

Sarika Gahlawat

Investigation of RF Fingerprinting approaches in GNSS

Faculty of Information Technology
Master's thesis
May 2020

Abstract

Sarika Gahlawat: Investigation of RF Fingerprinting approaches in GNSS

Master's thesis

Tampere University

Master's Degree Programme in Information Technology

May 2020

Major: Communication Systems and Networks

Supervisors: Elena Simona Lohan and Helena Leppäkoski

With the increase of emerging technologies, demand for location and positioning services is increasing in all domains of life. Currently there is an imperative need to protect and safeguard the authenticity and integrity of user data.

In this thesis work Radio Frequency Fingerprinting (RFF) approaches are investigated in the context of Global Navigation Satellite System (GNSS) as the demand for authentication in location related data is increasing. The idea here is to exploit unique features that a device possesses[40]. It is very difficult to impersonate a specific device as the device uses certain linear and non-linear components which are unique. The devices made by the exact same manufacturer are also not exactly similar because of the nature of non-linear components used in making of the devices. The purpose of this thesis work is to identify relevant features in GNSS signals at sampled domain (baseband or Intermediate Frequency (IF)) that can distinguish satellites on the sky, detect multipath, etc. The features that are addressed and studied in this work can be described as the features for identifying the source.

We introduce different features and then convert the time series data signal into images by using frequency transforms. The images are then fed to machine learning algorithms. MATLAB was used for simulating this model. The images are then used as an input to the Machine Learning Algorithms (MLA) to study various device specific features. Once the features are identified, feature classification methods are applied to classify the transmitters in GNSS. The goal is to identify 3-5 top features and apply a classifier to classify the different transmitter devices.

It was found out that the spectrogram and wavelet transforms applied on raw I/Q GNSS data in combination with Support Vector Machine (SVM) and Convolutional Neural Networks (CNN) gave promising results in terms of RFF. Spectrogram was the best one out of all transforms at both low and high ranges of Carrier to Noise Ratio to achieve fingerprinting in Global Navigation Satellite System.

Keywords: RF fingerprinting, discrete wavelet method, continuous wavelet, spectrogram, spoofing, features, SVM, CNN, classifier, GNSS.

The originality of this thesis has been checked using the Turnitin Originality Check service.

Preface

First of all, I would like to thank my professors Elena Simona Lohan and Helena Leppäkoski for guiding and encouraging me throughout this research work. They gave me timely feedbacks and were very patient with me.

For me it was a completely new experience of doing a research work and following the research based approach. I convey my gratitude to Tampere University and communication faculty for providing me with best possible resources and ecosystem for my thesis work to get timely accomplished.

My special thanks to research students Ruben Morales Ferre, Nachiket Aiyer, Islam Tanash, Niloofar Okati and my fellow mates for their constant support and motivation.

Last but not the least, I would dedicate this work to my whole family who supported me till the end.

Tampere, May 2020

Sarika Gahlawat

List of Abbreviations

AIWB	Axial Integrated Wiger Bispectrum
ARP	Address Resolution Protocol
AWGN	Additive White Gaussian Noise
BoF	Bag of Features
BoW	Bag of Words
CDMA	Code Division Multiple Access
CNN	Convolutional Neural Networks
CNR	Carrier to Noise Ratio
CWT	Continuous Wavelet
DNS	Domain Name Server
DSSS	Direct Sequence Spread Spectrum
DWT	Discrete Wavelet
FEA	Forward Estimation Attack
GEO	Geostationary Orbits
GLONASS	GLOBAL NAVIGATION Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HDL	Hardware Description Language
IEEE	Institute of Electrical and Electronics Engineers
IGSO	Inclined Geosynchronous Orbits
IIP3	Third Order Input Intercept Point
IMEI	International Mobile Station Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
kNN	k Nearest Neighbor
KPCA	Kernel Principal Component Analysis
LAN	Local Area Network
LDC	Linear Discriminant Classifiers
LO	Local Oscillator
LoRa	Low Range
MAC	Medium Access Control
MEO	Medium Earth orbits
MLA	Machine Learning Algorithms
MSCNN	Multisampling Convolutional Neural Network

NLOS	Non-Line-of-Sight
NMA	Navigation Message Authentication
OSI	Open Systems Interconnection
PA	Power Amplifier
PCA	Principal Component Analysis
PNN	Probabilistic Neural Network
QDC	Quadratic Discriminant Classifiers
RAIM	Receiver Autonomous Integrity Monitoring
ReLU	Rectified Linear Unit
RF	Radio Frequency
RFF	Radio Frequency Fingerprinting
RFID	Radio-Frequency Identification Tags
ROI	Region of Interest
RPCA	Robust Principal Component Analysis
SCER	Security Code Estimation and Replay
SDR	Software Defined Radio
SMA	State Modeling Attack
SNR	Signal to Noise Ratio
SVM	Support Vector Machine
TESLA	Timed Efficient Stream Loss Tolerant Authentication
USRP	Universal Software Radio Peripheral
WLAN	Wireless Local Area Network

Contents

List of Abbreviations	
1 Introduction	1
1.1 State of the Art	1
1.2 Thesis Goals	3
1.3 Author Contribution	5
1.4 Thesis Structure	6
2 Overview and Background of GNSS	7
2.1 What is GNSS	7
2.2 GNSS Receiver Functioning	8
2.3 Vulnerabilities in GNSS signals	10
2.4 Types of interference in GNSS	11
2.5 Interference management solutions	12
2.6 Ways to Improve Localization/Positioning in GNSS	13
3 Spoofing	15
3.1 Types of Spoofing	16
3.2 Complexities Involved in Spoofing	17
3.3 Spoofing Countermeasures	18
4 RF Fingerprinting	20
4.1 Feature Selection and Classification	20
4.2 Fingerprinting method used	23
5 Machine Learning Algorithms	26
5.1 SVM	26
5.2 CNN	27
6 Simulation Approach	29
6.1 Feature Ranking and Selection Using DWT	32
6.2 Fingerprinting with two transforms in low CNR range	35
6.3 Fingerprinting with three transforms in high CNR range	37
6.4 Additional Simulations	39
6.5 Notes on the simulation environment	40
7 Design Recommendations	41
8 Conclusion	42
Bibliography	44

List of Tables

1.1	Current studies and work in RFF	4
2.1	Comparison of GNSS Characteristics	9
6.1	Summary of Input Parameters Used	30
6.2	Far non-linearity coefficients	30
6.3	Near non-linearity coefficients	30
6.4	IQ Imbalance Values for 3 classes	31
6.5	Phase Noise Values for 3 classes	31
6.6	Input Parameters Used for Simulation	32
6.7	Input Parameter changes for phase 2	35
6.8	Input Parameter used for phase 3	37

List of Figures

2.1	Basic GNSS Receiver block diagram	10
2.2	Types of Interferences	11
2.3	Stages for tackling Interference Management in a GNSS Receiver[26]	13
4.1	Fingerprinting Approach	22
4.2	RF Fingerprinting Classification	23
4.3	RF Fingerprinting Methodology	24
4.4	Sources of RF impairments in transceiver	25
5.1	Confusion Matrix	27
5.2	CNN Architecture	28
6.1	DWT types performance with SVM	33
6.2	Results for feature combinations	33
6.3	DWT(db1) Results for (50-100 dB)	34
6.4	Classifier results for Far Non-linearity Case	35
6.5	Classifier results for Near Non-lineairty Case	36
6.6	Classifier results for Far Non-linearity Case(high CNR)	38
6.7	Classifier results for Near Nonlineairty Case(high CNR)	38
6.8	Simulation results comparison with reference case of figure 6.7	39

1 Introduction

1.1 State of the Art

Authentication of data and secrecy is gaining attention globally as more and more people use mobile phones, location services and have privacy preferences. Organizations worldwide have critical information and their data needs to be safeguarded as the data may have secret information of clients using the services. People always have their preferences about sharing their location as various applications ask for it, as it is a privacy issue also. With new emerging applications of location and position based services lot of new opportunities open up for researchers in this field. In one of the studies its shown in detail how user preferences can affect the future GNSS industry and its market share [20].

Authentication between two parties is achieved by utilizing common measures of secrecy agreed by the two parties which are difficult for the third party to reproduce. Fingerprinting is a countermeasure which works to provide extended security and protection from illegitimate access by a third party [40]. The current emerging technology applications such as smart cities, Internet of things, military applications, mission critical situations require high bandwidth and have high security concerns which also face authentication problems. In the Software Defined Radio (SDR) technology, we can model the functional blocks of the processing chain and make use of it to study and identify a specific device.

There are many features at the physical layer, Medium Access Control (MAC) layer as well as upper layers which can be used for fingerprinting [43]. Some of those are IP and MAC addresses, International Mobile Station Equipment Identity (IMEI) numbers. The reason they are not suitable for fingerprinting is that they can be easily spoofed.

The RFF features can broadly be divided into transient-state features and steady-state features. Capturing transient signals is very hard, therefore, their application is also limited. Whereas the steady-state signals are longer in duration, and easy to capture, thereby, more practical to study [17].

Features such as the strength of a radio signal and information of the channel undergo continuous changes over a noisy and multipath channel and, therefore, not easy to capture and study. A device has many smaller components and multiple features, so deciding the right set of features for identification is very challenging.

The challenges are at the receiver end to identify the devices, as the signals are coming from various devices at any point in time. Every device has its own signatures and it is primarily because of the various non-linear components used. The non-linearity is because of the power amplifiers, resistors and transistor components for example. Over a noisy wireless channel these are the only features about a device which do not change and cannot be replicated easily, and that is why they are good for identifying the devices as they are hardware specific.

Over the past decade, with the increasing usage of location-based services, some methods have been employed to achieve fingerprinting in devices at various stages of correlation. RFF extraction is a technology that can identify a unique radio device for example; a transmitter at the physical level, using only external feature measurements which match the feature library. Extraction of the features of the transmission signals that are transmitted from different wireless devices play a significant role in RFF. RFF is the reflection of differences between hardware components of radio devices, and it contains non-linear characteristics of internal components within the radio devices. RFF techniques are being explored for enhancing the security of radio frequency communication, for example, one such proposed method explains the fingerprinting method by using permutational entropy [9].

An approach to radio frequency fingerprinting is explained in its entirety in [22]. It is explained that cryptographic keys are inefficient in IoT networks, and that the default keys can be brute-forced by attackers at the interception stage itself. MAC address id fields require extra power resources for preserving the ID number, which is difficult to achieve in IoT devices as they already have power limitation. Thereby, a passive approach of RFF is being considered. RFF features are difficult to impersonate as they are specific to a device. The results for high Signal to Noise Ratio (SNR) are promising but this work is primarily focussing on devices which consume low power (for SNR less than 10dB). A journal where different transmitters are identified using pattern mining algorithms, wherein time domain approach, permutational entropy method and spectrum method based approach along with k Nearest Neighbor (kNN) is explained very nicely in [21]. Clock derived metrics used for identification of transmitters from different manufacturers is explained in [5].

Wavelet method is used in [19] at the physical layer of the Open Systems Interconnection (OSI) model. The intention is to provide safety against unauthorised access. RFF features are extracted and after a reliable detection, the challenge is to look for robust fingerprint features in order to improve device recognition. Apart from that, it helps to understand why wavelets are useful for fingerprinting approach. An information theory approach is being studied to understand basic performance

limits of RFF [12].

Apart from these there is literature material which exploits the RFF extraction based on transient-based implementations, where classification is done on the basis of amplitude/phase of signal envelope [40] and modulation-based implementations [30]. Radio Frequency (RF) oscillator also is an important component which introduces non-linearities, a device identification method using fingerprinting is explained in [32]. The current work in this domain is summarised briefly in table 1.1 explaining the RFF methodology used, which classifiers are used and in which fields the method is being proposed.

RFF is a promising field and is being explored to enhance security as well as authenticity of a device. However, it has its own challenges such as:

1. No prior knowledge of fingerprints of a legitimate device.
2. Computational complexities.
3. Basis of selecting robust features.
4. After selection of right features, choosing the right combination of features can be difficult [43].
5. Collection of huge datasets of various devices in different scenarios including both indoor and outdoor locations while taking into consideration environmental conditions and multipath scenarios.
6. Since most of the studies are carried out in controlled manner, and simulations are mostly carried out on available data, it may lack traces of malicious sources, and hence the challenge still persists.

The challenges are presented and described in the journals in more detail [43], [35], [31].

1.2 Thesis Goals

The idea behind this thesis work is to investigate the fingerprinting approach in GNSS signals by identifying some device specific features (also called patterns) over varying CNR's in a controlled environment, so that the features can help in identifying a transmitter device. Once the feature or pattern is identified in the sampled baseband domain, it is used as a signature to identify the devices. The features that are addressed and studied in this work can be described as the features for identifying the source. The expectation is to find a combination of sensible channel

Table 1.1 *Current studies and work in RFF*

SNo	RFF Method	Classifier	Used where	Reference (citation)
1.	Axial Integrated Wigner bispectrum	SVM	GNSS	[38]
2.	Frequency domain analysis	kNN	USRP	[17]
3.	Probabilistic fingerprinting	Uses Probabilistic fingerprinting formulae more efficiently and avoids accuracy detriment	WiFi based indoor positioning	[3]
4.	Raw I/Q samples	CNN	RF chain SDR	[33]
5.	Wavelet method and HDL	LDC, QDC, kNN and SVM	RFID	[2] [14]
6.	Positioning algorithm by weighted fusion	Euclidean distance based WKNN algorithm	IoT	[10]
7.	RFF characteristics	PNN	IEEE 802.11b (WiFi)	[40]
8.	Wavelet coefficients, ReliefF and PCA	SVM	RF Devices	[22]
9.	Dimensional reduction methods PCA, RPCA and KPCA	SVM, Artificial neural networks and Grey correlation analysis	Intrusion detection in wireless devices	[23]
10.	Selected ROI	MSCNN	Zigbee Devices	[45]
11.	Pattern mining algorithms	kNN	Wireless device Identification	[21]
12.	Physical layer fingerprinting	Supervised and zero-shot learning	LoRa devices	[34]

parameters, carrier to noise ratio, and device parameters which can help in identifying the correct device.

