWB channel measurements demonstrated that all proposed methods outperformed the reference work in terms of AR, MDR, and FAR.

Among the four methods, Sparse-DL-SVM emerged as the most effective approach, achieving the highest authentication accuracy (up to 82%) while maintaining a balanced trade-off between MDR and FAR across diverse testing scenarios. The PCA-SVM approach also exhibited competitive performance, particularly in scenarios with moderate channel variations. Conversely, the SRC and PCA-SRC methods, while conceptually promising, exhibited higher sensitivity to parameter tuning and a tendency to lose critical channel information, resulting in lower classification accuracy and higher error rates.

Despite the promising results, several limitations must be acknowledged. The evaluation was conducted in a controlled indoor environment, which, while realistic, does not fully encapsulate the complexity of dynamic, large-scale wireless networks. Additionally, the sensitivity of SRC-based methods to parameter selection suggests the need for more adaptive feature extraction techniques. Future research directions should focus on real-time

implementation of CIR-based authentication on resource-constrained IoT devices, adversarial robustness against sophisticated spoofing attacks, and multi-node authentication in large-scale wireless networks. The integration of deep learning techniques, such as CNNs or RNNs, could further enhance feature extraction and classification accuracy, offering new pathways for developing advanced CIR-based authentication schemes.

In summary, this research underscores the viability of CIR-based authentication as a scalable, efficient, and secure solution for future wireless communication systems. By demonstrating the efficacy of physical layer authentication in real-world conditions, this work lays a foundation for future advancements in wireless security, paving the way for practical deployment in emerging technologies such as 5G, 6G, and large-scale IoT networks.

Acronyms

ML Machine Learning
CIR Channel Impulse Response
CFR Channel Frequency Responses
CSI Channel State Information
RSS Received Signal Strength
RSSI Received Signal Strength Indicators
USRP Universal Software Radio Peripherals
IoT Internet of Things
PLA Physical Layer Authentication
ULA Upper Layer Authentication
SNR Signal-to-noise ratio
OFDM Orthogonal Frequency Division Multiplexing
ELM Extreme Learning Machine
MIMO Multiple-Input Multiple-Output
NCA Neighborhood Component Analysis
RBF Radial Basis Function
SVM Support Vector Machine
PCA Principal Component Analysis
SVD Singular Value Decomposition
AUC Area Under The Curve
OCC-SVM One-Class Classifier Support Vector Machine
SRS Sounding Reference Signal
MDR Missed Detection Rate
FAR False Alarm Rate
AR Authentication Rate
OMP Orthogonal Matching Pursuit
Wifi Wireless Fidelity
Lasso-LARS Lasso Least Angle Regression
UWB Ultra-Wideband

ALPLA Adaptive lightweight physical layer authentication
t-SNE t-distributed Stochastic Neighbor Embedding
UMAP Uniform Manifold Approximation and Projection
LDA Linear Discriminant Analysis
CNNs convolutional neural networks
RNNs recurrent neural networks

List of Figures

Bibliography

[1] K. P. F.R.S., "Liii. on lines and planes of closest fit to systems of points in space," *Philosophical Magazine Series 1*, vol. 2, pp. 559–572, 1901. [Online]. Available: https://api.semanticscholar.org/CorpusID:125037489.

[2] H. Hotelling, "Analysis of a complex of statistical variables into principal components.," *Journal of Educational Psychology*, vol. 24, pp. 498–520, 1933. [Online]. Available: https://api.semanticscholar.org/CorpusID:144828484.

[3] C. Eckart and G. M. Young, "The approximation of one matrix by another of lower rank," *Psychometrika*, vol. 1, pp. 211–218, 1936. [Online]. Available: https://api.semanticscholar.org/CorpusID:10163399.

[4] A. V.N.Vapnik and V. N. Vapnik, "On a perceptron class," *Avtomat. i Telemekh*, vol. 25, pp. 112–120, 1964. [Online]. Available: http://mi.mathnet.ru/at11558.

[5] S. Mallat and Z. Zhang, "Matching pursuits with time-frequency dictionaries," *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3397–3415, 1993. DOI: 10.1109/78.258082.

[6] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995. DOI: 10.1007/BF00994018. [Online]. Available: https://link.springer.com/article/10.1007/BF00994018.

[7] C. Cortes and V. N. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, pp. 273–297, 1995. [Online]. Available: https://api.semanticscholar.org/CorpusID:52874011.

