



# A Review of Recent Developments on Secure Authentication using RF Fingerprints Techniques

 Hüseyin Parmaksız<sup>1</sup>,  Cihan Karakuzu<sup>2</sup>

<sup>1</sup>Corresponding Author; Bilecik Şeyh Edebali University, Department of IT; huseyin.parmaksiz@bilecik.edu.tr;

<sup>2</sup> Bilecik Şeyh Edebali University, Department of Computer Engineering; cihan.karakuzu@bilecik.edu.tr;

Received 7 March 2022; Revised 10 April 2022; Accepted 11 October 2022; Published online 31 December 2022

## Abstract

The Internet of Things (IoT) concept is widely used today. As IoT becomes more widely adopted, the number of devices communicating wirelessly (using various communication standards) grows. Due to resource constraints, customized security measures are not possible on IoT devices. As a result, security is becoming increasingly important in IoT. It is proposed in this study to use the physical layer features (PLF) of wireless signals as an effective method of increasing IoT security. According to the literature, radio frequency fingerprinting (RFF) techniques are used as an additional layer of security for wireless devices. To prevent spoofing or spoofing attacks, unique fingerprints appear to be used to identify wireless devices for security purposes (due to manufacturing defects in the devices' analog components). To overcome the difficulties in RFF, different parts of the transmitted signals (transient/preamble/steady-state) are used. This review provides an overview of the most recent RFF technique developments. It discusses various solution methods as well as the challenges that researchers face when developing effective RFFs. It takes a step towards the discovery of the wireless world in this context by drawing attention to the existence of software-defined radios (SDR) for signal capture. It also demonstrates how and what features can be extracted from captured RF signals from various wireless communication devices. All of these approaches' methodologies, classification algorithms, and feature classification are explained. In addition, this study discusses how deep learning, neural networks, and machine learning algorithms, in addition to traditional classifiers, can be used. Furthermore, the review gives researchers easy access to sample datasets in this field.

**Keywords:** IoT, security, deep learning, RFF, SDR

## Nomenclature Acronyms

AI/ML: artificial intelligence/machine learning	MLE: maximum likelihood estimates
AWGN: additive white gaussian noise	NLP: natural language processing
BRCD: Bayesian ramp change detector	OFDM: orthogonal frequency division multiplexing
BSCD: Bayesian step change detector	PCs: phase characteristics
CFO: carrier frequency offset	PCA: principal component analysis
CNN: convolutional neural network	PD: phase detector
CSIR: channel state information at the receiver	PLF: physical layer features
DCTF: differential constellation trace figure	PLS: partial least squares
DSP: digital signal processing	PSD: power spectral density
DWT: discrete wavelet transform	RF: radio frequency
ELM: extreme learning machine	RFF: radio frequency fingerprinting
EMD: empirical mode decomposition	RFID: radio frequency identification
FE: feature extraction	RSS: radio received signal strength
FFT: fast fourier transform	SDR: software defined radio
GSM: global system for mobile	SFO: sampling frequency offset
GLRTD: generalized likelihood ratio test detector	SNR: signal-to-noise ratio
HF: high frequency	SPoTS: starting point of transient signal
HHT: Hilbert-Huang transform	STSP: short training sequence preamble
IoT: internet of things	SVM: support vector machine
LTSP: long training sequence preamble	TS: transient signals
MCPD: mean change point detector	URH: universal radio hacker
MDA: multiple discrimination analysis	VFDTD: variance fractal dimension threshold detector

## 1. Introduction

Kevin Ashton coined the term IoT in a presentation (where the benefits of RFID technology to the company and its use were suggested) prepared for the Procter & Gamble Company in 1999. In general terms, it is possible to define the IoT as a system of devices that communicate with each other and form an intelligent network by connecting and sharing information, thanks to various communication protocols. Digital Agenda, published by the European Union, is an emerging technology and market that enables objects and applications to communicate between themselves, produce data and share this data. This structure is defined as “*an ecosystem of smart applications and services that make people's lives easier and raise their living standards*”. The European Technology Platform, on the other hand, defined it as “*a common network established between things/objects that can be physical and virtual, also have pre-defined functions and work in smart environments, and this network exchanges information with other networks and users*”. Today, one of the areas where technological developments are applied the fastest is objects. Both the vital convenience and benefits brought by technological innovations, and the rapid increase in the use of people by adapting to technology very quickly, communication with objects is the most current issue. With spread of smart devices, social structures have changed, and the phenomenon of “*Information Society*” has been fully formed. In the past, the information was based only on the information that people gave voluntarily, and the accuracy of the data received was often discussed. However, at this point, data is now collected with smart devices independently of the declaration of individuals, and the accuracy level increases. In this way, reliable knowledge will also increase with smart objects. Development of IoT concept and technology; changes the social structure by facilitating life, raising living standards, increasing productivity and contributing to economies. Like all good things, when it is not taken care of, its bad points are serious. The key point is information security. Information security problems related to smart objects, why the issue of security is really important and the precautions that can be taken are emphasized. In 2013, Russia's state channel Rossiya 24 claimed that the hacker irons produced in China and imported to the country contained a special wireless internet control chip, thus spying on the personal computers of the users by organizing a cyber-attack. Although this news may seem like exaggerated news or fake news at first, its accuracy has been determined in the examinations [1, 2].

It will be seen in real life from science fiction movies that the car we use is the target of attackers and causes accidents, smart alarm and lock systems are broken and cyber thefts occur, infiltrating wearable objects, detecting discomfort from body activities and the emergence of cyber murders. If we give an example from our house in a narrower area; if all objects in a house are managed from a single center; it is possible to seize that system with a cyber-attack, to start a fire by playing with the oven settings, to steal by turning off alarm system and opening the door, to copy all personal data on the computer or to violate the privacy of private life by watching the house from camera system. Information security violations that may occur in smart devices have a chance to be prevented by certain controls to be made by both the manufacturer and the user. Considering the most common security vulnerabilities in smart devices, it can be determined that “*Web Interface Configuration, Authentication/Authorization, Network Services, Encrypted Transport, Privacy, Mobile Applications, Cloud, Security Configurations, Software and Physical Security*” checkpoints should be made [2]. The security policy defines all the rules, regulations and procedures that must be followed to ensure system security and can be applied to many different areas. Some policies to prevent risks can be categorized as follows:

**Remote Access Policy:** It is the standardization of who can connect to the system, when and how, and what kind of devices can be connected to this system remotely.

**Information Privacy Policy:** It is the definition of which methods will be used to protect information depending on the level of sensitivity. Generally, more sensitive information has a higher level of security.

**Computer Security Policy:** Defines which computers users will use. This policy defines who will use certain computers and which programs will be used to protect a computer or whether a particular storage device will be used.

**Physical Security Policy:** Defines how physical assets are secured.

Password Policy: Determines how long a password should be changed, what type of passwords to use, and the criteria for defining password security levels.

The review's chronology continues as follows. First and foremost, what is an RF fingerprint, where it is used, the importance of using modern software defined radios instead of the antenna and oscilloscope used in the literature to capture the RF signal, which parts of the signal are used in determining the feature, effective algorithms in FE, what features are used in this area, and what classification algorithm is used and provides a general idea of how successful its methods have been. Furthermore, the extensive literature review and sample data sets are expected to shed light on the scientists who will work in this field.

## 2. Radio Frequency Fingerprinting and Data Acquisition

RFF is a technique that's used to identify the radio signals emitted by various devices. In monitoring radars, RFF is widely used in the military field. It's also used to authenticate wireless connections.

The process of extracting the radio signal's unique features involves firstly identifying the source code. The code then passes these features to a classifier. The data acquisition subsystem of a wireless device is used to acquire and digitize a radio signal. It is typically built into a device to minimize signal degradation due to noise [3].

In SDR, the software acts as the front end while the hardware provides the signal processing engine. The software that will allow this interaction is called GNU Radio. It is possible to create a "flow graph" which is a collection of interconnected signal processing blocks, by appropriately combining the blocks (to which algorithms and functions can be implemented) in GNU Radio. URH was created with theoretically oriented researchers in mind who want to focus on protocol logic rather than diving deep into HF and DSP. URH can perform spectrum analysis, signal recording, and protocol sniffing [4]. SigDigger, like GNU Radio and URH, is another software that can be used in the field of signal capture. SigDigger (digital signal analyzer written in Qt5 by BatchDrake for Unix systems) collaborates with three projects: Sigutils (DSP library that distributes the load using multi-core CPUs), Suscan (real-time signal analysis library), and SuWidgets.

Signal acquisition can be done either actively or passively. In the active mode, a radio signal is captured from a wireless device to be used for identification, and signal collection is used for sampling [5]. In passive mode, while the device communicate with other devices, radio signal get caught from it. As an example, mobile phones in GSM communication with passive reception base stations can be defined [6].

### 2.1 Software Defined Radios

SDRs is used in the literature for radio communication. Unlike hardware-based solutions, SDR is a software-defined radio technology based on radio and wireless communication protocols. Figure 1 provides a general perspective of the wireless world with SDR. Thanks to its reprogrammable feature, it meets the needs without the need for extra equipment. In this way, it strengthens the possibility of working on multi-functional and multi-band radio and wireless devices [7]. SDR is a major innovation development that develops a reconfigurable wireless communication system that replaces the traditional hardware communication devices implementation [8] SDR, it would be difficult and extra costly to install hardware from scratch or add new hardware to the existing system for minor design changes [9]. SDR allows the same hardware platform to be reused for many communications equipment with different protocols, reducing time to service and development cost to the end user [10]. The report in [7], it was expected SDR market is being worth more than \$29 billion for the year 2021. Global Industry Analysts, Inc. reports the following SDR market tendencies: (i) growing military interest in developing countries in communication/information and large-scale distribution systems; (ii) rising requisition for public safety and disaster preparedness applications; and (iii) the need for developing of virtual base stations. It is evaluated that SDRs with their physically small size and low power consumption are convenient to design and implement of systems of the future [11-13], vehicle-to-vehicle communication

systems [11], Global Navigation Satellite System sensors [12] and IoT applications [13], [14]. HackRF One is a low cost SDR. It is critical to know which frequency band range the communicating devices operate in when using the HackRF One (low cost) device for signal capture. The HackRF package includes the ANT500 (telescopic antenna). The frequency band range of many communication protocols can be used with HackRF, which operates in the 1MHz-6GHz range. GNU Radio can be used to create a programming interface [15].