Our primary aim here is to select those features which do not change as the GNSS signals travel over long distance and changing multipath and harsh environmental conditions. It is very important that the selected features be robust and do not change with varying environmental conditions.

MATLAB was used for performing the simulations. The images were then fed to the Machine Learning Algorithms (MLA) to study various device specific features. Once the features are identified, feature classification methods are applied to classify the transmitters in GNSS. The goal was to identify forge resistant features and apply a classifier to classify the different transmitter devices. For this thesis work supervised learning approach was used. This type of work involves big collection of labeled samples for training the MLA.

1.3 Author Contribution

To achieve fingerprinting we start by introducing various features at pre-correlator stage in an RF chain. After introducing different features the time series data signal was converted into images by using various frequency transforms. We are using the wavelet method to extract features as there have been some good work in the past using the wavelet method [1, 19, 2, 22]. The wavelet feature extraction method is general for any time-domain signal, and the classification results can be improved by features drawn for the particular domain. The success of this technique has shown to achieve high accuracy in past researches [1]. The wavelets used were Discrete Wavelet, Continuous Wavelet and spectrogram.

Once the features are identified, feature classification methods are applied to classify various transmitter devices in GNSS. For this approach we use machine learning techniques like SVM and CNN. The reason for using them is because of their performance as explained in [33]. Classifiers are selected based on their performance. The goal is to identify 3-5 top features and apply a classifier to classify the measurement data.

In this thesis work we investigate the fingerprinting approach in MATLAB and MLA to see if the method works to some extent. It is important to note here that a trade-off is an important consideration for evaluation, for example, if we deteriorate the channel conditions too much we may not be able to see promising results, however in reality channel is never ideal and always keeps changing. It is evident from the results of the measurement subsections 6.3 and 6.4 that the overall performance of

all three transforms improved as Carrier to Noise Ratio (CNR) range was increased. After the simulations and analysis of results design recommendations are given in section 7.

1.4 Thesis Structure

The chapters in the thesis cover following topics:

1. **Chapter 1** explains introduction, state of art, thesis goals and author contribution.
2. **Chapter 2** covers GNSS, its working, vulnerabilities of the signal, interferences and their management in GNSS.
3. In **Chapter 3** we explain Spoofing, how easy or difficult it is to spoof, types of spoofing in GNSS and measures that can be taken to safeguard from spoofing.
4. **Chapter 4** covers RF fingerprinting, features, their extraction, classification and the methods used in the thesis work for extracting features.
5. **Chapter 5** explains in short about the MLA used in fingerprinting method.
6. **Chapter 6** the results of the phasewise simulations and simulation environment are described.
7. **Chapter 7** is about design recommendations.
8. **Chapter 8** discusses about conclusion.

2 Overview and Background of GNSS

Location services are catching a lot of attention over the past two decades. They are becoming a topic of concern and area of interest for a lot of research students and companies all over the world. Here, we present a brief background of the existing systems in the GNSS. The existing systems are explained in short with some comparisons and then a description of the GNSS signal. Thereafter, the working of a typical GNSS receiver is explained. Since the GNSS signal is very weak, a short section is there to explain the vulnerabilities of these signals. The positioning methods are subject to errors because of noise and multipath effects, measurement procedures used, offsets because of clock timings and atmospheric changes as the signals travel through ionosphere.

2.1 What is GNSS

Global Navigation Satellite System (GNSS) is a constellation of satellites which provides signals from space and transmits positioning and timing data to receivers. The receivers are also known as GNSS receivers. The receivers then use this data to determine location and provide positioning services. GNSS is widely used for many applications which include military and financial services, and people of all age groups are heavily dependent on the positioning, timing and navigational services provided by GNSS all over the globe. However, many factors affect service quality of a GNSS signal. Such parameters can be natural as well as intentional. The interference results in great losses to many systems and networks.

The currently available GNSS have lot of similarities. The new modulation techniques help in minimizing the interference in the same frequency band. Besides the similarities each system is different in its own way.

The table 2.1 shows some details for the current GNSS including planned number of satellites, orbital information, frequency bands, etc. BeiDou signals kept changing during the three phases (Phase 1, Phase 2, Phase 3), some keep making new additions while some are being eliminated. Hence, they are described here after their full operational ability is achieved.

The current GNSS systems are explained in brief:

1. **GPS:** The Global Positioning System (GPS), also known by the name NAVSTAR GPS, is a satellite-based navigation system which is owned by the United States government and is used primarily by the United States Air Force. It

gives geolocation and time information to a GPS receiver anywhere on the Earth where there is an unobstructed line of sight to four or more GPS satellites. The GPS furnishes critical positioning capabilities for defense as well as commercial users around the world, its maintained by the United States government. The GPS is free for use by anyone and doesnt require telephone or internet and thus enhances the positioning information. The GPS project was started by the U.S. Department of Defense in 1973.

2. **GLONASS:** GLObal NAVigation Satellite System (GLONASS) is a space based satellite navigation system and is comparable in precision to GPS. After GLONASS the positioning services have improved in high latitudes, which was not the case with GPS. It was started by Russia in 1976 and has come a long way since then. The fully operational constellation consists of 24 satellites. For an exact position the object should be in range of atleast 4 satellites.
3. **Galileo:** Galileo is the global navigation satellite system created by the European Union. The main aim behind it is to provide a high precision positioning system so that they dont have any dependency on GPS or GLONASS. The use of low precision services is free for everyone, whereas the high-precision capabilities are available for those ready to pay more and have commercial needs. Galileo provides horizontal and vertical position measurements within one metre precision, and improved positioning services at high latitudes also. Galileo offers Navigation Message Authentication (NMA) as a protection against spoofing attacks [7]. NMA is a cryptographic mechanism that protects the integrity and authenticicty of a GNSS navigation message. A very dynamic NMA scheme is achieved after a compromise between security, communication load, robustness to channel interferences, as well as available receiver resources [7, 42].
4. **BeiDou 2:** BeiDou is a chinese navigation system.The first generation of this navigation system had only three satellites which had limited coverage capability for chinese users and neighbouring areas. In 2015, China launched the third generation BeiDou system (BeiDou-3) for global coverage constellation. BeiDou-3 will be having 35 satellites and is expected to provide global services after completion in 2020.

2.2 GNSS Receiver Functioning

To estimate the position, a GNSS receiver has to search and then acquire the signal from the visible satellites and later decode the ephemeris data from the signals for

Table 2.1 Comparison of GNSS Characteristics

Characterstics	GPS	Galileo	Glonass	BeiDou
Number of planned satellites	31	27 + 3(spare)	27	35
Number of orbital planes	6	3	3	3(MEO) 3(IGSO) 1(GEO)
Orbital altitude (km)	20200	23222	19100	21500(MEO) 35800(IGSO) 35800(GEO)
Orbital inclination (degrees)	55	56	64.8	55 (MEO and IGSO)
Frequency bands	L1, L2 and L5	E1, E6 E5, E5a and E5b	L1, L2 and L3	B1, B2 B3
Signal spreading	DSSS	DSSS	DSSS	DSSS
Multiple access scheme	CDMA	CDMA	FDMA and CDMA	CDMA
PRN codes length for open signals	1023 10230	4092 5115 10230	511 10230	2046

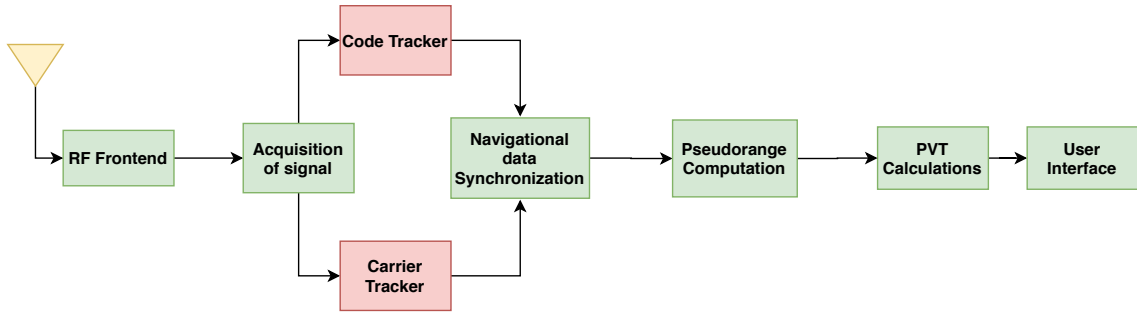
finding the position of satellites and measure pseudoranges. So, the receiver has many tasks which include acquiring the signal (acquisition and tracking function), while continuing to extract data and estimation of the final position. A basic block diagram of a GNSS receiver is shown in figure 2.1.

In the front end block the functions performed are amplification, filtering, frequency conversion and digitization of the signal. After digitization the signal is fed to the baseband processing unit where it goes through signal processing operations.

In the baseband preprocessing unit the first phase is of signal acquisition where the objective is to identify and detect satellites which are visible in the sky and to get estimation of the code phase and carrier frequency. After signal acquisition, tracking is performed in which the coarse estimates are improved and enhanced. The navigation unit then takes care of the position calculations.

2.2.1 Errors in GNSS

When the GNSS signals pass through tropics, they are subject to noise and errors. As the usage of GNSS is increasing day by day, the detection and mitigation of

Figure 2.1 Basic GNSS Receiver block diagram

errors is even more important to attain better accuracy, integrity and availability. A detailed explanation and means of reducing the errors is explained in [15, 16]. The errors in GNSS are of following types:

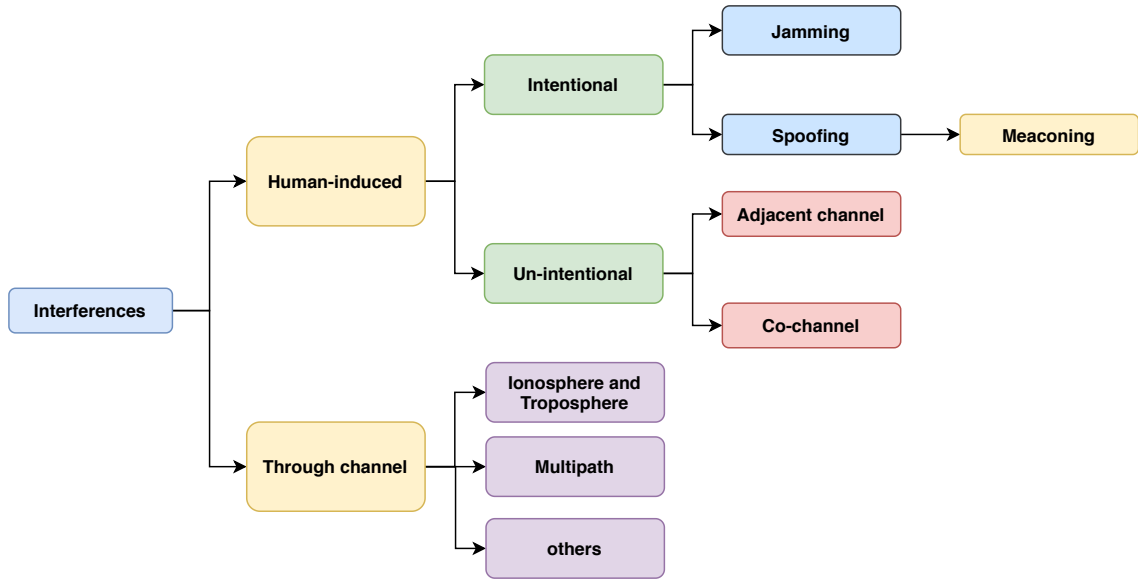
1. Clock error: The satellite clock errors appear when actual time cannot be synchronized with the satellite oscillator.
2. Ionospheric errors: Ionosphere has a huge concentration of ions and free electrons in the atmosphere. Free electrons and ions are produced by Ultra-violet light and x rays from the sun. The error is determined by the number of electrons that the signal will encounter during its path from the satellite to the receiver.
3. Multipath errors: When radio signals travel through buildings, mountain ranges, and other obstructions multipath errors are bound to occur. As the GPS signals have different wavelengths, multipath effect can cause error in signal at different levels.

Differential computations or measurements method is often used to correct the above errors. One receiver is taken as a reference and it does the main calculations which are then transmitted to other receivers over radio links and eliminate the errors in order to get proper range and position.

2.3 Vulnerabilities in GNSS signals

GNSS signals are highly vulnerable, and subject to losses because of natural and human induced interferences. The vulnerabilities are mentioned in good detail in [28]. The vulnerabilities are mainly because of the following reasons:

1. GNSS signal is of very low magnitude in strength, as mentioned in [28].
2. The GNSS signals travel through ionosphere and troposphere, which causes further attenuation in them.