[8] B. A. Olshausen and D. J. Field, "Emergence of simple-cell receptive field properties by learning a sparse code for natural images," *Nature*, vol. 381, pp. 607–609, 1996. [Online]. Available: https://api.semanticscholar.org/CorpusID:4358477.

[9] R. Tibshirani, "Regression shrinkage and selection via the lasso," *Journal of the Royal Statistical Society. Series B (Methodological)*, vol. 58, no. 1, pp. 267–288, 1996, ISSN: 00359246. [Online]. Available: http://www.jstor.org/stable/2346178 (visited on 02/13/2025).

[10] K. Engan, S. Aase, and J. Hakon Husoy, "Method of optimal directions for frame design," in *1999 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99 (Cat. No.99CH36258)*, vol. 5, 1999, 2443–2446 vol.5. DOI: 10.1109/ICASSP.1999.760624.

[11] B. Efron, T. Hastie, I. Johnstone, and R. Tibshirani, "Least angle regression," *The Annals of Statistics*, vol. 32, no. 2, pp. 407–499, 2004. DOI: 10.1214/009053604000000067. [Online]. Available: https://doi.org/10.1214/009053604000000067.

[12] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *2007 IEEE International Conference on Communications*, 2007, pp. 4646–4651. DOI: 10.1109/ICC.2007.767.

[13] J. Mairal, F. Bach, J. Ponce, and G. Sapiro, "Online dictionary learning for sparse coding," in *Proceedings of the 26th Annual International Conference on Machine Learning*, ser. ICML '09, Montreal, Quebec, Canada: Association for Computing Machinery, 2009, pp. 689–696, ISBN: 9781605585161. DOI: 10.1145/1553374.1553463. [Online]. Available: https://doi.org/10.1145/1553374.1553463.

[14] Chen, Yang, Trappe, and Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Transactions on Vehicular Technology*, 2010.

[15] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," *2010 Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010)*, 2010.

[16] H. Kuehne, H. Jhuang, E. Garrote, T. Poggio, and T. Serre, "Hmdb: A large video database for human motion recognition," in *2011 International Conference on Computer Vision*, 2011, pp. 2556–2563. DOI: 10.1109/ICCV.2011.6126543.

[17] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," *2011 - MILCOM 2011 Military Communications Conference*, 2012.

[18] I. Ali and S. Sabir, "Internet of things security, device authentication and access control: A review," *International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016*, 2016.

[19] J. Fan, J. Lv, and L. Qi, "A selective overview of feature screening for ultrahigh-dimensional data," *Science China Mathematics*, vol. 59, no. 7, pp. 1345–1364, 2016. DOI: 10.1007/s11425-015-5062-9. [Online]. Available: https://link.springer.com/article/10.1007/s11425-015-5062-9.

[20] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "Phy-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Transactions on Vehicular Technology*, 2016.

[21] L. Xiao, Y. Li, G. Liu, Q. Li, and W. Zhuang, "Spoofing detection with reinforcement learning in wireless networks," *2015 IEEE Global Communications Conference (GLOBECOM)*, 2016.

[22] A. Mahmood, W. Aman, M. O. Iqbal, M. M. U. Rahman, and Q. H. Abbasi, "Channel impulse response-based distributed physical layer authentication," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–5. DOI: 10.1109/VTCSpring.2017.8108524.

[23] N. Wang, T. Jiang, S. Lv, and L. Xiao, "Physical-layer authentication based on extreme learning machine," *IEEE Communications Letters*, 2017.

[24] Q. Wang, "A novel physical layer assisted authentication scheme for mobile wireless sensor networks," *Sensors*, vol. 17, no. 2, 2017, ISSN: 1424-8220. [Online]. Available: https://www.mdpi.com/1424-8220/17/2/289.

[25] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (iot) authentication schemes," *Sensors*, vol. 19, no. 5, 2019, ISSN: 1424-8220. DOI: 10.3390/s19051141. [Online]. Available: https://www.mdpi.com/1424-8220/19/5/1141.

[26] J. Yoon, Y. Lee, and E. Hwang, "Machine learning-based physical layer authentication using neighborhood component analysis in mimo wireless communications," *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, 2019.

[27] Z. Zeng, S. Liu, and L. Wang, "Uwb nlos identification with feature combination selection based on genetic algorithm," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1–5. DOI: 10.1109/ICCE.2019.8662065.