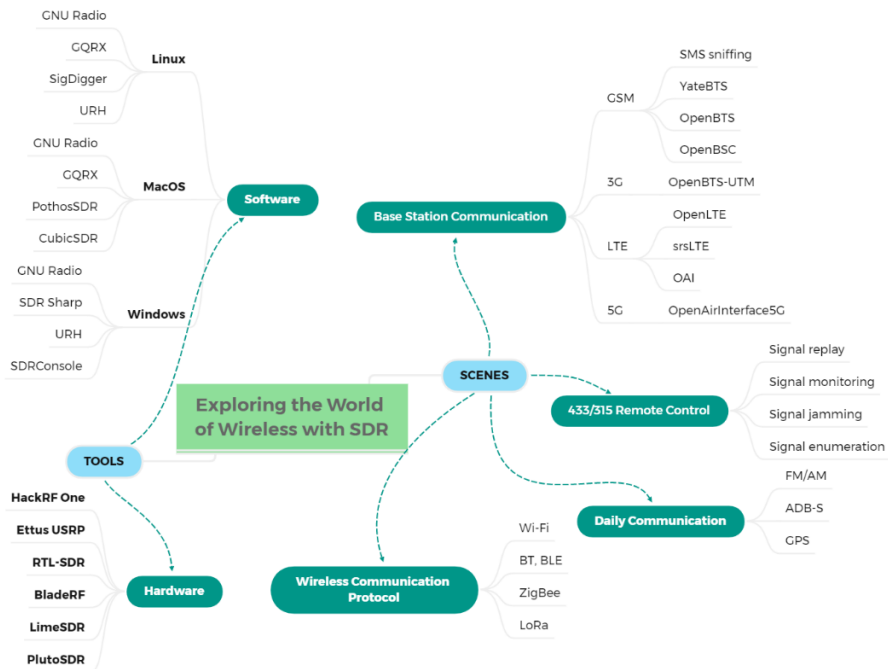


Figure 1 Exploring the Wireless World with SDR.

## 2.2 RF Fingerprints and Datasets

The RF spectrum given in Figure 2, which is part of the natural electromagnetic radiation spectrum, is between 3 kHz and 300 GHz frequency values. The spectrum used by wireless systems such as cell phones, radio and television broadcasts is in the critical frequency range. This spectrum covers frequencies in the [225 MHz to 3.7 GHz] range.

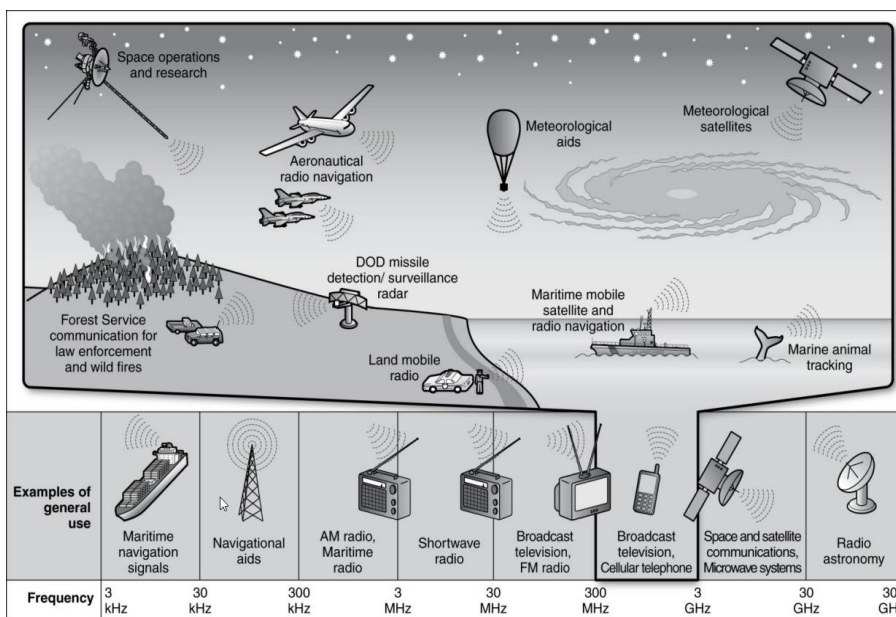


Figure 2 Dedicated Spectrum Uses and Federal Spectrum Uses with a Significant Value [16].

Sound perceivers identify the speaker by using unique variations and some aspects of the sound. RFF can mimic human speech in this regard. RFF uses the signal's time/frequency domain properties to automatically identify various radio and wireless devices. Almost all current and upcoming wireless communication standards employ OFDM [17].

What features of the signal are commonly extracted and what conclusions are drawn described below. In RF fingerprint capture, [18] uses SDR platform. Scrambling seed (from Descrambler), SFO (from Channel Estimator), CFO, and frame transient are the main features extracted (from OFDM Synchronizer). According to the article's conclusion, the results show that it is possible to identify Wi-Fi devices. And [19] conducted RFF on ZigBee devices using the SDR platform. In that study, DCTF, CFO, modulation shift, and I-Q shift properties were obtained. PSD coefficients are used in [20]. Because of the high performance of high-end receivers, it is emphasized when defining the RFF that identification accuracy is strictly related to the receiver. The identification accuracy of PSD coefficients and SNR is examined [21]. [22] used PSD as RFF for device identification. The identification performance degrades as the distance increases due to the multipath channel effect. The LTSP is subtracted from the time-domain signal received. The PSD is computed after the FFT. CFOs can also be calculated using a combination of different inputs.

In the literature, a number of learning datasets (protocol classifiers) for wireless communication have been published. Due to the acceleration in education, healthcare, e-commerce, computer vision and NLP in AI/ML and the lack of a common standard for organizing datasets, they are not yet integrated with a standard framework. Practitioners may be unable to access datasets because they are unaware of their existence [39]. Table 1 presents a summary excerpt from each explicitly available RF fingerprint datasets to educate those in this field.

Table 1 Summary Table of RFF Datasets

Made-up/ real-life	Freq. (GHz)	Waveform	Emmitter	Emmitter Count	Receiver	Dataset Ref.	Dataset Format
real-life	2.4	bluetooth	smartphones	86	TDS7404 Tektronix	[23]	.txt
real-life	2.4	out of standard	drone far controller	17	MSOS604A Keysight	[24]	.mat
real-life	1.09	ADS-B	aircraft	100	BladeRF	[25]	.mat
real-life	1.09	ADS-B	aircraft	>140	B210 (USRP)	[26]	.mat
made-up	2.45	Wi-Fi 2	X310	16	B210 (USRP)	[27]	SigMF
made-up	2.4065	out of standard	M100 Dji	7	X310 (USRP)	[27]	SigMF
made-up	2.685	Wi-Fi 2, LTE, 5G	X310	4	B210	[27]	SigMF
made-up	2.432	Wi-Fi 2/3	X310, N210	20	N210 (USRP)	[28]	SigMF

### 2.3 Classification of Features

The PLF are obtained by using the waveforms of the captured RF signals. It is categorized as position-dependent features and radio metrics that is position-independent features.

Position-independent Features: Due to defects in its analog components and manufacturing process, each transmitter has a separate RFF [29]. Device flaws are used to detect fingerprints used to identify devices. Some of these flaws include channel width, oxide thickness, and channel doping [30]. The primary goal of FE is to obtain an RFF profile that can be used to distinguish one transmitter from another. Previously, researchers [31] constructed an RFF using PSD and normalized PSD coefficients. Hall et al. [32] employs distinctive properties such as phase, amplitude, phase angle, and frequency. They use the DWT to extract these properties. The power amplifiers are the final component of the transmitter board. It is not easy for attackers to directly damage amplifiers with software. Power amplifier defects are also used in PL identification. Non-linear properties of power amplifiers can be

modeled using the Volterra series [33]. Passive Radiometric Device Identification System (PARADIS) was proposed by [34]. It makes use of frame size and phase errors, as well as I/Q origin offset and sync correlation. [35] uses transmitter phase shift and carrier frequency differences as fingerprints. It identifies devices with a second-order cyclic feature (SOCF). FE in radiometric techniques can be divided into transient and steady-state properties [34]. Transient-based methods [36] are adaptable but difficult to implement. It is based on time and frequency. I/Q instances are used as features in steady-state methods. Modulation-based methods have a better structure, but first the modulation scheme must be understood.

**Position-dependent Features:** The primary goals of RFF techniques (RFFTs) are to locate the device emitting the signal and the device from which signal originates [37]. RSS is an essential feature used in position-based RFFTs [38]. RSS is directly affected by the transmit power and channel attenuation of the transmitter. CSIR is another feature in classification and is extremely sensitive to motion. Furthermore, because location-related features are extremely sensitive to environmental changes, they cannot be used as individual fingerprints [30].

### 3. Feature Extracting

Transient features extracted from on/off transients or transmitted RF signal variations (envelope and phase shift of the transient signal) are used in device identification. The received signal is processed to extract stable features (such as SFO, CFO, and modulation features) [39]. A summary of studies with RFF in the literature is given in Table 2.

Table 2 An Overview of RFF Research Published in the Literature.