Figure 2.2 Types of Interferences

3. The GNSS signals undergo microscopic errors, such as signal interferences (while passing through tunnels, canyons, buildings), multipath interferences, etc.

Locally generated noise signals can easily overpower the legitimate GNSS signals. At times the locking in the tracking device is lost because of genuine reasons, for example, a signal passing through a tunnel or heavily dense areas. This gives jammer's an opportunity to spoof the location of the actual device. A commonly employed method used for jamming is transmitting a chirping noise signal at a known frequency, which is the frequency of the GPS signal.

Jamming and spoofing are two terms which are used in the context of GNSS signals very frequently and interchangeably. Aircraft industry as well as vehicle applications are highly vulnerable to such threats [24, 28].

2.4 Types of interference in GNSS

GNSS signals undergo two types of interference. The first one is induced by humans and second one is because of the channel. The human induced interference can be intentional/deliberate or un-intentional/non-deliberate. Some of these are explained below in brief:

1. **Natural and Unintended:** Such interference is caused due to nature and because of their travel paths, like tropics, buildings, cloud absorptions, foliages, tunnel, mountain ranges, etc.

2. **Interference due to Multipath:** Sometimes there are chances that a receiver can pick up signals which are reflected (from building corner or edges for example), and if the reflected signal locks itself with the receiver it can cause positioning errors as the reflected signal is different from the direct signal.
3. **Spoofing:** Spoofing in GNSS is to 'fake' the receiver's position or to mislead the receiver to think as if it is placed somewhere else. Meaconing is a particular case of spoofing. In meaconing, the received signal is rebroadcasted on the same frequency after a delay to create a confusion in navigation. The rebroadcasting is usually done at higher power as compared to the original signal. The meaconing can be done by both analog and digital methods. This can be dangerous specially in aviation industry.
4. **Jamming:** Jamming is a method of disrupting or interfering with an authorized wireless communication channel. It can also be intentional or non intentional.

2.5 Interference management solutions

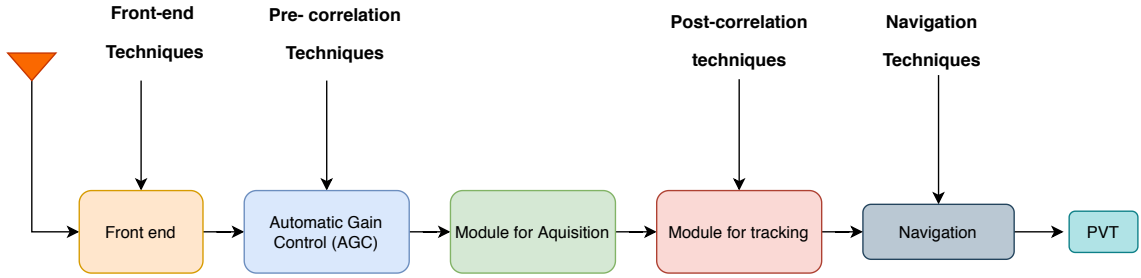
According to the receiver stages the interference management can be classified into different categories [26]. The categories are pre correlation and post correlation. The pre correlation method takes into account the RF and IF samples in the RF module and the samples are taken before or after the analog to digital converter. As compared to the pre correlation methods which are suited for detecting the interference, the post correlation methods are more suited for interference mitigation [24].

Another category for interference management is at system level and takes into consideration the pseudo ranges calculated by the receiver and on signals from multiple satellites. Some methods in this category are Sum of Squares Detector and Dispersion of Double Differences Detector methods.

The figure 2.3 explains briefly the stages of correlation and the stage where the interference management techniques [24] can be deployed:

1. **Link-level Approaches:** In this approach we focus on the front end, pre-correlation and post correlation, the RF and IF samples are fed to the algorithms.
2. **System-level Approaches:** Here, we take into account the navigational and other system-level approaches and take into consideration the pseudorange and other information as an input to the algorithms for analysis of interference.

Figure 2.3 Stages for tackling Interference Management in a GNSS Receiver[26]



The front-end and pre-correlation techniques depend mainly on Radio frequency (RF) or Intermediate Frequency (IF) samples, before or after the Analog-to-Digital Converter (ADC) from the RF chain. Examples of such techniques include the Automatic Gain Control (AGC) detector and time and frequency power detectors.

The post-correlation techniques rely on the outputs of the tracking channel in a GNSS receiver and are typically more suited for interference mitigation than for interference detection. The last category of interference management methods are those at system-level or navigation domain, which are computed from the pseudo ranges computed by a GNSS receiver and from the signal arriving from multiple satellites on sky [24]. Some counter measures against interference in GNSS, have been identified in literature are [27]:

1. Detection and Mitigation: Here, the receiver is able to detect the presence of an interfering entity and has the capability to shut it down completely on a particular frequency.
2. Direction finding and localization method: In this case the position of the interfering entity can be estimated by the GNSS receiver and then the signals can be blocked from that specific direction.

There has been a large amount of research work so far regarding jamming detection, mitigation, and direction finding in GNSS bands. Some of them are [29, 4].

2.6 Ways to Improve Localization/Positioning in GNSS

Due to an increased demand for location-based services there is a need for developing accurate, efficient, and real-time localization techniques for both indoors and outdoors. GNSS is widely used for localization of a user equipment. In situations of blockage, multipath, building obstructions, cloud clutter and atmospheric disturbances the GNSS signals are highly attenuated and the localization performance gets deteriorated. There are various techniques employed these days for improving the accuracy of the localization and positioning techniques [44].

In the cellular and wireless Local Area Network (LAN) three kind of positioning methodologies are used, namely, lateration, angulation and fingerprint based algorithms.

For the **lateration-based algorithms**, the parameters taken into account are received signal strength indicator, reference signal received power, time of arrival and time difference of arrival of transmitted signals, are required to calculate the distances from multiple sites with known geographical locations to the GNSS receiver for estimation of the receiver's location.

The **angulation-based algorithms** localize the user equipment by estimating the angle of arrival of the signals received from at least two known sites. The lateration and angulation algorithms rely on the premise that a sufficient number of reference sites are available. The performance of these algorithms degrades significantly when the signals arrive at the user equipment from Non-Line-of-Sight (NLOS) and multipath paths, or when fading happens as it results in erroneous calculations at the receiver's end.

A third method called **Fingerprinting based algorithms** is employed wherein a training database is constructed and that database is used for estimation of precise location as well as identifying the right user equipment. The fingerprint is unique to each device and it provides a combination of values w.r.t a geographical location. The fingerprint can be images, acoustic waves, RF signals, etc.

3 Spoofing

Even after having protection by Navigation Message Authentication (NMA) the GNSS signals are still prone to attacks , which can affect the ranging/positioning information for a user. Spoofing is the act of disguising a communication from an unknown source as being from a known and trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an Internet Protocol (IP) address, Address Resolution Protocol (ARP), or Domain Name Server (DNS).

Spoofing can be used to gain access to a personal information, spreading malware through links and attachments, bypass network access controls, or redistribution of traffic. Spoofing is the means of gaining access in order to execute a cyber attack .

A spoofing attack on a government or private organization leads to an infected computer systems and networks, breach of data, and even loss of revenue which can affect the public image of the organization or country.

In addition to the above, wrong routing of internet traffic can lead customers/clients to malicious sites aimed at stealing their personal information like bank passwords or secret information in case of military.

Jamming is sometimes confused with Spoofing, but they are different. "Jamming is the act of intentionally directing powerful electromagnetic waves toward a victim receiver with the ultimate goal of denying its operations" [4]. There are jammers in single frequency as well as multiple frequencies which can affect several GNSS signals at the same time.

Jamming can affect the front end, acquisition as well as the tracking stages. There is literature material on jammer classification by using machine learning algorithms in very good detail [25].

Spoofing Attack: A spoofing attack is a situation in which a person or a program successfully identifies as another by falsifying data, to gain an illegitimate advantage. There can be many type of spoofing attacks in GNSS [7], for example,

1. Meaconing is the simplest attack (explained further)
2. Selective Delay for inducing a different positioning information from the spoofer antenna, it is also called Security Code Estimation and Replay (SCER).

3. Forward Estimation Attack (FEA) makes use of forward error correction mechanism.
4. Lastly, there is State Modeling Attack (SMA).

3.1 Types of Spoofing

Spoofing can be applied to a number of communication methods and can be at various levels of technical know-how to carry out phishing attacks, which are used for gaining sensitive information from individuals or organizations.

Types of Spoofing:

There are different mechanisms employed for spoofing of information and devices to gain access to secret information. For ex:email spoofing, caller-ID spoofing, website, ARP, DNS and IP spoofing to name a few. In context of GNSS we have following types of spoofing identified :

1. **Simplistic Spoofing:** Simplistic spoofing can be achieved by connecting a signal generator to an antenna but will not likely synchronize with the real satellite signal. For deceiving the receiver high power RF noise is first transmitted, it will unlock it from the genuine signal, it is then followed by the counterfeit signal with higher power than the actual signal. The simplistic spoofing is easy to detect because the loss of the locking and abnormally high SNR will alert the receiver.
2. **Intermediate Spoofing:** Here the attack is via a receiver-spoofers, which has a GNSS receiver and a signal generator. The receiver tracks satellite signals for accurate synchronization with the satellite time and emphasis with estimates of the Doppler frequencies and code phases of every satellite signal tracked by the victim receiver. Thereafter, signal generator uses this information to generate counterfeit signals synchronized to the actual signal. The receiver-spoofers adjusts the code phase and the carrier frequency of the fake signal to align with the genuine signal and then increases the power a little to control the correlation peak so as to lead the correlation peak away from the genuine peak. This kind of spoofing can mislead the receiver without breaking the tracking state, and is hard to detect by receivers except in the case of multi-antenna receivers. A detection mechanism for detecting intermediate spoofing in GNSS using slope based metrics is explained here [18].
3. **Sophisticated Spoofing:** Sophisticated spoofing is somewhat similar to the intermediate spoofing but it requires additional equipments for synchronization with transmitting signals with a coordinated carrier phase, and can even

deceive multi-antenna receivers. Sophisticated attacks are very expensive and not been so successful so far.

3.2 Complexities Involved in Spoofing

There are a hoard of difficulties and challenges involved in spoofing at a practical level. Spoofing requires huge complexities and intelligence on the attacker's side and sometimes targets like mobile phones and personal devices are not even too lucrative as compared to bigger targets like ships, planes and big power stations which are more genuine targets. Spoofing hence requires lot of sophistication and intelligence. There are following practical challenges in spoofing:

1. Labour and Expenses:

- (a) Simulator Device Costs: Analog simulator devices are very expensive as compared to their digital counterparts. Digital simulators can broadcast at multiple frequencies. In case of digital simulators huge costs are incurred on software needed to run those simulators.
- (b) Meaconing Cost: Not too many options are available as of now on this.
- (c) Intermediate Level Spoofer Costs: The amount of expertise and costs needed are huge here. In one of the surveys of Humphrey's it took "four Ph.D. students several years" [36] .

2. **GNSS Device Information:** For performing a successful spoofing operation, the exact make and model information about a GNSS receiver device or equipment is a must apart from its exact location.

3. **Moving targets:** The following equation where P_t is the transmitted power, P_r is the received power and d the distance between transmit and receive antennas.

$$P_t = \frac{P_r}{4\pi d^2} \quad (3.1)$$

When the distance between the spoofer and the target starts varying the received signal power P_r varies even more with the d^2 term. So, with the varying distance and moving targets the spoofer will have further challenge to keep maintaining a locked state with the receiver. It can go out of sync any time.

4. **Need for Multiple Simulators:** In order to have a successful spoofing attack against many navigational receivers, would require multiple intermediate spoofers which are located close to the target. It, therefore increases the logistics as explained in [36] .

5. **Attacking Speed:** While performing experiments in laboratory a spoofing attack can be modified by adjusting the speed of the attack, whereas in real situations the type of receiver that is being attacked is completely unknown and there is no feedback to modify it [36]. Variations of speed affect the position solution in a big way.

All in all GNSS spoofing is still a nascent type of threat and is still evolving to show its presence in real life situations. However, it poses significant threats for shipping, smart grids power systems, lesser for criminal tags and train control systems and some residual threat towards the growing mobile phone infrastructure. It is hard to carry out GNSS spoofing but the cases of GNSS low cost jamming are eventually rising.

3.3 Spoofing Countermeasures

The following measures [36] are taken to prevent spoofing. They are explained in brief:

1. **Signal processing defenses:** If we look at figure 2.3 the signal processing defense approaches are applied at pre-correlator and post correlator stages. Some common methods used in this approach are discussed below.
The first one Receiver Autonomous Integrity Monitoring (RAIM) is applied at the navigational level while the remaining are applied at the post correlator stage.
 - (a) Receiver autonomous integrity monitoring(RAIM): this method checks the GNSS signals for spatial consistency and removes all erroneous satellites.
 - (b) Signal to Interference plus noise ratio
 - (c) Absolute Power: In this method the power of the received signal strength is monitored with the expected signal strength.
 - (d) Doppler Shift detection: Because of the different orbital speeds of the receivers with respect to the satellites the Doppler effect comes into play which takes into account the shortening of wavelengths when they move away.
 - (e) Correlation peak monitoring
 - (f) Clock Bias monitoring
2. **Cryptographic defense [11]:** This method has been proposed by some but is not feasible as adding encryption to public protocols may not be a feasible

solution. Some methods used in this category are discussed below.