[28] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *Journal of Communications and Information Networks*, vol. 5, no. 3, pp. 237–264, 2020. DOI: 10.23919/JCIN.2020.9200889.

[29] X. Qiu, J. Dai, and M. Hayes, "A learning approach for physical layer authentication using adaptive neural network," *IEEE Access*, vol. 8, pp. 26 139–26 149, 2020. DOI: 10.1109/ACCESS.2020.2971260.

[30] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity and confidentiality," *ArXiv*, vol. abs/2001.07153, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:210838914.

[31] P. Walther, R. Knauer, and T. Strufe, *Ultra-wideband channel state information and localization for physical layer security*, 2021. DOI: 10.21227/0wej-bc28. [Online]. Available: https://dx.doi.org/10.21227/0wej-bc28.

[32] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys Tutorials*, vol. 23, no. 1, pp. 282–310, 2021. DOI: 10.1109/COMST.2020.3042188.

[33] M. Abdrabou and T. A. Gulliver, "Adaptive physical layer authentication using machine learning with antenna diversity," *IEEE Transactions on Communications*, 2022.

[34] M. Abdrabou and T. A. Gulliver, "Physical layer authentication for satellite communication systems using machine learning," *IEEE Open Journal of the Communications Society*, vol. PP, no. 99, pp. 1–1, Jan. 2022. DOI: 10.1109/OJCOMS.2022.3225846. [Online]. Available: https://www.researchgate.net/publication/365941734_Physical_Layer_Authentication_for_Satellite_Communication_Systems_using_Machine_Learning.

[35] A. Kumar, C. Ottaviani, S. S. Gill, and R. Buyya, "Securing the future internet of things with post-quantum cryptography," *SECURITY AND PRIVACY*, vol. 5, no. 2, e200, 2022. DOI: https://doi.org/10.1002/spy2.200. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/spy2.200. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.200.

[36] P. Walther, "Towards practical and secure channel impulse response-based physical layer key generation," Ph.D. dissertation, Dresden University of Technology, Germany, 2022. [Online]. Available: https://nbn-resolving.org/urn:nbn:de:bsz:14-qucosa2-771959.

[37] S. Zeng, Y. Chen, X. Li, J. Zhu, Y. Shen, and N. Shiratori, "Visibility graph entropy based radiometric feature for physical layer identification," *Ad Hoc Networks*, vol. 127, p. 102 780, 2022, ISSN: 1570-8705. DOI: https://doi.org/10.1016/j.adhoc.2022.102780. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870522000014.

[38] L. Alhoraibi, D. Alghazzawi, R. Alhebshi, and O. B. J. Rabie, "Physical layer authentication in wireless networks-based machine learning approaches," *Sensors*, vol. 23, no. 4, 2023, ISSN: 1424-8220. DOI: 10.3390/s23041814. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/1814.

[39] W. Aman, S. Al-Kuwari, and M. Qaraqe, "Location-based physical layer authentication in underwater acoustic communication networks," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, 2023, pp. 1–6. DOI: 10.1109/VTC2023-Spring57618.2023.10199682.

[40] L. Das, R. Raman Chandan, P. Kaur, A. Singh, A. Rana, and B. D. Shivhare, "Advancements in wireless network technologies for enabling the (iot): A comprehensive review," in *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, vol. 6, 2023, pp. 807–814. DOI: 10.1109/IC3I59117.2023.10397952.

[41] L. Yang, S. Naser, A. Shami, S. Muhaidat, L. Ong, and m. Debbah, "Towards zero touch networks: Cross-layer automated security solutions for 6g wireless networks," Aug. 2023. DOI: 10.36227/techrxiv.23971707.v1.

[42] M. Abdrabou and T. A. Gulliver, "Secure authentication in mimo systems: Exploring physical limits," *Frontiers in Communications and Networks*, vol. 5, 2024, ISSN: 2673-530X. DOI: 10.3389/frcmn.2024.1370496. [Online]. Available: https://www.frontiersin.org/journals/communications-and-networks/articles/10.3389/frcmn.2024.1370496.

[43] Wikipedia contributors, *Sybil attack — Wikipedia, the free encyclopedia*, [Online; accessed 26-January-2025], 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Sybil_attack&oldid=1252547148.