Based on	Year / Ref.	Parameter/ Method	Devices	Classification	Performance
modulation	2008 [34]	IQ offset, frequency error, phase and magnitude error, sync correlation.	802.11 NICs	SVM & k-NN	99.9% / SVM, 97% / k-NN
modulation	2009 [40]	spectral PCA features, modulation shape.	JCOP NXP 4.1 cards & e-passports	Mahalanobis distance	classification acc. 100%, identification acc. 97.5%
modulation	2017 [41]	IQ imbalance.	Matlab simulation	SVM	$\geq 90\%$ (SNR $\geq 15$ dB)
modulation	2019 [42]	IQ imbalance & DC offset	Phones, laptops & drones	CNN	98.6% (dataset:[27])
modulation	2020 [43]	time-domain RF signal	NI N210 & NI X310	CNN	Training and testing $\geq 87.41\%$
transient	2012 [44]	variance-based threshold.	Bluetooth transceivers	k-NN (obtaining energy envelope with STFT)	99.9%
transient	2009 [45]	variance-based threshold.	IEEE 802.15.4	Mahalanobis distance	$\geq 99.5\%$
transient	2014 [46]	phase based.	GSM phones	SVM	100%
wavelet	2009 [47]	Dual-tree complex wavelet transform	Wi-Fi 2 cards	Fisher-based MDA	$\geq 98\%$ (SNR $\geq 25$ dB)
wavelet	2019 [48]	Three-stage wavelet decomposition.	micro-UAV controllers	k-NN, SVM, DA, neural networks	k-NN 96.3%, SVM 96.84%
wavelet	2011 [49]	Wavelet packet decomposition, dynamic wavelet fingerprint.	Avery-Dennison AD 612 & Runway Gen 2	k-NN, SVM, LDC and QDC	99%

machine learning	2020 [50]	Time-domain RF signal	Four BS in the POWDER platform	CNN (augmented with triplet loss)	99.98% for 10 slices majority voting
machine learning	2020 [51]	RF signal spectrum (STFT method: RF signal to spectrum )	5 transmitters simulation	CNN	99.7%
deep-learning	2018 [52]	Bispectrum (Specific emitter identification (SEI))	E310, B210 & N210	CNN	>87%
deep-learning	2019 [53]	DCTF	CC2530 ZigBee modules	CNN	99.1% (SNR=30dB)
deep-learning	2020 [54]	Time-domain RF signal	Wi-Fi & ADS-B devices	CNN	Task 4F, 92.5% (per-transmission ADS-B accuracy)
deep neural networks	2020 [55]	Multiple data bursts	Dji M100 UAVs	CNN	>99%
transient & steady	2017 [56]	Empirical Mode Decomposition in SEI	Mobile phones & WLAN cards	SVM	transient >%93 (correct identification rate) SNR>0dB

### 3.1 Based on Modulation

The received frequency domain signal is used to FE. CNN (CFO) occurs when the carrier frequency is out of synchronization (when the signal down-conversion at the receiver (Rx) and the signal up-conversion at the transmitter (Tx) are inconsistent). The inter-carrier interference effect is caused by the CFO. OFDM performance is influenced by inter-carrier interference. SFO occurs when the sampling rate between the receiver and transmitter front ends is not synchronized. If the system is out of sync, the signal thus received may not be demodulated afterwards. The CFO is effective in synchronizing the system, it is calculated with the symbols LTSP and STSP. In the CFO's calculation, the literature uses the Moose algorithm [57] The CFO's  $\epsilon$  is represented by:

$$\mathbf{y}[\mathbf{n} + N_t] = \mathbf{y}[\mathbf{n}]e^{j\frac{2\pi N_t \epsilon}{N_t} F.T} \rightarrow \mathbf{Y}[\mathbf{n} + N_t] = \mathbf{Y}[\mathbf{n}]e^{2\pi\epsilon} \quad (1)$$

That is, the estimated CFO in the frequency domain:

$$\epsilon = \frac{1}{2\pi} \angle \left( \frac{\sum_{n=0}^{N_t-1} I_m\{y_1^*[n]y_2[n + N_t]\}}{\sum_{n=0}^{N_t-1} R_e\{y_1^*[n]y_2[n + N_t]\}} \right) \quad (2)$$

Even though the CFO is calculated and compensated at the receiver, it is calculated with LSTP for greater accuracy. The two are combined to calculate the OFDM system's CFO. It should be noted that the CFO is subject to change and thus requires constant supervision. When calculating SFO, the sliding window method is used to find the start of the data symbol [58]:

$$\delta = \arg \min \sum_{i=\delta}^{N_t-1+\delta} J_{SFO} \quad (3)$$

The cost function of estimated SFO:

$$J_{SFO} = |\mathbf{y}[\mathbf{n} + i] - \mathbf{y}[\mathbf{n} + N + i]| \quad (4)$$

A is the amplitude,  $\phi$  is the phase imbalance.  $y_I(t)$  In-phase (I),  $y_Q(t)$  quadrature (Q) paths outputs. If  $\hat{y}(t)$  is the ideal receive signal, the I-Q imbalance will have an effect on it:

$$\begin{aligned} \hat{y}(t) &= y_I(t) + y_Q(t) \\ &= R_e\{y(t)\} + jI_m\{Ae^{i\phi}y(t)\} \end{aligned} \quad (5)$$

I and Q are  $y_I(t) = \cos(\omega_0 t)$  and  $\widehat{y}_Q(t) = \sin(\omega_0 t)$ .  $\omega_0$  is the baseband signal. After RF signal is down-converted to baseband, the baseband signal that affects the I-Q imbalance [59] is:

$$\begin{aligned} \widehat{y}_I(t) &= \alpha \cos(\omega_0 t) + \widehat{\beta}_I \\ \widehat{y}_Q(t) &= \sin(\omega_0 t + \varphi) + \widehat{\beta}_Q \end{aligned} \quad (6)$$

Where  $\alpha = 1/A$  and  $\varphi$  are amplitude and phase errors caused by the I-Q imbalance defined above.  $\widehat{\beta}_I$  and  $\widehat{\beta}_Q$  are the DC biases of I and Q paths after down-converting. Removing these biases and substituting by  $\sin(\omega_0 t + \varphi) = \sin(\omega_0 t) \cos(\varphi) + \cos(\omega_0 t) \sin(\varphi)$ , the baseband signal has the following matrix form:

$$\begin{bmatrix} \widehat{y}_I(t) \\ \widehat{y}_Q(t) \end{bmatrix} = \begin{bmatrix} \alpha & \mathbf{0} \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix} \begin{bmatrix} y_I(t) \\ y_Q(t) \end{bmatrix} \quad (7)$$

$\alpha$  and  $\varphi$  can be calculated as:

$$\begin{aligned} \langle y_I(t) \cdot y_I(t) \rangle &= \alpha^2 \langle \cos^2(\omega_0 t) \rangle = \frac{\alpha^2}{2} \\ \rightarrow \alpha &= \sqrt{2 \langle y_I(t) \cdot y_Q(t) \rangle} \end{aligned} \quad (8)$$

$$\begin{aligned} \langle y_I(t) \cdot y_Q(t) \rangle &= \frac{\alpha^2}{2} \sin(\varphi) \\ \rightarrow \varphi &= \sin^{-1} \left( (\alpha^2/2) \langle y_I(t) \cdot y_Q(t) \rangle \right) \end{aligned} \quad (9)$$

In the literature, CFO, SFO, amplitude shift and phase shift properties are commonly extracted from modulation-based signals. It makes use of the IQ components (in-phase and quadratic signal data) of signals collected at large scales from two different wireless standards (COTS: commercial ready and ADS-B: used for aircraft status updates). Modulations contain information providing unique signature about I-Q imbalance, phase noise, and carrier frequency shift while an information signal is being transmitted to an other device [54].

### 3.2 Based on transient

With non-stationary characteristics, it is not easy to separate TS and channel noise from each others. In this section, Bayesian Step Change Detector, Bayesian Ramp Change Detector, Variance Fractal Dimension Threshold Detector, Phase Detector, Average Point of Change Detector, Permutation Entropy, and Supremacy of Energy Criteria approaches are examined.

#### 3.2.1 Bayesian step change detector

Based on Higuchi's method in [65], the variance of the fractal dimension is calculated for successive parts of the signal. In this case, the fractal dimension variance between two consecutive sequences is proportional to ppDF (posteriori probability distribution function). The sample instant to which the maximum value calculated from the probability distribution function (pDF) belongs is found as the transient starting instant as in Fig 3. To do this, first, subsets of samples are rearranged:

$$X(m, k): X(m), X(m+k), \dots, X\left(m + \left\lceil \frac{N-m}{k} \right\rceil \times k\right) \quad (10)$$

$X(m, k)$  is the subset interval,  $m$  is the start time, and  $k$  is the interval time. Calculation the length of the curve  $L_m(k)$  is, its for each subset is:

$$L_m(k) = \left\{ \left( \sum_{i=1}^{\frac{N-m}{k}} |x(m+ik) - x(m+(i-1)k)| \right) \frac{N-1}{\left\lceil \frac{N-m}{k} \right\rceil k} \right\} / k \quad (11)$$

The mean value of  $k$  clusters is plotted, a log-log scale ( $L_m(k)$ ). After the curve fitting is done, the fractal dimension is calculated using the slope of the curve.



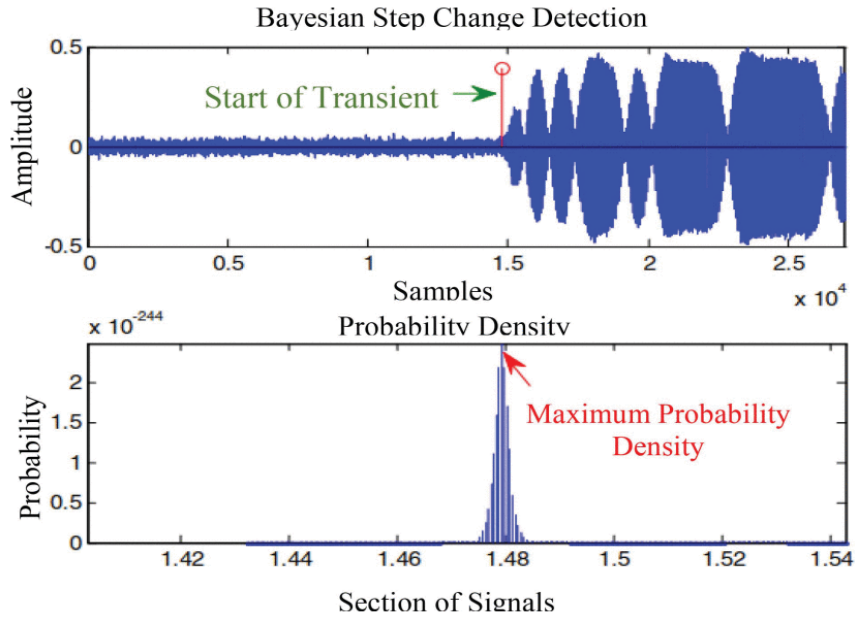


Figure 3 Bayesian step change detection on a sample signal [60]

The beginning of the transition ( $m$ ) is detected by tracking the ppDF in Equation 12. Here,  $N$  and  $d$  are the number of samples in a window and the fractal dimension respectively.

$$P(\{m\} | d) \propto \frac{1}{\sqrt{m(N-m)}} \left[ \sum_{i=1}^N d_i^2 - \frac{1}{m} \left( \sum_{i=1}^m d_i \right)^2 - \left( \frac{1}{N-m} \right) \left( \sum_{i=m+1}^N d_i \right)^2 \right]^{\frac{N-2}{2}} \quad (12)$$

### 3.2.2 Bayesian ramp change detector

Ureten and Serinken [61] proposed BRCD which is a modification of the BSCD. Transient due diligence is performed by estimating the point at which the signal's strength gradually increases. Prior to the transmission of actual data, typical transmission data includes channel noise. This signal's model is written in Equation 13 equation in matrix form.

$$d = Gb + e \quad (13)$$

$d$  is sample array in  $N \times 1$  dimension,  $G$  is a  $N \times M$  matrix of the basis functions estimated for each sample in the time series,  $b$  is an array in  $M \times 1$  dimension consist of linear coefficients, and  $e$  is  $N \times 1$  array of Gaussian noise examples. For change point determination, posteriori probability density is used [61]:

$$P(\{m\} | d, I) \propto \frac{[d^T d - d^T G(G^T G)^{-1} G^T d]^{\frac{N-m}{2}}}{\sqrt{\det(G^T G)}} \quad (14)$$

$I$  represents the pattern of the signal, the position of the starting point (SP) can be found in the matrix  $G$  in "as seen in Equation 15".

$$G^T = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 2 & 3 & \dots & N-m \end{bmatrix} \quad (15)$$

BRCD is more useful for Wi-Fi signals because it has 3 times lower standard deviation detection error than that of BSCD [62]. In fact, BRCD causes gradually an increase in power, such as Wi-Fi [60].