The cryptographic defense is applied at the navigational stage.

- (a) Spreading Code Encryption
 - (b) NMA: In this method a robust error correction mechanism is very important.
 - (c) Timed Efficient Stream Loss Tolerant Authentication (TESLA) based authentication [11]: Timed efficient Stream loss Tolerant Authentication, uses a delayed key disclosure scheme.
3. **Radio spectrum and antenna defense:** The biggest benefit of antenna defense is that they are immune to attacks from software and are quite resistant to spoofing and are hence utilised for improving security of GNSS receivers.
 4. **RF Fingerprinting Method:** RFF is still in a nascent stage and has its own challenges but offers promising results. Device identification is becoming increasingly important because increasing use of mobile phone and other Internet of Things (IoT) devices applied with many wireless standards, for example, Zigbee, Bluetooth, UMTS, GSM, Wireless Local Area Network (WLAN) standards such as 802.11a, 802.11b, and 802.11n, etc.

Fingerprinting of electronic devices is often based on imperfections such as the errors generated by the Local Oscillator (LO), Power Amplifier (PA), analog to digital converters, etc of the device. Radio frequency fingerprinting technique identifies the device or signaler from which a radio transmission originated by looking at the properties of its transmission, including radio frequencies. Each signal originator has its own specific "fingerprints" based on the location and configuration of its transmitted signals. It is a mechanism used as a means of increasing the security of wireless networks. The RF signal from a transmitter has a transient behavior with respect to instantaneous frequency and amplitude. We are going to investigate this method here next in detail.

4 RF Fingerprinting

What is RFF ?

Just like we each have unique fingerprints, radio transmitters also have different radio frequency fingerprints, namely, RF fingerprints. The RF fingerprints hence come from differences between hardware components of transmitters, and the differences can be reflected in communication signals having a unique pattern. The fingerprints can be extracted by processing transient signal [12] or steady-state signal from received RF signals. Its difficult to extract features from transient signal, thereby steady state signal is more useful for extracting features as they are more reliable.

Transient signal behavior is because of various reasons, for example modulator subsystems, local oscillators and RF amplifiers. The timing of the transient behavior keeps changing, and depends on the make and model of the transmitter device. There are differences even for transmitters of the same type and manufacturer, because of the tolerances at the time of manufacturing and the aging of the components like diodes, transistors, resistors and other electronic devices, etc. The unique transient signal behavior is called the RF fingerprint of a device (for ex: transmitter here) and is used for identification of the transmitter.

The RF fingerprints primarily work in physical layer within transmission devices, so they cannot be destroyed or copied and are hence unique for every device [9].

The method for obtaining transmitter hardware characteristics is called **RF fingerprint extraction**, and the method used for identification of individual transmitter with fingerprints is called RF fingerprint identification. A detailed work using this methodology by using Axial Integrated Wiger Bispectrum (AIWB) in GNSS is explained in [38]. The others are also listed in table 1.1. Next step is identification of features used for RFF method.

4.1 Feature Selection and Classification

4.1.1 What is a Feature ?

The measurable properties of a process can be identified as features. There can be millions of features which can be recognized in a process/device. Several techniques are being developed to address the problem of reducing irrelevant and redundant variables.

4.1.2 Feature Selection

Feature Selection is a way to eliminate the variables. The main idea behind feature selection is to choose a subset of variables from the incoming data, such that it can be described by using these variables and reduces the effect of noise and irrelevant variables. The dependent variables sometimes do not give any extra information about the classes and act as a noise in prediction. So by removing the dependent variables extra data is removed and that improves the classifier performance.

By using feature selection techniques we gain more information about the process under study which improves the predictor performance. The purpose is to have complete information about the input by using fewer variables. It helps to understand complex data, reduces computational requirements, reduces the dimensions of data and further helps in enhancing the predictor performance [8]. Whenever we decide to select some features for device fingerprinting, the features should meet the following two criteria which are also explained in the studies [43], [6], and [5]:

1. The features must be difficult to counterfeit or fake.
2. The features should not change with respect to changes in environmental conditions.

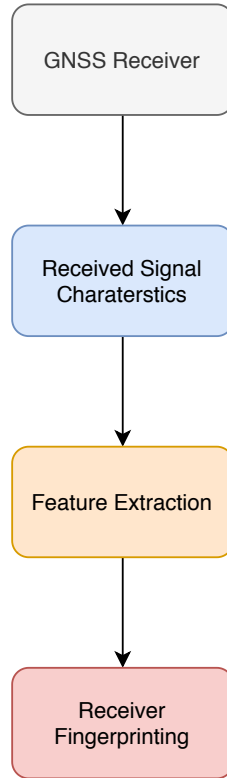
In the figure 4.1 we can see a very basic approach being used for extracting device related features from the received GNSS signal. The feature selecting methods can be different [5]. The objectives of feature/variable selection for fingerprinting are [13]:

1. Improving the prediction performance of the predictors
2. A better understanding of the underlying process with the generated data
3. Having faster, cost-effective predictors

4.1.3 Classification basis for feature selection methods

Due to the availability of multivariate data and high dimensions there are currently many methods of classification, for example, on the basis of protocol stack [43], features computed from the receiver clock drift [6] and some use ranking techniques like filter methods and wrapper methods [8].

Features in RFF can be broadly classified into supervised and unsupervised learning [33]. Semi-supervised learning is another class wherein both labeled and unlabeled data are used for learning. In this thesis work supervised learning approach is being

Figure 4.1 Fingerprinting Approach

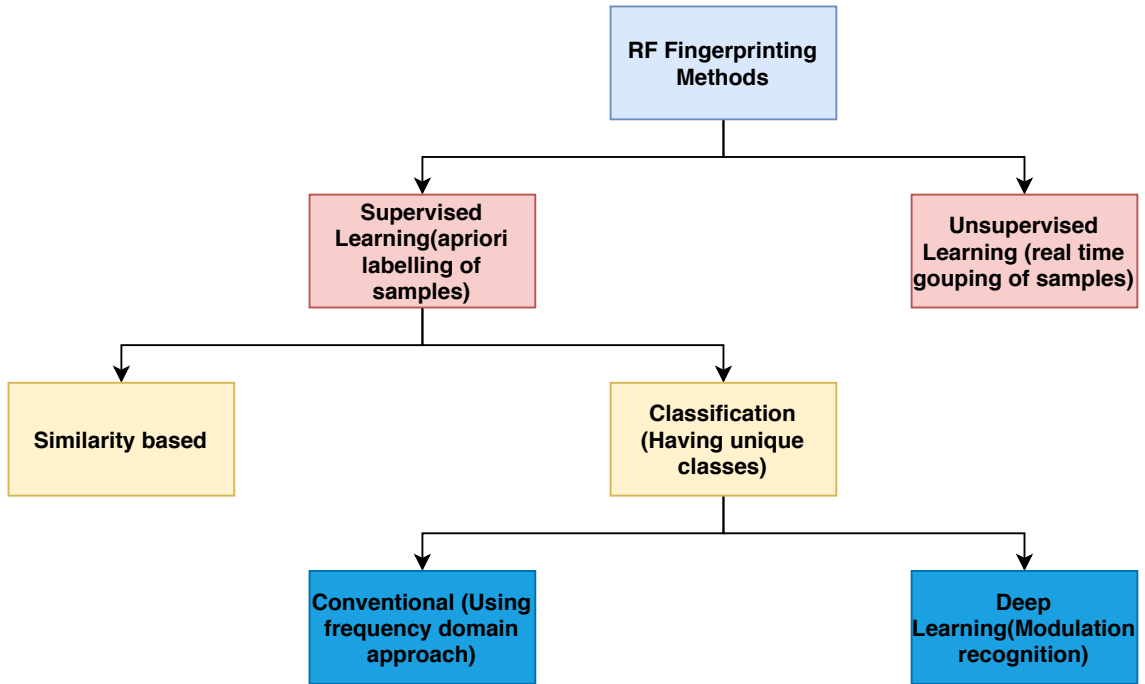
used which involves using frequency domain methods and approach for extracting features. This type of learning involves a big collection of labeled samples before deploying and training of MLA.

Supervised learning is of two types as shown in figure 4.2:

1. **Similarity basis:** Here observed signature of a given device is compared with references stored in master database. Example, bayesian approach.
2. **Classification:** Here the data is divided in to various classes which are labeled. This method is further divided into conventional and deep learning methods. For this work the conventional approach in which frequency domain approach is used for feature extraction. The features that can be studied are I/Q Imbalance, phase imbalance, received signal strength, etc.

4.1.4 Feature Extraction

In feature extraction the raw signal is used for generating some attributes and characteristics. The purpose is to reduce the dimensionality. An efficient extraction algorithm would ideally reduce the dimensions without losing the important information [40].

Figure 4.2 RF Fingerprinting Classification

4.1.5 Transforms used for extracting features

As explained the wavelets take care of the resolution problem in classic fourier transforms, they are a good choice for this work, and the approach has been used in other fingerprinting methods as well [19, 2]. For this thesis work we have decided to use the following transforms.

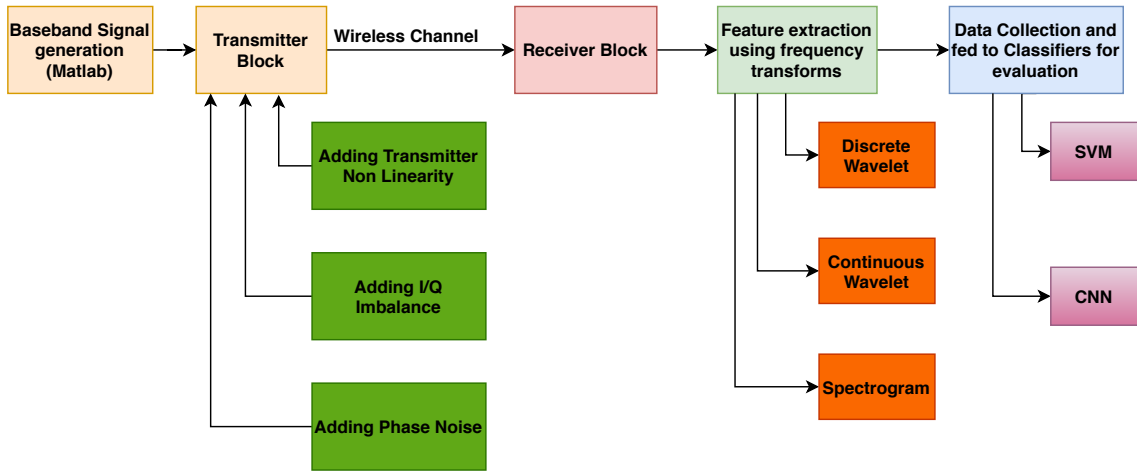
1. Continuous Wavelet (CWT)
2. Discrete Wavelet (DWT)
3. Spectrogram

4.2 Fingerprinting method used

For this thesis work the simulations are done by using communications system toolbox in MATLAB. We have created a typical wireless communication setup with Additive White Gaussian Noise (AWGN) channel, transmitter and receiver blocks. The blocks of the wireless communication chain have been modified to introduce distortions/impairments which try to show the real hardware component imperfections. The sources of radio frequency impairments are shown in the block diagram 4.4. As depicted in the block diagram 4.3, we generate the baseband signal, introduce the impairments in our transmitter block, extract features using various transforms and then feed the images to classifiers for evaluation. There can be following types of impairments/distortions:

1. **Harmonic Distortions:** These are because of the non-linear components on the transmitter hardware components for example: digital to analog converters. This type of distortion is measured in (dB). Radio transmitter equipment have a complicated structure, and they are composed of many electronic devices. Initially, the base-band signal is processed in digital signal processor block and then goes into analog circuit parts. There are many non-linear elements and unit circuits in analog circuit components. Examples of some non-linear elements include power amplifier, non-linear resistors, diodes, transistors, and field-effect tubes. The existence of these non-linear devices makes communication signals have non-linear components.

Figure 4.3 RF Fingerprinting Methodology

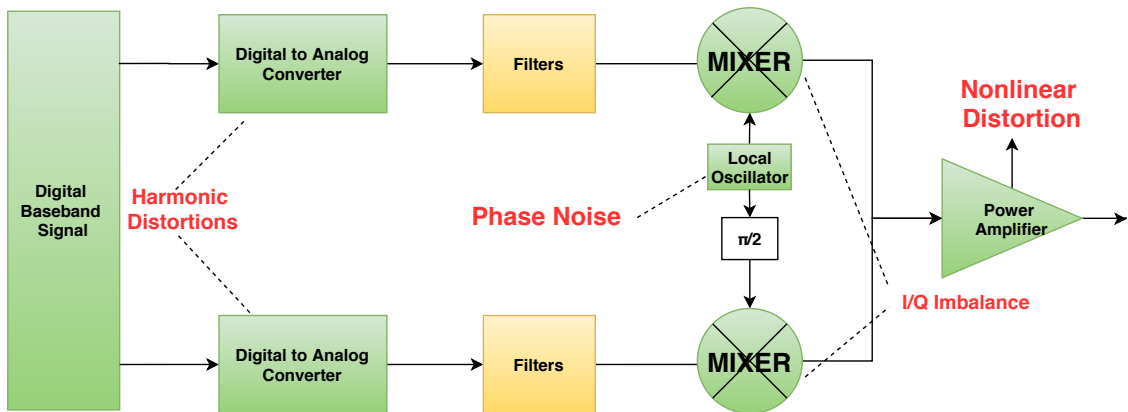


2. **Power amplifier Distortions:** The non-linearities of a power amplifier mainly appear when it is operated in its non-linear region, which is its operation at maximum output power and in that region the output signal gets significantly compressed. The non-linearity is usually modeled using Third Order Input Intercept Point (IIP3). This article explains how non-linearity of a power amplifier has an effect on wireless networks [37].
3. **Carrier frequency phase offset:** Crystal oscillators are normally used for generating carrier frequencies. However, there is always a difference in frequencies generated at the transmitter and receiver side, and that gives rise to carrier frequency phase offset.
4. **I/Q Imbalance:** I/Q signal processing is used in almost all communication receivers. The I/Q processing receivers face a common problem of matching the amplitudes and phases of the I and Q branches. Amplitude and phase

imbalances are unavoidable in the analog front-end, which results some finite rejection of the image frequency band and this results into the image signal to look as interference on top of the actual or desired signal. In quadrature mixing where the baseband signals are converted to RF signals there are amplitude and phase mismatches. The mixer components are not always having an exact 90 degree shift, so a phase imbalance is introduced. We are using `iqimbal` function of matlab here to introduce some amplitude and phase imbalances. The imbalance is mainly due to the analog components which use the capacitor and resistors as components [41].

5. **Phase Noise:** While doing up conversion there is always an additional phase noise component instead of a pure tone at carrier frequency. Phase noise is expressed in dBc/Hz. It has two components, phase noise level (expressed in dBc/Hz) and the frequency offset (expressed in Hz).

Figure 4.4 Sources of RF impairments in transceiver



The simulations were carried out with Additive White Gaussian Noise channel, adding channel and different multipaths and apply the frequency domain transforms to our received Global Navigation Satellite System (GNSS) signal. The signal model was baseband signal model.

MLA are then employed to extract features in steady state of devices. With advanced signal processing mechanisms time series and image based fingerprinting techniques have been researched upon in [39, 33]. We then study performance of different learning algorithms such as linear SVM and CNN.

5 Machine Learning Algorithms

In this section, we are explaining about the machine learning methods used to perform the classification. Classification as explained in [40] is the task performed by a network trained to respond when an input vector resembling a learned vector is presented. The network recognizes the input as one of the original target vectors. We are using here SVM and CNN. The reason for choosing them as classifiers is their accomplished performance as shown in some literature work [39], [33].

The Bag of Features (BoF) approach has been used here for extracting the features. It is somewhat similar to using Bag of Words (BoW) but here we use image features rather than words.

5.1 SVM

In the Support Vector Machine (SVM) method, the image features are extracted by using the method called Bag of Features (BoF). The features are then fed to the SVM classifier. The SVM classifier has two phases, a training stage phase wherein the training data available and a classification stage based on new data which is the test data. Support-vector machines are supervised learning models which help in analyzing data used for classification and regression analysis. With a given set of training data, an SVM algorithm builds a model and assigns new examples to a category, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible.

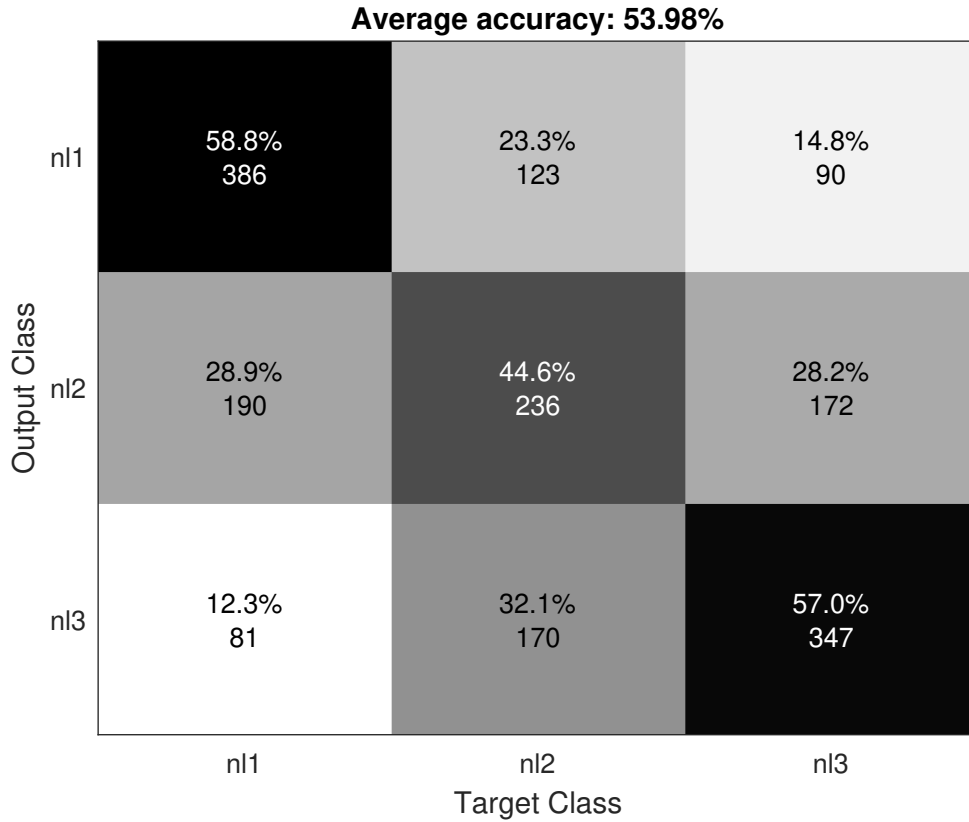
In addition to performing linear classification, SVM's can efficiently perform a non-linear classification using what is called the kernel trick, implicitly mapping their inputs onto a high-dimensional feature spaces. A confusion matrix is then plotted. It looks somewhat like in the figure 5.1. The average accuracy here is 53.98% which is calculated by taking average of the three figures in the diagonal which are 58.8%, 44.6% and 57.0%. Accuracy can be calculated as a fraction of correct predictions to total number of predictions calculated by a model.

$$Accuracy = \frac{\# \text{ of correct predictions}}{\text{Total } \# \text{ of predictions}} \quad (5.1)$$

After obtaining the support vectors, the training and test samples are classified with known class labels. For example, as shown in figure 5.1 there are three classes namely, nl1, nl2, and nl3. From the known class labels the true positive, false positive and false negatives are then computed. This gives the accuracy of the classification

from the obtained support vectors.

Figure 5.1 *Confusion Matrix*



5.2 CNN

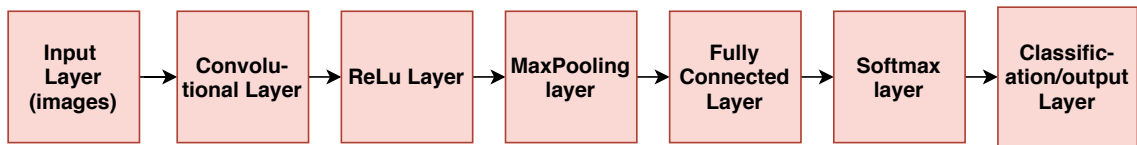
The convolutional neural networks is somewhat analogous to human brain. The neural network here is trained to perform a match between an input image and an output image, for example, classification and pattern recognition. A neural network consists of a number of neurons. For training a network a learning algorithm is utilized till the time we get a target output and a good match between the training and test images set data. In order to do so, we make classes of our data and feed them to a network in the form of image sample. This method is very widely used approach to get information about a pattern which exhibits a non-linear relationship between a known input and target output, which makes the fingerprint-based localization feasible with help of neural network [44].

In this thesis work the CNN architecture having convolutional and max-pooling layers is specifically developed for performing the task of RF fingerprinting [33]. The layered architecture looks like the block diagram 5.2.

There is a brief explanation about each layer.

1. **Input layer:** The purpose of this layer is to convert the input image into three dimensional data which will be then fed to the next subsequent layers.
2. **Convolutional layer:** This is the main building block of the CNN and its primary purpose is extraction of features from input data. It consists of filters that perform convolution on input data.
3. **ReLU layer:** It is also called Rectified Linear Unit (ReLU) layer. ReLU is the max function($\max(x,0)$) with input from a convolved image and it basically sets all negative values in the input matrix to zero while keeping other values at a constant.
4. **Pool layer:** The pooling layer introduces shift variance and reduces the dimensionality of feature maps of the preceding layers and preserving the most important information.
5. **Fully Connected layer:** The primary purpose of this layer is to perform classification task on a high level on features that have been extracted by previous layers.
6. **Softmax layer:** This layer limits the output of the previous step to classification into the range zero to one [25].
7. **Classification layer:** Here the classification is performed on the basis of output from previous layers.

Figure 5.2 CNN Architecture



The output is represented as in the case of SVM with the help of confusion matrix by taking the average of the diagonal as shown in figure 5.1.

6 Simulation Approach

For extracting the features in order to study fingerprinting, the spectrogram and wavelet transforms (discrete and continuous) were used. The reason for using the wavelet method to extract features is because there are some promising results shown in the studies [1, 19, 2, 22] and they also take care of the resolution problem.

In the simulation part we have three steps:

1. **Feature ranking and selection using Discrete Wavelet (DWT):** In this phase for a good CNR range we try to evaluate the best feature out of non-linearity, IQ imbalance and phase noise. Different types of DWT types are tested with all three features. After evaluating the standalone features and deciding the DWT type, feature combinations of two and three features are also tested.
2. **Fingerprinting with two transforms in low CNR range:** In the second phase we test spectrogram and DWT with one, two and three features with both SVM and CNN in a low range of CNR.
3. **Fingerprinting with three transforms in high CNR range:** In this part of the simulations three transforms are tested with both classifiers in a high range of CNR.
4. **Additional simulations:** Here, the best transform of the last phase is chosen and tested further by changing number of images in training and test dataset, introducing multipath, etc.

The general parameters used for simulation and their values are listed in the table 6.1.

The identified features for this thesis work are explained as follows:

1. Non-linearity

Since non-linearity is a forge resistant feature and is primarily because of the non-linear components of which the devices are made, we are considering it here. The non-linearity is introduced by choosing different coefficients a_i in the equation 6.1:

$$y(t) = \sum_{i=0}^N a_i * x^i(t), \text{ where, } N \geq 1 \quad (6.1)$$

Table 6.1 Summary of Input Parameters Used

Parameter	Value
Signal duration	50 milliseconds
Spreading Factor	1023
Sampling Frequency	11.253 MHz
Carrier frequency	1.57 GHz
Chip rate	1.02 MHz
Nc (signal length)	10
Number of satellites	1
Image resolution	ranging from 200 to 1000 dpi
CNR	varying from 30 to 100 dB
No. of images in training database	varying from 100 to 5000
No. of images in test database	varying from 50 to 1000

where, $y(t)$ is the output signal of a non-linear device and $x(t)$ is the input signal. We have introduced two types of non-linearity:

- (a) **Far coefficients:** In this case the assumption is made, such as the transmitters look as if they are of different manufacturer's. The non-linearity coefficients chosen for the three classes are mentioned in table 6.2.

Table 6.2 Far non-linearity coefficients

Selection - A		Selection - B	
Class	Coefficients	Class	Coefficients
1	1	1	1
2	(1, (1/3))	2	(1, - (1/3))
3	(1, 1/4, 1/7)	3	(1, -(1/4), 1/7)

- (b) **Near coefficients:** In this, the idea is to choose the coefficients closer so that the devices seem to be of the same manufacturer. The three classes are chosen as shown in table 6.3.

Table 6.3 Near non-linearity coefficients

Selection - A		Selection - B	
Class	Coefficients	Class	Coefficients
1	(1, 1/3)	1	(1, -(1/3))
2	(1, 1/4)	2	(1, -(1/4))
3	(1, 1/5)	3	(1, -(1/5))

2. IQ Imbalance

As explained in section 4.2 above mismatches between the local oscillator

signals and branches of mixers, the following amplifiers, and low-pass filters, cause the quadrature baseband signals to be shifted, this results in amplitude and phase differences. This is termed as IQ imbalance, where I and Q are the inphase and quadrature components.

It was decided to consider a phase imbalance of 1-2 degrees and an amplitude imbalance of 1-2 percent as suggested in a literature study [41]. The selected values for 3 classes taken are shown in table 6.4.

Table 6.4 *IQ Imbalance Values for 3 classes*

Class	Amplitude Imbalance (dB's)	Phase Imbalance (degrees)
1	0	0
2	1	-5
3	2	5

3. **Phase noise:** Phase noise is the terminology used for explaining the noise spectrum which results from the phase jitters and is because of random phase variations in a signal. The phase noise also gives rise to a rotational jitter. It is expressed in units of dBc per Hertz, which represents the noise power relative to the carrier contained in a 1 Hz bandwidth centered at a certain offset from the carrier. For this thesis work the selected values of phase noise level were in the range [-100, -48] dBc/Hz, and selected values for frequency offset were in the range [20, 200] Hz as suggested in the literature material [33]. The values chosen for the three classes are tabulated in table 6.5:

Table 6.5 *Phase Noise Values for 3 classes*

Class	Phase Noise Level	Frequency Offset
1	0	0
2	-80	40
3	-85	45

The forthcoming sections 6.1 to 6.4 explain the results from four simulation rounds.