### 3.2.3 Variance fractal dimension threshold detector

VFDTD was proposed in [36]. It computes the fractal size of signal amplitude variance when detecting Wi-Fi transmitter transients. Furthermore, the VFDTD implementation is as follows [60]:

Calculation of fractal size of each segment of the signal given in Equation 16 where  $H$  denotes the Hurst index giving the correlation between  $\Delta X(t_i, \Delta t)$  and  $\Delta t$ .  $\Delta X(t_i, \Delta t)$  is amplitude difference between any two points of the signal, and  $\Delta t$  is sampling time that is  $\Delta t = |t_{i+1} - t_i|$ .

$$D(t) = 2 - H \tag{16}$$

Hurst index in the equation is calculated as in Equation 17 using least squares regression. In the equation,  $(x_i, y_i)$  pair is the pair of  $(\log(\Delta t_i), \log(\text{var}(\Delta X(t_i, \Delta t_i))))$ .

$$2H = \frac{N \sum_{i=1}^N x_i y_i - (\sum_{i=1}^N x_i)(\sum_{i=1}^N y_i)}{N(\sum_{i=1}^N x_i^2) - (\sum_{i=1}^N x_i)^2} \tag{17}$$

It is critical to select an appropriate time sequence and to ensure that there are enough  $(x_i, y_i)$  pairs. Next, we need to determine the SPoTS using the fractal size we have obtained, and then adjust the threshold  $\tau$  to be the average of the fractal size of the channel noise. If a set of values is less than the threshold value as given in Equation 18, then  $n$  is SPoTS.

$$D(n), D(n + 1), \dots, D(n + 450) \leq \tau \tag{18}$$

Figure 4 depicts the start of a wireless network card network core's temporal and fractal trajectory. The fractal dimension of the channel noise and crossover signal appears to differ significantly. These features determine the starting point's location, making it simple and quick. The threshold, on the other hand, is sensitive to noise and can only be determined through trial and error.

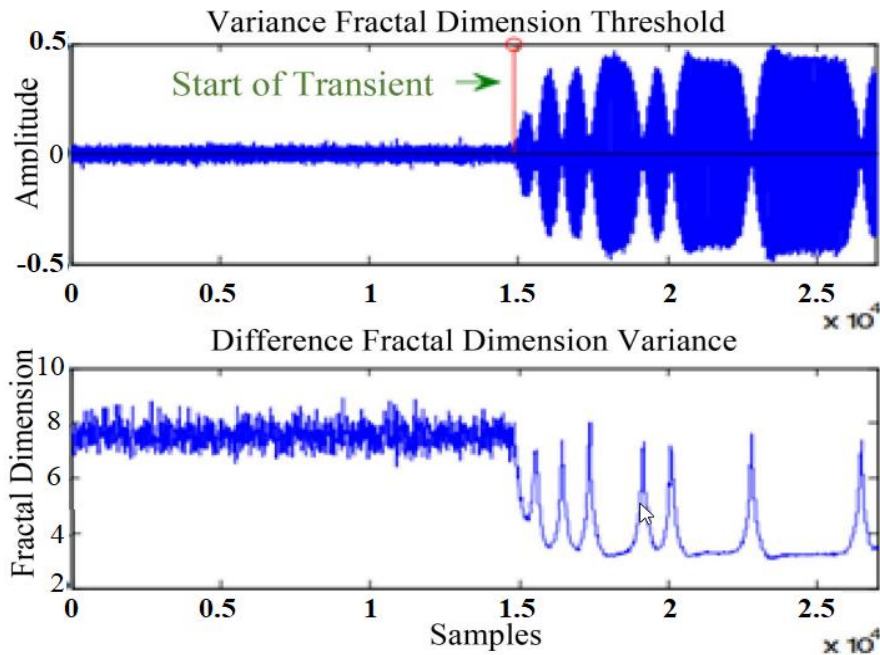


Figure 4 Variance fractal dimension threshold detection on a sample signal [60].

### 3.2.4 Phase detector

J. Hall proposed phase detection [32], which uses PCs. This method can be defined as follows: The Hilbert transform of a real signal can receive an analytical signal as in Equation 19 and 20.

$$X(t) = I(t) + jQ(t) \tag{19}$$

$$\theta(t) = \tan^{-1} \left[ \frac{Q(t)}{I(t)} \right] \tag{20}$$

$Q(t) = (s_q^a(n))$  and  $I(t) = (s_i^a(n))$ . However, the instantaneous phase of the signal in Equation 20, is unwrapped to remove the discontinuities caused by multiples of  $2\pi$  radians. Each element's AV (absolute value) in unwrapped vector is obtained as in Equation 21 in this method.

$$AV = \begin{cases} \theta(t) & |\theta(t) - \theta(t - 1)| \leq \pi \\ \theta(t) \pm 2\pi & \text{others} \end{cases} \quad (21)$$

TV (variance of phase) is calculated for each successive portion of AV to magnify the variation between the noise and transient portions of the signal as in Equation 22. To do this, size of a non-overlapping window (s) is used.

$$TV(i) = \text{var}(\overline{AV}(d + 1), \overline{AV}(d + 2), \dots, \overline{AV}(d + g)) \quad (22)$$

In the previous equation, i indeks takes values interval of  $[1, N/s]$ , g is  $i \times s$ , d is  $(i-1) \times s$ , and var represents the phase's variance. Finally, the difference in phase variance (PV) is calculated using Equation 23 in order to generate the fractal trajectory.

$$VT = |TV_i - TV_{i+1}|, i = 1, 2, \dots, \frac{N - w}{s} \quad (23)$$

It is obvious that the PV of a TS changes more slowly than the PV of noise. The onset of a TS and the detection of its fractal trajectory by PD are depicted in Figure 5. All in all, the onset of a transient state can be easily detected using this characteristic.

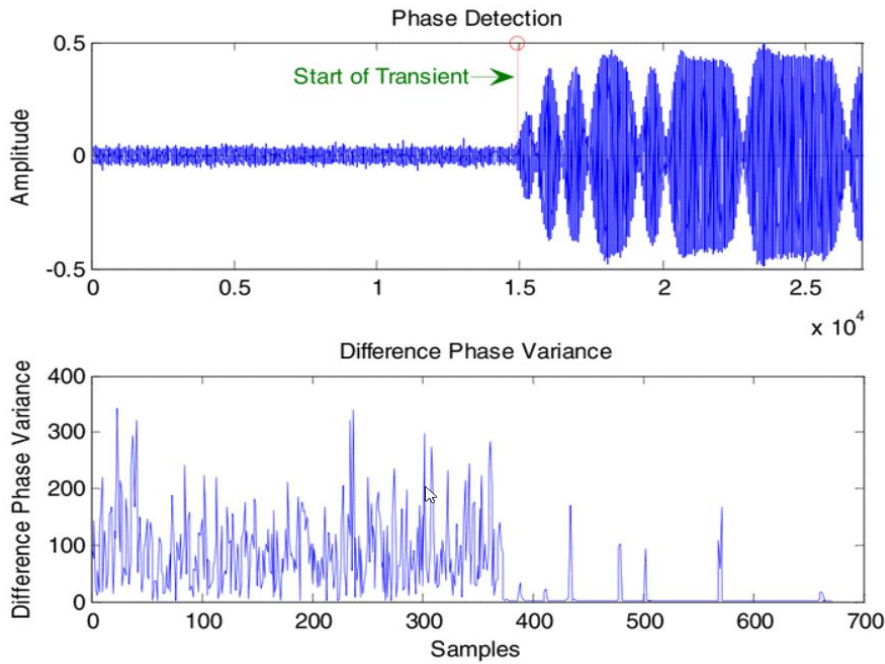


Figure 5 Phase detection on a sample signal [60].

Phase properties are used in PD sensing. Because noise has little effect on phase properties. It is quick and simple to detect the onset of the transient by changing the phase variance fractal trajectories; thus, its computational power is low and its robustness is high; however, there is a threshold problem [60].

### 3.2.5 Mean change point detector

In this method, difference between the statistics of the samples is taken as main principle. As can be seen from Figure 6, the sampling moment or index where the greatest difference is found is taken as the SPoTS [60].

The temporal vector is divided into two parts:  $x_1, x_2, \dots, x_{i-1}$ , and  $x_i, x_{i+1}, \dots, x_N$ . The average and statistics of each section are calculated as in following equations.

$$S_i = \sum_{n=1}^{i-1} (x_n - \bar{X}_{i1})^2 + \sum_{n=i}^N (x_n - \bar{X}_{i2})^2 \quad (24)$$

$\bar{X}$  is the mean of the combined partitions and the statistics ( $S$ ) of the real sample are expressed below:

$$S = \sum_{n=1}^N (x_n - \bar{X})^2 \quad (25)$$

The point having the largest amplitude of the  $S - S_i$  curve is the start point of the transient. The idea behind MCPD is to enlarge the difference, and then determine the where the maximum value occurs to be starting point of the transient [60].

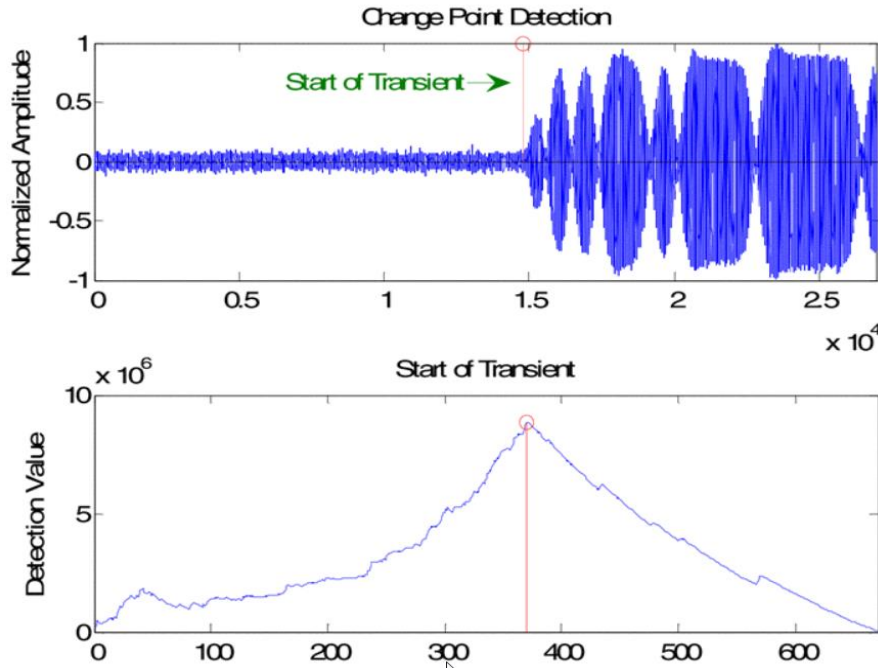


Figure 6 Mean change point detection on a sample signal [60].

### 3.2.6 Permutation entropy (PE) and generalized likelihood ratio test detector

Bandt-Pompe introduced PE, which can assess the irregularity and complexity of time series [63]. This method detects a TS using PE and GLRTDs. A GLRTD is used to determine the SP of the captured signal's PE [64]. The  $X_i, (i = 1, 2, \dots, N)$  time series are formed in an  $m$ -dimensional space as follows to calculate the PE:

$$X_i = [x(i), x(i + l), \dots, x(i + (m - 1)l)] \quad (26)$$

where  $l$  is the time lag,  $x(i)$  denotes the  $i$ -th point in  $m$ -dimensional space;  $1 \leq i \leq N - (m - 1)l$ . The actual  $X_i$  values in Equation 26 are then sorted in ascending as in Equation 27:

$$X_i = [x(i + (j_1 - 1)l) \leq x(i + (j_2 - 1)l) \leq \dots \leq x(i + (j_m - 1)l)] \quad (27)$$

When an equality occurs, sorting can be done according to their corresponding index of  $j$ . That is, if  $j_{n1} < j_{n2}$ , then the order is  $x(i + (j_{n1} - 1)l) \leq x(i + (j_{n2} - 1)l)$ , else the order is  $x(i + (j_{n2} - 1)l) \leq x(i + (j_{n1} - 1)l)$ . A permutation pattern  $\pi$  can be used to map the vector  $X_i$ :

$$\pi_i = [j_1, j_2, \dots, j_m] \quad (28)$$

$j$  in Equation 28 is the time index. One of the  $m!$  permutations of  $m$  different signs is  $\pi_i$ . The probability of finding  $\pi_i$  is easily calculated with  $p(\pi_i) = f(\pi_i) / (N - (m - 1)l)$ . In the equation  $f(\pi_i)$  is the number of occurrences of  $\pi$ . Finally, Shannon Entropy is used to calculate the PE [65]:

$$0 \leq H_p = - \sum_{j=1}^K p_j \ln p_j / \ln (m!) \leq 1 \quad (29)$$

In Equation 29,  $K$  is the number of different signs  $[\pi_1, \pi_2, \dots, \pi_{N-(m-1)l}]$ . SPoTS can be identified using PE data. Firstly, the PE trajectory of the transient can be computed using a rectangular window of length  $L_{wnd}$  that scrolls one sample at a time. A signal's PE is smaller than the noise series' PE. The main reason for this is the noise's irregularity. The following equation can be used to easily model the PE trajectory:

$$H_P(n) = \begin{cases} H_{pn}(n) & 1 \leq n \leq n_0 \\ H_{pt}(n) & n_0 \leq n \leq n_1 \\ H_{ps}(n) & n_1 + 1 \leq n \leq N \end{cases} \quad (30)$$

where  $n$  denotes the  $n$ th slide,  $H_p$  is the corresponding PE,  $N$  is the total of sliding,  $n_0$  is the first time there is a TS in the sliding window, and  $n_1$  is the last time there is a TS in the sliding window.  $H_{pn}$  is the probability of noise;  $H_{pt}$  is the probability of TS in the sliding window; and  $H_{ps}$  is the probability of stable signal. It is self-evident that  $H_{pn} > H_{pt} > H_{ps}$ .

PE begins to decrease when there is a transient in a sliding window, and PE changes slightly for a stable signal in the sliding window. The PE for slides with a TS is modelled as follows: [64]:

$$H_P(n) = \begin{cases} A_0 + w(n) & 1 \leq n \leq n_0 \\ A_0 + k \times (n - n_0) + w(n) & n_0 \leq n \leq N_0 \end{cases} \quad (31)$$

In Equation 31,  $w(n)$  denotes Gaussian noise with zero-mean and  $\sigma$  standard deviation;  $A_0$  is the mean of  $H_{pn}(n)$ ;  $k$  is the decreasing slope after  $n_0$ . When  $T_0$  is the mean PE,  $n_0$  is the first slide containing the TS;  $N_0$  denotes the changing point when  $n \leq N_0$ ,  $H_{pn}(n) > T_0$  and  $H_{pn}(N_0 + 1) \leq T_0$  and is computed as in Equation 32 and 33.

$$T_0 = \frac{\max(H_P) + \min(H_P)}{2} \quad (32)$$

The binary hypothesis test can be used to solve the transient detection problem:

$$H_0: A_0 + w(n) \\ H_1: \begin{cases} A_0 + w(n) & 1 \leq n \leq n_0 \\ A_0 + k \times (n - n_0) + w(n) & n_0 \leq n \leq N_0 \end{cases} \quad (33)$$

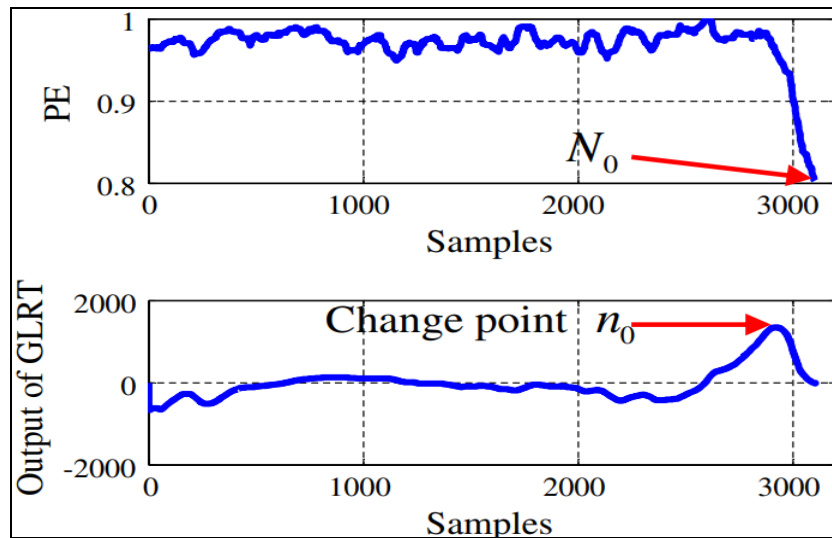


Figure 7 For a PE Trajectory (upper) Output of GLRT Dedector (lower) [64].

$H_P(n)$ 's GLRTD can be represented as: [66]:

$$L_G(x) = \frac{p(x; n_0, H_1)}{p(x; H_0)} = \frac{p(x; A_1 = \hat{A}_0, A_2 = \hat{A}_0 + \hat{k} \times (n - n_0), H_1)}{p(x; A_1 = \hat{A}_0)} \quad (34)$$

$p(x; n_0, H_1)$  and  $p(x; A_1)$  are computed as shown below; since  $A_0$  and  $k$  are unknown, instead of them their MLE can be used [67, 68].

$$p(x; A_1, A_2) = \frac{1}{(2\pi\sigma^2)^{N_0/2}} \exp \left[ -\frac{1}{2\sigma^2} \left( \sum_{n=1}^{n_0} (x(n) - A_1)^2 + \sum_{n=n_0+1}^{N_0} (x(n) - A_2)^2 \right) \right] \quad (35)$$

$$p(x; A_1) = \frac{1}{(2\pi\sigma^2)^{N_0/2}} \exp \left[ -\frac{1}{2\sigma^2} \left( \sum_{n=1}^{N_0} (x(n) - A_1)^2 \right) \right] \quad (36)$$

To determine  $A_0$  under the two hypotheses  $H_0$  and  $H_1$ , let the MLE of  $A_0$  under  $H_0$  and  $H_1$  be  $\hat{A}_{00}$  and  $\hat{A}_{01}$ , respectively.

$$\hat{A}_{00} = \hat{A}_0 = \frac{1}{N_0} \sum_{n=1}^{N_0} H_p(n) \quad (37)$$

$$\hat{A}_{01} = \hat{A}_0 = \frac{1}{n_0} \sum_{n=1}^{n_0} H_p(n) \quad (38)$$

The least squares fitting algorithm can estimate the MLE of slope  $k$  algorithm [65] and is provided below:

$$\hat{k} = \frac{(N_0 - n_0) \sum_{n=1}^{N_0-n_0} n H_p(n + n_0) - \sum_{n=1}^{N_0-n_0} n \sum_{n=1}^{N_0-n_0} H_p(n + n_0)}{(N_0 - n_0) \sum_{n=1}^{N_0-n_0} n^2 - (\sum_{n=1}^{N_0-n_0} n)^2} \quad (39)$$

The GLRTD is defined using the above equations as follows [64]:

$$\begin{aligned} & \text{Ln} \left( L_G(H_p(n)) \right) \\ &= \frac{1}{2\sigma^2} \left[ \sum_{n=1}^{N_0} (H_p(n) - \hat{A}_{00})^2 - \sum_{n=1}^{n_0} (H_p(n) - \hat{A}_{01})^2 \right. \\ & \quad \left. - \sum_{n=n_0+1}^{N_0} (H_p(n) - \hat{A}_{01} - \hat{k} \times (n - n_0))^2 \right] \end{aligned} \quad (40)$$

The GLRTD's maximum is the estimated SPoTS  $n_0$  [64]:

$$\hat{n}_0 = \arg \max_n \left[ \text{Ln} \left( L_G(H_p(n)) \right) \right] \quad (41)$$

As shown in Figure 7, when the PE trajectory falls down, the GLRTD output occurs in there, which can be identified as the change point  $n_0$ . It is reasonable to conclude that a very small number of signal samples in the sliding window cannot result in a noticeable decrease in the PE trajectory.