6.1 Feature Ranking and Selection Using DWT

During the first round of simulations the objective is to find the following things:

1. Individual performance of 3 features with various discrete wavelet types using SVM.
2. Seeing feature performance by grouping two or more than two features.

6.1.1 Fingerprint feature selection

The first set of simulations are carried out by introducing only non lineairty, IQ Imbalance and phase noise independently and choosing discrete wavelet (various types) for extracting the features. The list of important parameters used for simulation are summarized in table 6.1 and some new parameters are mentioned in table 6.6.

Table 6.6 *Input Paramters Used for Simulation*

Parameter	Value
Training set images	100
Test set images	50
Transform	Discrete Wavelet (DWT)
CNR	50-100 dB
Non-linearity Class Values	Table 6.2 Selection-A
IQ Imbalance Values	Table 6.4
Phase Noise Values	Table 6.5

There are many types of discrete wavelets, for example, haar, daubechies, biorthogonal, coiflets, symlets, morlets, meyer, fejr-korovkin, and reverse biorthogonal etc. The performance of different mother wavelet types are depicted in figure 6.1. As is evident from figure 6.1 non-linearity has the best performance out of all three.

6.1.2 Feature Selection

With the same set of parameters as in tabulated in table 6.6 the following feature combinations were evaluated with SVM:

1. IQ imbalance and phase noise
2. Non-linearity and phase noise
3. Non-linearity and IQ Imbalance
4. Non-linearity, IQ imbalance and phase noise

Figure 6.1 DWT types performance with SVM

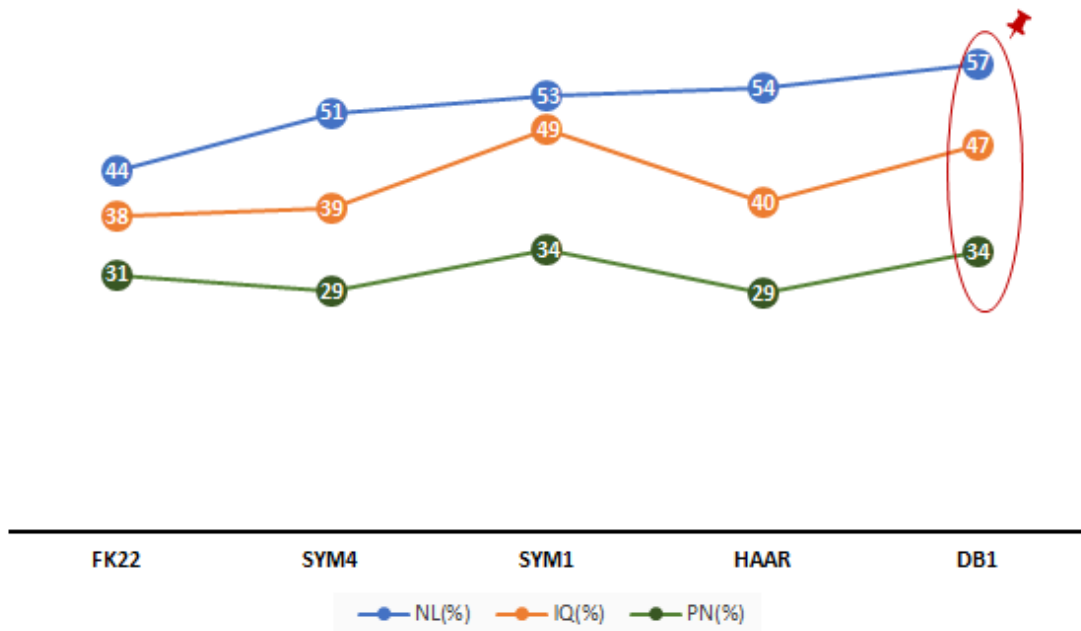
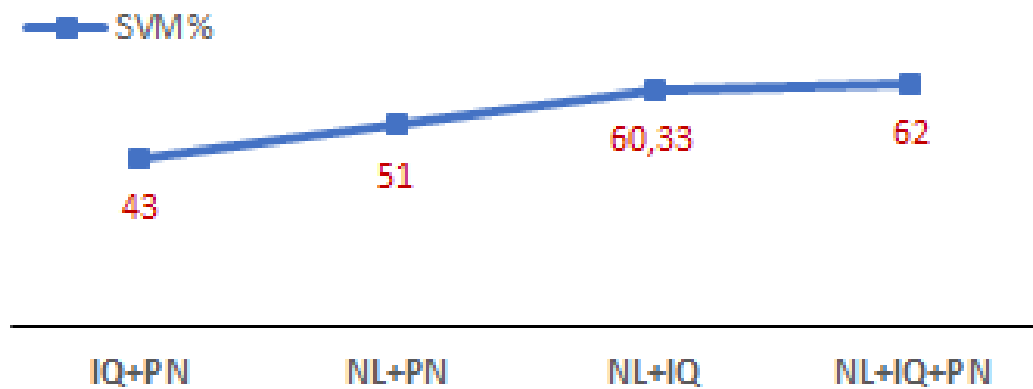


Figure 6.2 Results for feature combinations



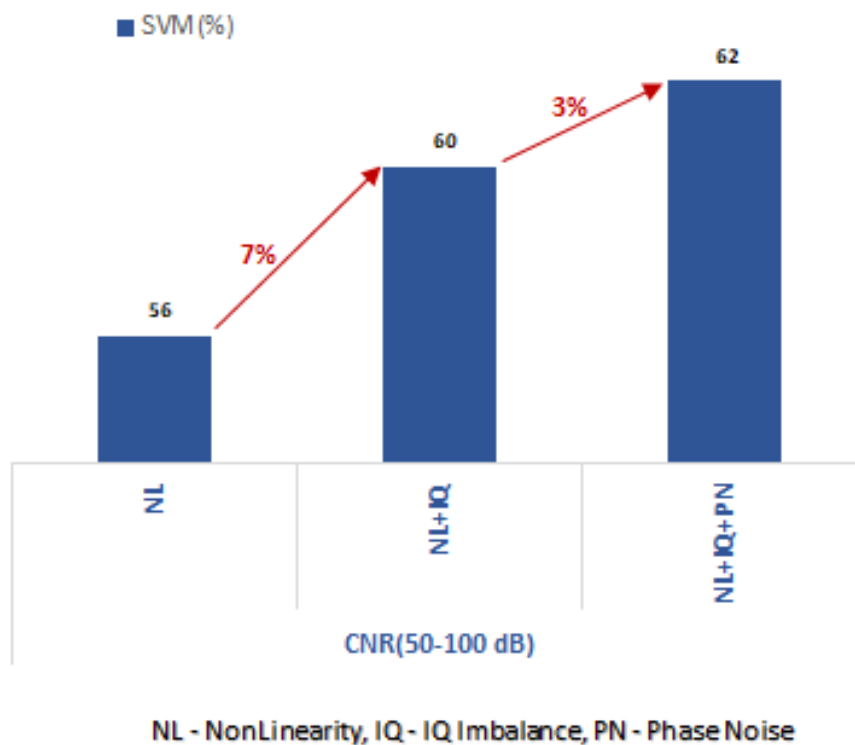
6.1.3 Outcomes

From the first round of simulations we have the following key takeaways:

1. Discrete wavelet type daubechie 'db1' is the best mother wavelet performer as compared to other Discrete Wavelet (DWT) types as shown in figure 6.1. It will be used as a wavelet type for further simulations for discrete wavelet.
2. When various DWT types are tested with individual features then non-linearity has emerged as the most prominent feature. In further simulations it will be chosen as a standalone feature to be tested with other transforms.

3. As a combination of two features, non-linearity and IQ imbalance was a better performer as compared to other two combinations.
4. By addition of one extra feature we can see an improvement of almost 7%, whereas adding the third feature is showing 3% improvement with SVM classifier as shown in bar plot 6.3. So, adding two features is showing better performance in relation to adding three features. There will be a somewhat similar trend in next rounds of simulations.

Figure 6.3 DWT(db1) Results for (50-100 dB)



6.2 Fingerprinting with two transforms in low CNR range

The simulations in this phase are carried out with two transforms, namely Discrete Wavelet(type db1) and Spectrogram by considering non-linearity's far and near for one, two and three features respectively. The list of important parameters used for simulation are already mentioned in table 6.1, the changed values are mentioned again here as reference in table 6.7. The results from this part are summarized in

Table 6.7 Input Parameter changes for phase 2

Parameter	Value
Training set images	1000
Test set images	200
Transforms	Spectrogram and DWT 'db1'
Classifier used	SVM and CNN
CNR	30-80 dB
Non-linearity Far Class	Table 6.2 Selection-A
Non-linearity Near Class	Table 6.3 Selection-A
IQ Imbalance Values	Table 6.4
Phase Noise Values	Table 6.5

the two graphs for far non-linearity case 6.4 and near non-linearity case 6.5.

Figure 6.4 Classifier results for Far Non-linearity Case

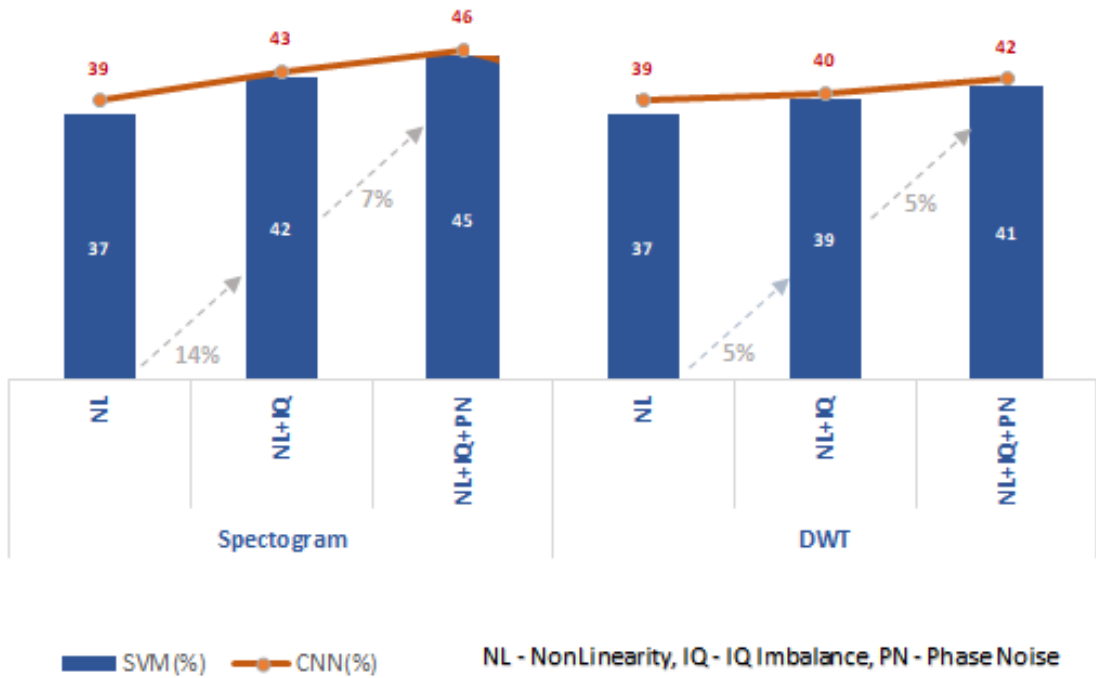
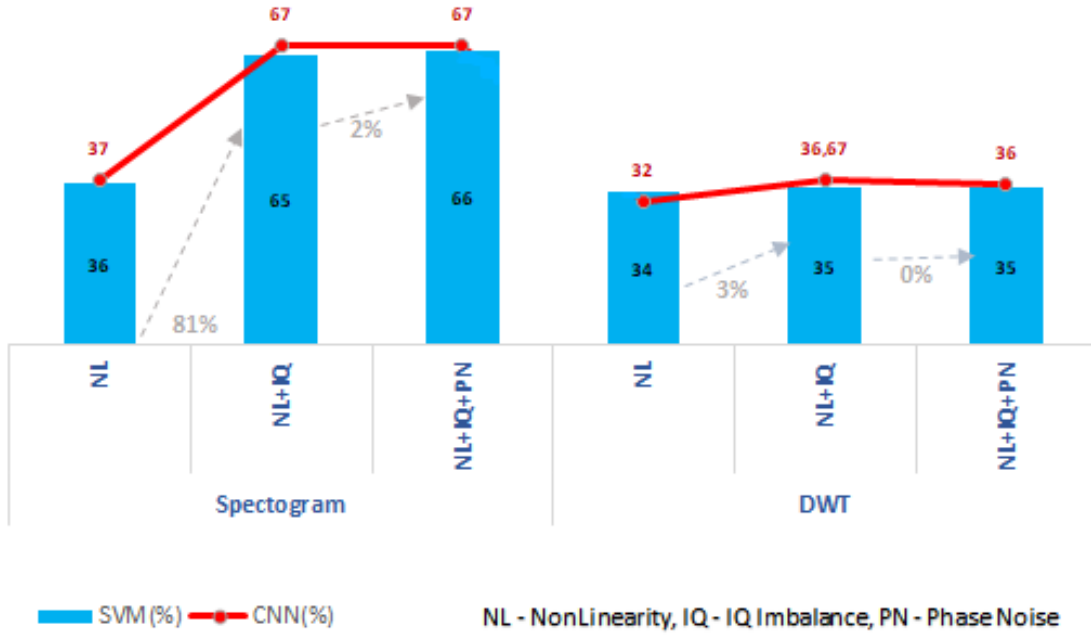


Figure 6.5 Classifier results for Near Non-lineairty Case



Note: The % increases are shown with a gray dotted line for SVM classifier in figures 6.4 and 6.5.

6.2.1 Outcomes

1. The performance of spectrogram is clearly better than Discrete Wavelet for near and far non lineairty cases for low Carrier to Noise Ratio (CNR) range.
2. For Spectrogram also, adding two features shows an improvement of 14% for far non-lineairty case, and 80% improvement in case of near non-lineairty.
3. Convolutional Neural Networks (CNN) is somewhat showing the same performance as Support Vector Machine (SVM) for both Spectrogram and Discrete Wavelet for low Carrier to Noise Ratio (CNR) range.

6.3 Fingerprinting with three transforms in high CNR range

Now the Carrier to Noise Ratio (CNR) is in a higher range of 60-80 dB and the purpose is to evaluate the overall performance of the fingerprinting method with all three transforms using Support Vector Machine and Convolutional Neural Networks classifiers. The list of important parameters used for simulation are already mentioned in table 6.1, the changed values are mentioned again here as a reference in table 6.8.

Table 6.8 *Input Parameter used for phase 3*

Parameter	Value
Training set images	1000
Test set images	200
Transforms	Spectrogram, DWT, CWT
Classifier used	SVM and CNN
CNR	60-80 dB
Non-linearity Far Class	Table 6.2 Selection-B
Non-linearity Near Class	Table 6.3 Selection-B
IQ Imbalance Values	Table 6.4
Phase Noise Values	Table 6.5

The results are summarized in the two graphs for far non-linearity case figure 6.6 and near non-linearity case figure 6.7.

6.3.1 Outcomes

1. The % increases are shown with a gray dotted line for SVM classifier in figures 6.6 and 6.7.
2. Here also, as seen in previous results that addition of one extra feature shows substantial improvement (5%-20%) in performance. Further on addition of one more extra feature there is a slight improvement (4%-8%).
3. Spectrogram is outrightly the best transform as the overall performance in all cases is better than Discrete Wavelet and Continuous Wavelet in high CNR case.
4. There is a red pointer on figure 6.7 for spectrogram. This will be taken as a reference for some additional testing scenarios for the section 6.4. The additional simulations are done with different number of images in training and test sets, introducing multipath, changing pixel size and number of satellites, as will be shown in figure 6.8.

Figure 6.6 Classifier results for Far Non-linearity Case(high CNR)

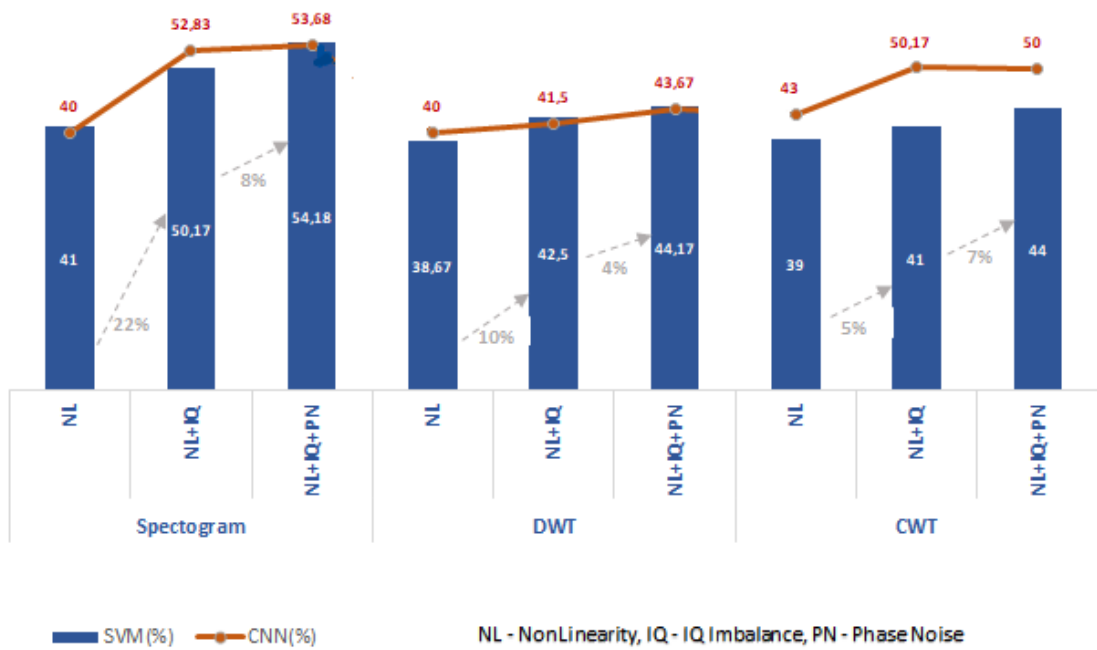
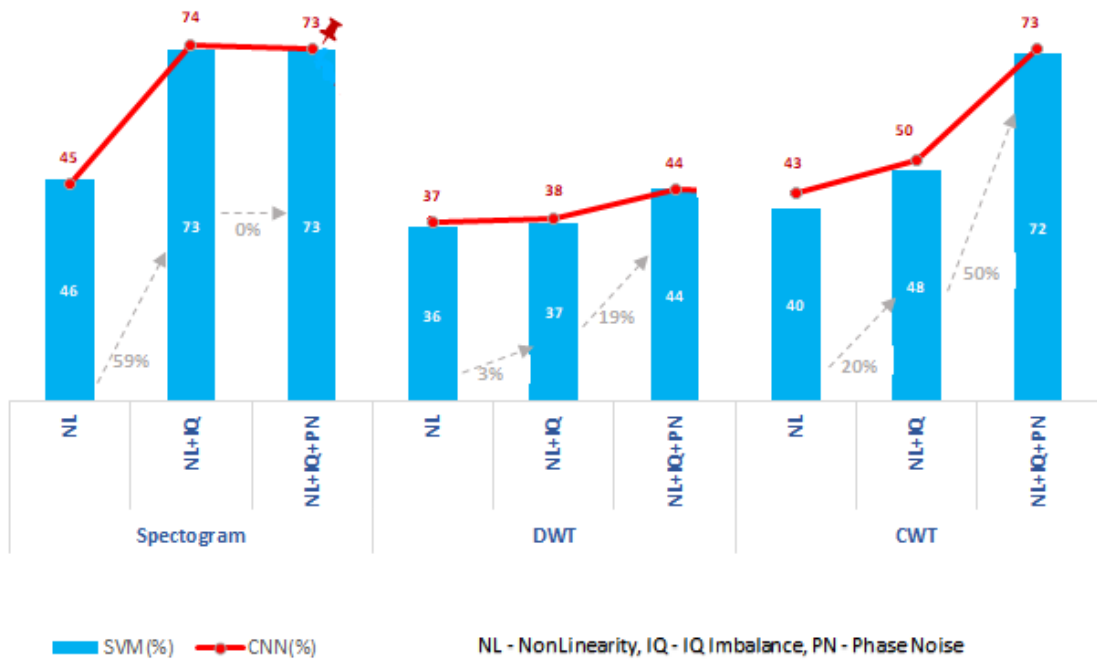


Figure 6.7 Classifier results for Near Nonlinearity Case (high CNR)

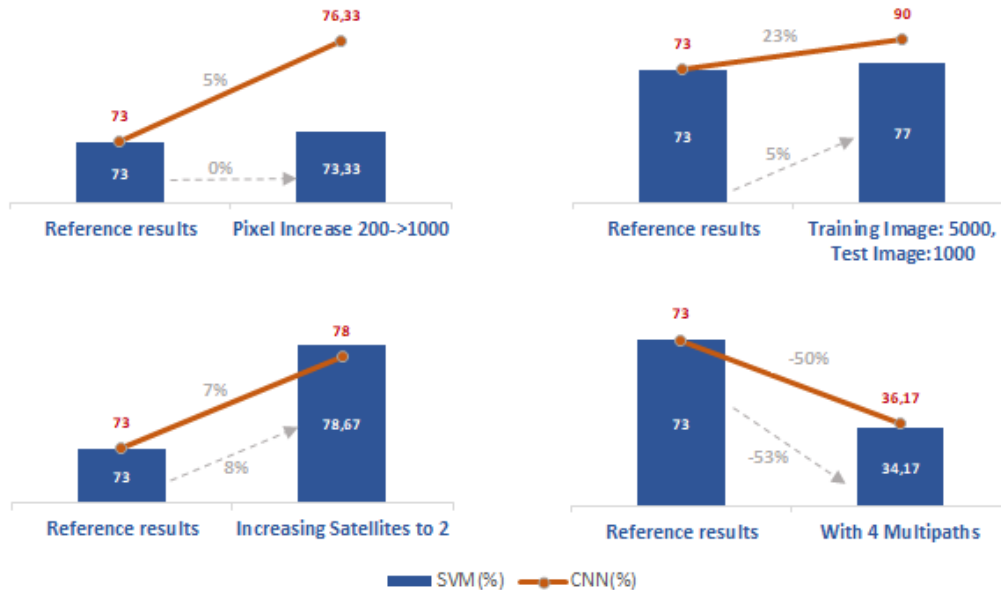


6.4 Additional Simulations

In this phase the spectrogram scenario pointed by a red pin in figure 6.7 is taken as a reference and further evaluated under different set of scenarios. The results are compared for both Support Vector Machine (SVM) and Convolutional Neural Networks (CNN) classifiers as seen in figure 6.8 with the spectrogram results from figure 6.7. The % increases are shown with a gray dotted line for SVM and CNN classifier in figure 6.8.

1. **Varying the pixel size:** As depicted in the figure 6.8, there is not much effect of changing the pixel size.
2. **Increasing the training images to 5000 and test images to 1000:** With increase in images of training (from 1000 to 5000) and test datasets images (from 200 to 1000) there was a considerable improvement seen (around 23%) for CNN.
3. **Introducing four multipath:** Multipath can degrade the classification accuracy by almost 50% for both SVM and CNN.
4. **Increasing the number of satellites:** By increasing the number of satellites, there was almost same improvement in classifier performances for both SVM and CNN. Here, the idea used is to add the signals at receiver coming from two different transmitting satellites. The combined signal is then used to generate the images.

Figure 6.8 Simulation results comparison with reference case of figure 6.7



6.5 Notes on the simulation environment

The laptop which was used for the thesis work was having the processor, Intel(R) Core(TM) i7-8750H CPU@2.20GHz 2.21 GHz, a RAM of 32GB, 64 bit operating system, x64-based processor. The version of Matlab R2019a was used. While performing the thesis work there were some minor challenges which are listed below:

1. When the simulations were carried out for a training size of 1000 images, the time taken per simulation was close to 60-240 minutes varying from one frequency transform to another.
2. Storing the images requires lot of space also. Saving 15000 images takes about 2 GB of space.
3. The scenario wherein the number of images number was increased to 5000 took almost 8-9 hours to generate the images. After that the classifiers also took about 50-60 minutes for evaluation.
4. Its difficult to generate real time simulator scenario as the channel parameters are always changing.

7 Design Recommendations

Some key design recommendations as an outcome of this thesis work are following:

1. Non-linearity is the strongest feature followed by IQ imbalance and phase noise for device identification shown in subsection 6.1.2.
2. Non-linearity and IQ imbalance grouped together (as two features) help in achieving much better performance results for both far and near case in different CNR ranges 6.3.
3. Spectrogram performance is better among all other transforms (DWT and CWT) in both far and near scenarios for different CNR ranges as observed in section 6.2 (for low ranges CNR) and section 6.3 (for high range CNR).
4. The feature extraction process improves significantly with two features (non-linearity and IQ imbalance here), however, performance increases only marginally on further addition of the third feature.
5. Number of features (more than 2) to be used for feature extraction should be evaluated keeping in view that adding more feature might increase computational complexity and overall device computational performance (specially for low cost devices). The classification accuracy can be improved if complexity is taken care of.
6. Better classification accuracy can be achieved with CNN with high number of images in training dataset (up to 5000) and test dataset (up to 1000) of images is considered. CNN has shown an accuracy of almost 90% for one tested scenario for spectrogram in high range CNR in the case of near non-linearity with three features.

8 Conclusion

This work proposes a Radio Frequency Fingerprinting (RFF) method using wavelet and spectrogram transforms in context of Global Navigation Satellite System signals. The aim was to see the efficacy of this method to improve the RF fingerprints authentication and classification accuracy for different transmitter devices. The classification accuracy with Support Vector Machine (SVM) and Convolutional Neural Networks (CNN) in different ranges of Carrier to Noise Ratio (CNR) was evaluated.

A set of three features was chosen, namely non-linearity, IQ imbalance and phase noise. The fingerprint feature selection method is proposed by combining the wavelet transform DWT having different mother wavelet types, and SVM together in a good range of CNR from 50-100 dB.

As a result the non-linearity feature which is device specific and difficult to forge emerged out as the strongest feature, followed with IQ imbalance and phase noise. Thereafter, a grouping of two features was done to see the improvement in classification accuracy from one to two features. There was a good improvement with combination of two features with discrete wavelet. Adding the third feature also improved the classification accuracy, but the increment was marginal.