### 3.2.7 Superiority of energy criterion

This technique, which is widely used to predict the arrival time of signals in a variety of applications, is also a pioneer in detecting acoustic and electromagnetic partial discharges. The basic idea behind energy criterion (EC) is to characterize the arrival of a signal by a change in energy content. A sampled signal's ( $x$ ) energy ( $E_i$ ) is the sum of its amplitude values. [69], [70].

$$E_i = \sum_{k=0}^i x_k^2, i = 1, \dots, N \quad (42)$$

The length of the signal is represented by  $N$ . As follows, the signal is isolated from the noise component:

$$E'_i = E_i - i\delta = \sum_{k=0}^i (x_k^2 - i\delta) \quad (43)$$

$\delta$  in Equation 43, defined as in Equation 44.

$$\delta = \frac{E_N}{\vartheta \cdot N} \tag{44}$$

The  $\vartheta$  factor lessens the delay effect of  $\delta$ . As a result, the parameters that  $\delta$  influence are the total energy of the signal ( $E_N$ ) and the  $\vartheta$  factor. Two methods can be used to use the EC technique for transient SP detection: the EC (EC-a) method based on  $\mathbf{a}(\mathbf{n})$  features and the EC (EC- $\emptyset$ ) method based on  $AV(\mathbf{n})$  features.

When using the EC-a method to calculate ( $E'_i$ ), we first use the  $\mathbf{a}(\mathbf{n})$  features of the analytical signal found in Equation 45.

$$\mathbf{a}(\mathbf{n}) = \sqrt{(s_I^a(\mathbf{n}))^2 + (s_Q^a(\mathbf{n}))^2} \tag{45}$$

The energy curve's global minimum is then defined. The sample corresponding to the global minimum is used to determine the starting point of the transient. However, within a flat region, there may be several local minimums. In this case, the transition SP can be determined by selecting the region's first local minimum. It should be noted that the  $\delta$  factor chosen has a significant influence on the energy curve as seen in Equation 44. The value of the  $\delta$  factor under noise-free conditions is  $\delta = [1, 2, \dots, 100]$  [70]. When considering different SNR levels, the  $\delta$  factor value should be determined empirically. In this context, they discovered that when  $\delta = 30$  for the given data set, the detection accuracy increases significantly [71].

Figure 8 illustrated the energy curve computed using EC-a for  $\delta = 1, 2, 30$  and the discovered starting points.

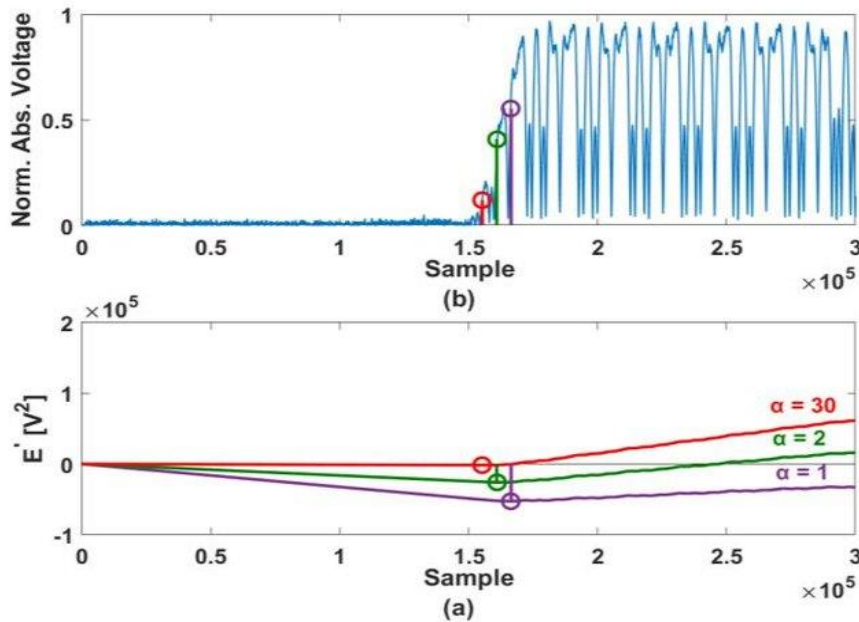


Figure 8 Illustration the energy curve obtained by EC-a method (lower) and the determined transient starting point (upper) [71].

The EC- a method is based on using  $AV(\mathbf{n})$  in Equation 46.

$$AV(\mathbf{n}) = \begin{cases} \emptyset(\mathbf{n}) & |\emptyset(\mathbf{n}) - \emptyset(\mathbf{n} - 1)| \leq \pi \\ \emptyset(\mathbf{n}) \pm 2\pi & \text{otherwise} \end{cases} \tag{46}$$

The basic logic is to generate another random signal with roughly equal variance by using the random change in the noise portion of the signal's unwrapped IP features. In the noise part of the signal, a monotonically increasing energy curve is expected to be obtained using this signal. The starting point is the global maximum point of the curve. As a result, the method begins by calculating the absolute differences between each mean window of the signal's unwrapped instantaneous PCs. After calculating  $E'_i$ , the maximum of the curve is shown in Figure 9(a). In the unwrapped instantaneous PCs

of the signal, the example corresponding to the window index providing the global maximum of the curve is defined in Figure 9(b). Figure 9(c) shows the determination of the starting point.

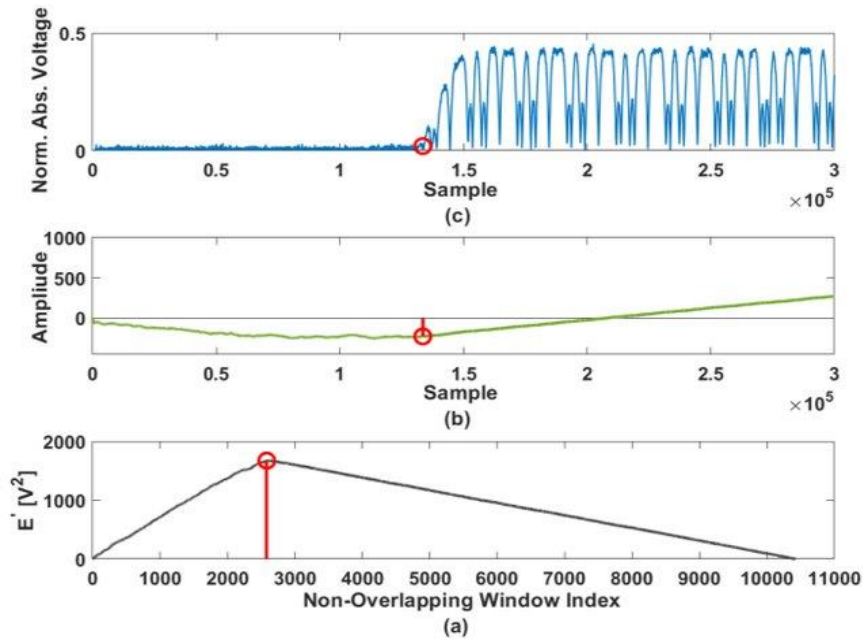


Figure 9 (a) Energy curve generated by the EC-  $\emptyset$  method, (b) instantaneous phase signal, (c) the determined of the starting point [71].

The transient-based signal characteristic recognition algorithms available in the literature are summarized in Table 3.

Table 3 Summary Table Transient Detection Algorithms.

Algorithms Ref.	Pros	Cons	Complexity	Success Rate	Signal/SNR
BSCD [72]	no threshold needed, high detection rate (hiDeR) (with suitable amplitude/without leading response).	weak detection (with small amplitude) for TS, need a long time, complicated calculation.	$O(n^3)$	% 80-85  Wi-Fi 1 transceiver	Radio/NA
BRCd [73]	no threshold needed, outperforming BSCD.	works well in signal models with linear power increases, complex calculation.	N/A	% 95  Wi-Fi 1 transceiver	Wi-Fi 1/NA
VFDTD [74]	hiDeR	threshold needed, highly sensitive to noise, need long time, complicated calculation.	$O(n^2)$	N/A	Radio/NA
PD [75]	fast and simple	less susceptible to noise, practically define a starting point, poor detection rate in low SNR.	$O(n)$	% 85-90  Wi-Fi 1 transceiver	Bluetooth/NA
MCPD [76]	no threshold needed, high detection, simple	takes long time to compute.	$O(n)$	% 90-92.5  8 different transmitters	Wi-Fi/6-30dB



PE & GLRT [64]	no threshold needed, hiDeR, detection of the start point is extremely accurate.	complicated calculation.	N/A	N/A	GSM/0-25dB
EC [71]	more effective different SNR levels	N/A	O(n)	N/A	Wi-Fi/-3-25db