In the second phase the fingerprinting method was tested with SVM and CNN with spectrogram and discrete wavelet. Spectrogram demonstrated good results and showed significant improvement in classifier performance of around 21% from one feature to three features at low CNR range.

When the fingerprinting method was tested with three transforms and both Support Vector Machine and Convolutional Neural Networks classifiers, spectrogram was the overall best transform giving good classification accuracy in high range of CNR. In additional part of the simulations, it was observed that both SVM and CNN have better classification performance accuracy when the image database is increased. However, it may add to additional complexity as storing high number of images will increase overheads for low cost applications.

Refinement of the machine learning algorithms can be an interesting topic for extending this research work. Also, the RF fingerprints were accumulated in a very controlled environment with no extreme variations in temperature, atmospheric disturbances and multi-path interference, in presence of interference the classification accuracy may get reduced as shown in a part of additional simulations of figure 6.8.

Additional features can be studied to see if they can help in achieving better fingerprinting accuracy. The robustness of selected features is very important.

Receiver front end also has non-linear components and can be a compelling topic for further research work. In this research work, the additional non-linearity of components added by the Digital-to-Analog Converters was not taken into account, it can also be incorporated in the future works and the non-linear effects can be investigated in more detail.

Bibliography

- [1] C. Bertoncini. “Applications of pattern classification to time-domain signals”. In: (Jan. 2010).
- [2] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders. “Wavelet Fingerprinting of Radio-Frequency Identification (RFID) Tags”. In: *IEEE Transactions on Industrial Electronics* 59.12 (Dec. 2012), pp. 4843–4850. ISSN: 1557-9948. DOI: 10.1109/TIE.2011.2179276.
- [3] I. Bisio, F. Lavagetto, M. Marchese, and A. Sciarrone. “Energy efficient WiFi-based fingerprinting for indoor positioning with smartphones”. In: *2013 IEEE Global Communications Conference (GLOBECOM)*. 2013, pp. 4639–4643.
- [4] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti. “Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers”. In: *Proceedings of the IEEE* 104.6 (June 2016), pp. 1233–1245. ISSN: 1558-2256. DOI: 10.1109/JPROC.2016.2543266.
- [5] D. Borio, C. Gioia, G. Baldini, and J. Fortuny. “GNSS Receiver Fingerprinting for Security-Enhanced Applications”. In: Sept. 2016. DOI: 10.33012/2016.14688.
- [6] D. Borio, C. Gioia, E. Cano, and G. Baldini. “Feature Selection for GNSS receiver fingerprinting”. In: *Inside GNSS* 12 (July 2017), pp. 54–62.
- [7] G. Caparra, S. Ceccato, N. Laurenti, and J. Cramer. “Feasibility and Limitations of Self-Spoofing Attacks on GNSS Signals with Message Authentication”. In: Sept. 2017. DOI: 10.33012/2017.15402.
- [8] G. Chandrashekar and F. Sahin. “A Survey on Feature Selection Methods”. In: *Comput. Electr. Eng.* 40.1 (Jan. 2014), pp. 16–28. ISSN: 0045-7906. DOI: 10.1016/j.compeleceng.2013.11.024. URL: <https://doi.org/10.1016/j.compeleceng.2013.11.024>.
- [9] S. Deng, Z. Huang, X. Wang, and G. Huang. “Radio Frequency Fingerprint Extraction Based on Multidimension Permutation Entropy”. In: *International Journal of Antennas and Propagation* 2017 (2017). DOI: 10.1155/2017/1538728.
- [10] P. Fonseka and K. Sandrasegaran. “Indoor localization for IoT applications using fingerprinting”. In: *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. 2018, pp. 736–741.
- [11] G. Caparra. “Authentication and Integrity Protection at Data and Physical layer for Critical Infrastructures”. URL: <http://paduaresearch.cab.unipd.it/9797/>.

- [12] O. Gungor, C. E. Koksal, and H. E. Gamal. “An information theoretic approach to RF fingerprinting”. In: *2013 Asilomar Conference on Signals, Systems and Computers*. Nov. 2013, pp. 61–65. DOI: 10.1109/ACSSC.2013.6810230.
- [13] I. Guyon and A. Elisseeff. “An Introduction to Variable and Feature Selection”. In: *J. Mach. Learn. Res.* 3.null (Mar. 2003), pp. 1157–1182. ISSN: 1532-4435.
- [14] Y. Huang, C. Yuan, M. Chen, W. Lin, and H. Teng. “Hardware Implementation of RFID Mutual Authentication Protocol”. In: *IEEE Transactions on Industrial Electronics* 57.5 (2010), pp. 1573–1582.
- [15] S. Joardar, T. A. Siddique, S. Alam, and M. Hossam-E-Haider. “Analyses of different types of errors for better precision in GNSS”. In: *2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*. 2016, pp. 1–6.
- [16] Y. Kamatham. “Estimation, analysis and prediction of multipath error for static GNSS applications”. In: *2018 Conference on Signal Processing And Communication Engineering Systems (SPACES)*. 2018, pp. 62–65.
- [17] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau. “Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach”. In: *2008 IEEE 68th Vehicular Technology Conference*. 2008, pp. 1–5.
- [18] A. M. Khan, N. Iqbal, A. Khan, M. Khan, and A. Ahmad. “Detection of Intermediate Spoofing Attack on GNSS Receiver through Slope based Metrics”. In: *Journal of Navigation* (Apr. 2020). DOI: 10.1017/S0373463320000168.
- [19] R. W. Klein, M. A. Temple, and M. J. Mendenhall. “Application of wavelet-based RF fingerprinting to enhance wireless network security”. In: *Journal of Communications and Networks* 11.6 (Dec. 2009), pp. 544–555. ISSN: 1976-5541. DOI: 10.1109/JCN.2009.6388408.
- [20] A. Kolomijeca, J. A. López-Salcedo, E. Lohan, and G. Seco-Granados. “GNSS applications: Personal safety concerns”. In: *2016 International Conference on Localization and GNSS (ICL-GNSS)*. 2016, pp. 1–5.
- [21] Y. Li, X. Chen, Y. Lin, G. Srivastava, and S. Liu. “Wireless Transmitter Identification Based on Device Imperfections”. In: *IEEE Access* 8 (2020), pp. 59305–59314.
- [22] Y. Lin, L. Chen, J. Chen, F. Xie, S. Chen, and H. Wen. “A Low Complexity Feature Extraction for the RF Fingerprinting Process”. In: *2018 IEEE Conference on Communications and Network Security (CNS)*. May 2018, pp. 1–2. DOI: 10.1109/CNS.2018.8433156.

- [23] Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou. “The individual identification method of wireless device based on dimensionality reduction and machine learning”. In: *The Journal of Supercomputing* 75 (Dec. 2017). DOI: 10.1007/s11227-017-2216-2.
- [24] E. S. Lohan, R. Morales Ferre, P. Richter, E. Falletti, G. Falco, and A. Fuente. “GNSS Navigation Threats Management on-Board of Aircraft”. In: *INCAS BULLETIN* 11 (Sept. 2019), pp. 111–125. DOI: 10.13111/2066-8201.2019.11.3.10.
- [25] R. Morales Ferre, A. Fuente, and E. S. Lohan. “Jammer Classification in GNSS Bands Via Machine Learning Algorithms”. In: *Sensors* 19 (Nov. 2019), p. 4841. DOI: 10.3390/s19224841.
- [26] R. Morales Ferre, P. Richter, E. Falletti, A. Fuente, and E. S. Lohan. “A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft”. In: *IEEE Communications Surveys & Tutorials* PP (Oct. 2019), pp. 1–1. DOI: 10.1109/COMST.2019.2949178.
- [27] R. Morales Ferre, P. Richter, A. Fuente, and E. S. Lohan. “In-lab validation of jammer detection and direction finding algorithms for GNSS”. In: *2019 International Conference on Localization and GNSS (ICL-GNSS)*. June 2019, pp. 1–6. DOI: 10.1109/ICL-GNSS.2019.8752944.
- [28] H. Onishi, K. Yoshida, and T. Kato. “GNSS vulnerabilities and vehicle applications”. In: *2016 13th Workshop on Positioning, Navigation and Communications (WPNC)*. 2016, pp. 1–5.
- [29] C. Ouzeau, C. Macabiau, B. Roturier, and M. Mabillean. “Performance assessment of multi correlators interference detection and repair algorithms for Civil Aviation”. In: *ENC-GNSS 2008, Conférence Européenne de la Navigation*. Toulouse, France, Apr. 2008. URL: <https://hal-enac.archives-ouvertes.fr/hal-01022189>.
- [30] U. Pereg and Y. Steinberg. “The Arbitrarily Varying Channel Under Constraints With Side Information at the Encoder”. In: *IEEE Transactions on Information Theory* 65.2 (Feb. 2019), pp. 861–887. ISSN: 1557-9654. DOI: 10.1109/TIT.2018.2861776.
- [31] A. Pérez-Navarro, J. Torres-Sospedra, R. Montoliu, J. Conesa, R. Berkvens, G. Caso, C. Costa, N. Dorigatti, N. Hernández, S. Knauth, E. S. Lohan, J. Machaj, A. Moreira, and P. Wilk. “1 - Challenges of Fingerprinting in Indoor Positioning and Navigation”. In: *Intelligent Data-Centric Systems*. Academic Press, 2019, pp. 1–20. ISBN: 978-0-12-813189-3. DOI: <https://doi.org/10.1016/B978-0-12-813189-3>.

- 1016/B978-0-12-813189-3.00001-0. URL: <http://www.sciencedirect.com/science/article/pii/B9780128131893000010>.
- [32] A. C. Polak and D. L. Goeckel. “Wireless device identification based on RF oscillator imperfections”. In: *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2014, pp. 2679–2683.
- [33] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury. “Deep Learning Convolutional Neural Networks for Radio Identification”. In: *IEEE Communications Magazine* 56.9 (Sept. 2018), pp. 146–152. ISSN: 1558-1896. DOI: 10.1109/MCOM.2018.1800153.
- [34] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel. “Physical-Layer Fingerprinting of LoRa Devices Using Supervised and Zero-Shot Learning”. In: *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec ’17. Boston, Massachusetts: Association for Computing Machinery, 2017, pp. 58–63. ISBN: 9781450350846. DOI: 10.1145/3098243.3098267. URL: <https://doi.org/10.1145/3098243.3098267>.
- [35] L. Schauer. “2 - Wi-Fi Tracking Threatens Users’ Privacy in Fingerprinting Techniques”. In: *Intelligent Data-Centric Systems*. Academic Press, 2019, pp. 21–43. ISBN: 978-0-12-813189-3. DOI: <https://doi.org/10.1016/B978-0-12-813189-3.00002-2>. URL: <http://www.sciencedirect.com/science/article/pii/B9780128131893000022>.
- [36] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren. “A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures”. In: *ACM Computing Surveys* 48 (May 2016), pp. 1–31. DOI: 10.1145/2897166.
- [37] P. Singya, N. Kumar, and V. Bhatia. “Effect of non-Linear power amplifiers on future wireless communication networks”. In: *IEEE Microwave Magazine* 18 (July 2017). DOI: 10.1109/MMM.2017.2691423.
- [38] M. Sun, L. Zhang, J. Bao, and Y. Yan. “RF fingerprint extraction for GNSS anti-spoofing using axial integrated Wigner bispectrum”. In: *Journal of Information Security and Applications* 35 (Aug. 2017), pp. 51–54. DOI: 10.1016/j.jisa.2017.05.002.
- [39] M. Takagi, A. Sakurai, and M. Hagiwara. “Quality Recovery for Image Recognition”. In: *IEEE Access* 7 (2019), pp. 105851–105862. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2932726.
- [40] O. Ureten and N. Serinken. “Wireless security through RF fingerprinting”. In: *Canadian Journal of Electrical and Computer Engineering* 32.1 (May 2007), pp. 27–33. ISSN: 0840-8688. DOI: 10.1109/CJECE.2007.364330.

- [41] M. Valkama, M. Renfors, and V. Koivunen. “Advanced methods for I/Q imbalance compensation in communication receivers”. In: *IEEE Transactions on Signal Processing* 49.10 (Oct. 2001), pp. 2335–2344. ISSN: 1941-0476. DOI: 10.1109/78.950789.
- [42] C. Wullems, O. Pozzobon, and K. Kubik. “Signal authentication and integrity schemes for next generation global navigation satellite systems”. In: Jan. 2005.
- [43] Q. Xu, R. Zheng, W. Saad, and Z. Han. “Device Fingerprinting in Wireless Networks: Challenges and Opportunities”. In: *IEEE Communications Surveys & Tutorials* 18 (Jan. 2015). DOI: 10.1109/COMST.2015.2476338.
- [44] X. Ye, X. Yin, X. Cai, A. Pérez Yuste, and H. Xu. “Neural-Network-Assisted UE Localization Using Radio-Channel Fingerprints in LTE Networks”. In: *IEEE Access* 5 (2017), pp. 12071–12087. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2712131.
- [45] J. Yu, A. Hu, G. Li, and L. Peng. “A Robust RF Fingerprinting Approach Using Multisampling Convolutional Neural Network”. In: *IEEE Internet of Things Journal* 6.4 (2019), pp. 6786–6799.