### 3.3 Based on Steady-State

The unrivalled features extracted from the modulated signals are the focus of some steady-state studies. Gerdes and colleagues in their work [77], they proposed a based on steady-state RFF and preferred cards of the same manufacturer and model. The IEEE Ethernet 802.3 input part is used to identify the fingerprint profile, as well as the device emitting the signal. In the classification, a basic threshold and a matching filter application were used. [34] proposed a PARADIS. This system identifies the physical layer of a modulated signal based on five properties (frequency error, synchronous correlation, I/Q origin offset, magnitude and phase errors). The k-NN and SVM classifiers were used to create the RFF profile. To demonstrate the classifier's accuracy, 138 identical model Wi-Fi 1 signals are used. These signals were captured with a vector signal analyzer at distances in the interval of (3,15) meters from the antenna. With their proposed method, Shi and Jensen hoped to define Multiple Input Multiple Output devices. It has become a system comparable to PARADIS by utilizing the radiometric properties of these devices in modulation [78]. They used modulation-based approaches to classify RFID devices. They make use of spectral features from RFID transmitters as well as modulation features. Four different RFID transmitter classes and models are tested in the study (ISO 14443, HF 13.56 MHz) [40]. Frequency domain features were used in the study to identify RFF transmitters. The use of FFT allows for a great deal of flexibility in spectral feature selection. In laboratory testing, eight USRP transmitters are used. Optional feature selection the k-NN discriminator is used to generate the classification engine automatically. It achieves 97 and 66 percent accuracies at 30dB SNR and at 0dB SNR respectively. It also provides a less expensive alternative to the its counter approach requiring very high speed ADCs [79]. Suski and colleagues for their unique feature selection, they used the PSD coefficients in the Wi-Fi 2/3 signal input [80]. Table 4 details the IEEE 802.11 standards [81-89]. Integration employs the feature selection method, as opposed to other known feature selection methods (RELIEF-F, F Score, and Laplacian Score). The covariance feature is used as an RF fingerprint, and the K-Nearest Neighbor (KNN) classifier is used. The Spearman correlation coefficient is used to assess the method's stability [90]. It is a fact that the steady state component of the signal is not shared by all transmitters. On the other hand, transient part of the signal is always present. As a result, the study focuses on transient-based RFF. It is a significant difficulty to obtain the amplitude of the signal, in this context a higher sampling rate is needed to be able to detect the starting of the transient [79]. WLAN, RFID, and almost all other technologies use preamble as it simplifies receiver design at the start of transmission. Therefore, these approaches do not require a steady-state signal [31]. For deep learning RFF approaches, Yu et al. offer a general Denoising Auto Encoder based model. A partially stacking technique has also been developed for efficiently identifying ZigBee devices using both quasi-stable and steady-state RFFs. Under AWGN channels at lower SNRs (-10 dB to 5 dB), their suggested PSCDAE beats traditional CNN by 14 to 23.5 percent in terms of identification accuracy [91].

Table 4 Information of IEEE 802.11 Standards.

Release date	Standard	Common name	Freq. (GHz)	Modulation type	Bandwidth (MHz)	Data speed (bps)	Approx. range (meter)	Number of clients
1997	802.11	Wi-Fi 0	2.4	DSSS, FHSS	22	2 M	20-100	N/A
1999	802.11a	Wi-Fi 2	5	DSSS	20	54 M	35-120	N/A
1999	802.11b	Wi-Fi 1	2.4	CCK	22	11 M	35-140	N/A
2003	802.11g	Wi-Fi 3	2.4	OFDM	20	54 M	38-140	N/A
2009	802.11n	Wi-Fi 4	2.4 & 5	OFDM	20-40	600 M	70-250	<50
2013	802.11ac	Wi-Fi 5	5	OFDM	20-40-160	6.9 G	35-...	50-100

2019	802.11ax	Wi-Fi 6	2.4 & 5	OFDM, OFDMA	80-160	9.6 G	N/A	200-400
2020	802.11ax	Wi-Fi 6E	6	OFDMA	80-160	9.6 G	N/A	200-400
Expected in (2 <sup>nd</sup> half of 2022)	802.11be	Wi-Fi 7	2.4, 5 & 6	OFDMA	320	30 G	N/A	N/A

### 3.4 Other Methods

These approaches typically employ a proprietary wireless technology and/or extract additional signal and logical layer features [92], [47]. The PL is described by Danev et al. using the modulation pattern, spectral characteristics, and timing of device response signals. Timing and modulation are used to distinguish devices from various manufacturers, while spectral features are used to identify devices from the same manufacturer when fingerprints are used to identify devices [40]. Jana and Kasera identified access points in a wireless local area network using clock skew as a distinguishing feature [92]. In [93], the effectiveness of this technique for complex networks has been demonstrated. The results demonstrated that various access points could be distinguished with high accuracy. 802.11a OFDM signal devices are defined by a complex wavelet transform. MDA is used to categorize the features [47], [94]. To identify wireless devices, Suski et al. [95] generates an RF fingerprint. It makes use of the PSD of the Wi-Fi 2 preamble and spectral correlation is used for classification. When the SNR value of the captured packet frames is greater than six decibels, the average classification error rate is 20 percent in this method, which was tested on three devices. Recent research has focused on various RFID classes for PL identification [96], [97]. Periaswamy et al. [97], [98] used UHF-RFID tags to identify devices. According to the results of the study, the minimum power response feature can be used to identify devices with a 94.4 percent success rate. Recently, researchers looked into various signal characteristics and signal components [99], [6] in GSM devices. They identified and classified devices from four different manufacturers by using the intermediate and temporal parts of the GSM-GMSK burst signals. When the results of GSM signal identification are examined, it is discovered that the near temporal part is more effective in classification accuracy, while the mid-level part is less effective. Padilla et al. assess system performance using 20 Wi-Fi device datasets with 15 fingerprint samples per device. Both methods combine subspace transform-based feature reduction techniques with similarity-based analysis techniques such as PCA and PLS regression as identification methods. When only one device per manufacturer is used, accuracy is greater than 90%, and accuracy is around 70% when two devices per manufacturer are used [100]. To extract RFF features, the DCTF, a two-dimensional representation of the differential relationship of signal time series, is used. When defining devices, the developed DCTF-CNN is used [53]. Furthermore, HHT [101], EMD and Welch methods, which are employed in signal classification in several domains, will add to the literature if used to RFF [102].

## 4. Classification Methods

The classification methods used in the literature can be summarized as in Figure 10. As seen in the figure, methods divide into two main category as supervised and unsupervised. Unsupervised learning is not effective if there is prior tag information about devices. For Wi-Fi fingerprinting, infinite hidden Markov random field (ihMrf) based unsupervised clustering techniques are proposed using online classification algorithm and batch updates [103]. Transmitter features are used in [35], where Bayesian approach passively classifies equipments unsupervised.

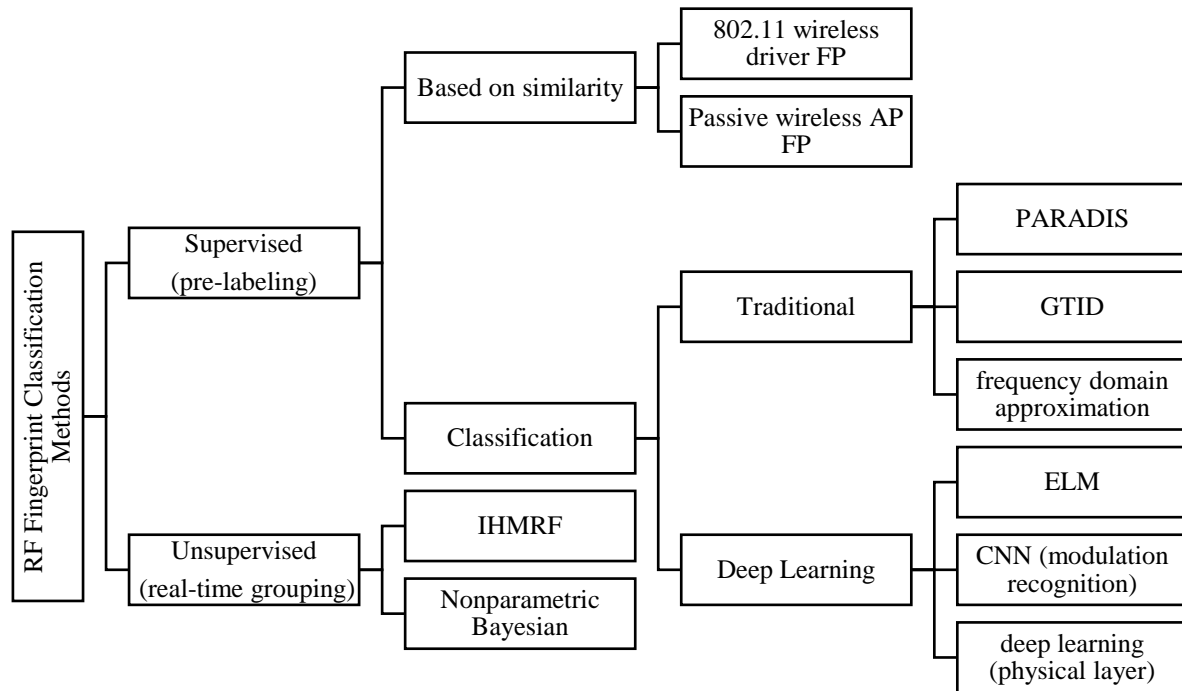


Figure 10 Perspective on RFF Classification.

In supervised learning, the network requires multiple labeled samples gathering prior to deployment to train for ML algorithm [104]. Below are studies using supervised learning-based methods in four different categories.

**Based on Likeness:** Comparing the observed signature of the transmitting device with records in a master database is necessary for similarity metrics. A passive fingerprint technique has been proposed in [105], to identify the Wi-Fi device driver running on an IEEE 802.11. Analysis of the collected traces and fingerprinting of device drivers is done using the Supervised Bayes approach. Using wavelet analysis [106] describes a passive black box-based technique that uses the time from TCP or UDP packet to determine type of access points. These techniques are based on priory knowledge about vendor-specific features.

**Classification-Based:** As can be seen in Figure 10, there are studies in the literature on classification-based supervised learning that makes use of RF features such as I/Q and phase imbalance, frequency error and RSS.

**Traditional:** In traditional classification, matching with pre-selected features is examined using the domain knowledge of the system. To do this, dominant features must be known beforehand. The method proposes a classification based on subtracting known input parts and calculating spectral ingredients. The log spectral energy property is given as input to the k-nearest neighbors (KNN) discriminant classifier [79]. PARADIS achieves 99% accuracy using SVM and KNN algorithms, fingerprinting 802.11 Wi-Fi devices, based on modulation specific errors in the frame [34]. A structure called GTID is proposed for physical device classification with artificial neural networks. This structure takes advantage of variations in clock skewness as well as hardware combinations of devices [107]. They investigated the problem of detecting and classifying micro-UAV control signals. The proposed detection method executes a Bayesian approach based on the Markov models of UAV and non-UAV classes, while the classification method relies on energy-time domain RF signal and uses features (skewness ( $\gamma$ ), variance ( $\sigma^2$ ), energy spectral entropy (H), and kurtosis ( $\kappa$ )) extracted in this domain [48]. The mathematical calculations of these properties are given in the following equations.

$$\kappa = \frac{1}{L\sigma^4} \sum_{n=1}^L (\alpha(n) - \mu)^4 \quad (47)$$

$$\gamma = \frac{1}{L\sigma^3} \sum_{n=1}^L (\alpha(n) - \mu)^3 \quad (48)$$

$$\sigma^2 = \frac{1}{L} \sum_{n=1}^L (\alpha(n) - \mu)^2 \quad (49)$$

$$\mu = \frac{1}{L} \sum_{n=1}^L \alpha(n) \quad (50)$$

Choosing an appropriate feature set is an important huge duty when using many different features. When there are many devices, scalability problems may occur. This causes to increased computational complexity in training.

Deep Learning is also a popular approach in recent years using supervised learning. It is a network structure consisting of many layers, capable of solving complex problems by processing big data. It implements deep learning at the PL, focusing on modulation recognition using CNNs [108] [109]. However, it does not define a device as Riyaz et al. does, it only defines the modulation type used by the transmitter [104]. Three deep learning models (CNN, LSTM and MLP) were found successful in the literature, considering the characteristics of IQ samples, FFT results and spectrogram. In the literature, it appears that CNN is efficient in processing spatially relevant data such as images (spectrogram) in deep learning, whereas LSTM is efficient in temporally related time series (IQ samples) [110]. AlexNet, GoogleNet, VGG16, and ResNet are examples of popular CNN models. In the RF field, two new models are proposed as deep CNN architectures, inspired by Alex-Net and ResNet [54].

Extreme Learning Machines (ELM) was proposed for single layer neural networks by G. Huang in 2006. It presents a fast and not iterative numeric supervised learning. ELM provides good generalization performance at extremely fast learning speed [111, 112]. One of its most important features is that it does not require iterative calculations based on derivatives. It uses pseudo inverse computations for determining networks parameters [113]. This area is very untouched in RFF. A long time is required for the training of the above-mentioned structures used in deep learning. ELMs have the potential to reduce this time to extremely low values with an extremely fast operation. In this context, it is considered as an open field that is recommended to be used in the future.

## 5. Conclusion

Finally, this review focuses on the rapid development and widespread use of IoT and the security part. Considering the IoT's own hardware resources, the use of RFF to ensure security due to the error experienced during production at the physical layer draws attention. Therefore, RFF methods for Wi-Fi communication devices have been reviewed. Essentially, unique features from Wi-Fi communication devices are extracted and adapted to two-factor authentication systems for identification purposes. SDRs take the lead in signal capture and preprocessing to support different communication protocols. This review gives a summary of the most recent RFF detection and extraction techniques. FE methods used for different fingerprinting methods are detailed in this review.

## Acknowledgments

This study is supported by the project numbered 2021-01.BŞEÜ.01-01 within the scope of Bilecik Şeyh Edebali University Scientific Research Projects.

## References

- [1] (03.10.2022). *Hackersnewbulletin*. "Chinese Irons have hidden chips which serve malware in systems". Available: <http://www.hackersnewsbulletin.com/2013/11/russia-chinese-irons-hidden-chips-serve-malware-systems.html>
- [2] M. Z. Gündüz and R. Daş, "Internet of things (IoT): Evolution, components and applications fields," *Pamukkale University Journal of Engineering Sciences*, vol. 24, pp. 327-335, 2018.
- [3] D. Nouichi, M. Abdelsalam, Q. Nasir, and S. Abbas, "Iot devices security using rf fingerprinting," in *2019 Advances in Science and Engineering Technology International Conferences (ASET)*, 2019, pp. 1-7.
- [4] J. Pohl and A. Noack, "Universal radio hacker: A suite for analyzing and attacking stateful wireless protocols," in *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, 2018.
- [5] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys (CSUR)*, vol. 45, pp. 1-29, 2012.
- [6] M. D. Williams, M. A. Temple, and D. R. Reising, "Augmenting bit-level network security using physical layer RF-DNA fingerprinting," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 2010, pp. 1-6.
- [7] R. Akeela and B. Dezfouli, "Software-defined Radios: Architecture, state-of-the-art, and challenges," *Computer Communications*, vol. 128, pp. 106-125, 2018.
- [8] M. Gummineni and T. R. Polipalli, "Implementation of reconfigurable transceiver using GNU Radio and HackRF One," *Wireless Personal Communications*, pp. 1-17, 2020.
- [9] H. Miyashiro, M. Medrano, J. Huarcaya, and J. Lezama, "Software defined radio for hands-on communication theory," in *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, 2017, pp. 1-4.
- [10] M. Sruthi, M. Abirami, A. Manikoth, R. Gandhiraj, and K. Soman, "Low cost digital transceiver design for Software Defined Radio using RTL-SDR," in *2013 international mutli-conference on automation, computing, communication, control and compressed sensing (iMac4s)*, 2013, pp. 852-855.
- [11] W. Xiang, F. Sotiropoulos, and S. Liu, "xRadio: an novel software defined radio (SDR) platform and its exemplar application to vehicle-to-vehicle communications," in *International Conference on Ad-Hoc Networks and Wireless*, 2015, pp. 404-415.
- [12] J. Seo, Y.-H. Chen, D. S. De Lorenzo, S. Lo, P. Enge, D. Akos, *et al.*, "A real-time capable software-defined receiver using GPU for adaptive anti-jam GPS sensors," *Sensors*, vol. 11, pp. 8966-8991, 2011.
- [13] Y. Chen, S. Lu, H.-S. Kim, D. Blaauw, R. G. Dreslinski, and T. Mudge, "A low power software-defined-radio baseband processor for the Internet of Things," in *2016 IEEE international symposium on high performance computer architecture (HPCA)*, 2016, pp. 40-51.
- [14] Y. Park, S. Kuk, I. Kang, and H. Kim, "Overcoming IoT language barriers using smartphone SDRs," *IEEE Transactions on Mobile Computing*, vol. 16, pp. 816-828, 2016.
- [15] J. N. Samuel, "Specific emitter identification for GSM cellular telephones," University of Pretoria, 2018.
- [16] B. Skorup, "Reclaiming federal spectrum: Proposals and recommendations," *Colum. Sci. & Tech. L. Rev.*, vol. 15, p. 90, 2013.
- [17] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "An IEEE 802.11 a/g/p OFDM Receiver for GNU Radio," in *Proceedings of the second workshop on Software radio implementation forum*, 2013, pp. 9-16.
- [18] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting Wi-Fi devices using software defined radios," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016, pp. 3-14.
- [19] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, "Design of a hybrid RF fingerprint extraction and device classification scheme," *IEEE Internet of Things Journal*, vol. 6, pp. 349-360, 2018.

- [20] S. U. Rehman, S. Alam, and I. T. Ardekani, "An overview of radio frequency fingerprinting for low-end devices," *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, vol. 6, pp. 1-21, 2014.
- [21] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," *IET Communications*, vol. 8, pp. 1274-1284, 2014.
- [22] T.-Y. Lin, C.-M. Lai, and C.-W. Chen, "Using SDR Platform to Extract the RF Fingerprint of the Wireless Devices for Device Identification," in *CS & IT Conference Proceedings*, 2020.
- [23] E. Uzundurukan, Y. Dalveren, and A. Kara, "A database for the radio frequency fingerprinting of Bluetooth devices," *Data*, vol. 5, p. 55, 2020.
- [24] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Drone remote controller RF signal dataset," *IEEE Dataport*, 2020.
- [25] Y. Liu, J. Wang, S. Niu, and H. Song, "ADS-B signals records for non-cryptographic identification and incremental learning," *IEEE, Piscataway, NJ, USA, Data Set*, 2021.
- [26] Y. Liu, J. Wang, H. Song, S. Niu, and Y. Thomas, "A 24-hour signal recording dataset with labels for cybersecurity and IoT," *IEEE, Piscataway, NJ, USA, Data Set*, 2020.
- [27] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges," *arXiv preprint arXiv:2201.00680*, 2022.
- [28] A. Al-Shawabka, F. Restuccia, S. D'Oro, and T. Melodia, "Massive-Scale I/Q Datasets for WiFi Radio Fingerprinting," *Computer Networks*, vol. 182, p. 107566, 2020.
- [29] S. Dolatshahi, A. Polak, and D. L. Goeckel, "Identification of wireless users via power amplifier imperfections," in *2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers*, 2010, pp. 1553-1557.
- [30] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 18, pp. 94-104, 2015.
- [31] P. Scanlon, I. O. Kennedy, and Y. Liu, "Feature extraction approaches to RF fingerprinting for device identification in femtocells," *Bell Labs Technical Journal*, vol. 15, pp. 141-151, 2010.
- [32] J. Hall, M. Barbeau, and E. Kranakis, "Detection of transient in radio frequency fingerprinting using signal phase," *Wireless and Optical Communications*, pp. 13-18, 2003.
- [33] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE Journal on selected areas in communications*, vol. 29, pp. 1469-1479, 2011.
- [34] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 116-127.
- [35] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," in *2011 Proceedings IEEE INFOCOM*, 2011, pp. 1404-1412.
- [36] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE Journal of Radio Frequency Identification*, vol. 4, pp. 222-233, 2020.
- [37] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, 2007, pp. 111-122.
- [38] R. Zekavat and R. M. Buehrer, *Handbook of position location: Theory, practice and advances* vol. 27: John Wiley & Sons, 2011.
- [39] Y. Ren, L. Peng, W. Bai, and J. Yu, "A practical study of channel influence on radio frequency fingerprint features," in *2018 IEEE International Conference on Electronics and Communication Engineering (ICECE)*, 2018, pp. 1-7.
- [40] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer Identification of RFID Devices," in *USENIX security symposium*, 2009, pp. 199-214.
- [41] Y. Huang, "Radio frequency fingerprint extraction of radio emitter based on I/Q imbalance," *Procedia computer science*, vol. 107, pp. 472-477, 2017.

- [42] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized radio classification through convolutional neural networks," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, 2019, pp. 370-378.
- [43] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, *et al.*, "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, 2020, pp. 646-655.
- [44] S. U. Rehman, K. Sowerby, and C. Coghill, "RF fingerprint extraction from the energy envelope of an instantaneous transient signal," in *2012 Australian Communications Theory Workshop (AusCTW)*, 2012, pp. 90-95.
- [45] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *2009 International Conference on Information Processing in Sensor Networks*, 2009, pp. 25-36.
- [46] Y. Yuan, Z. Huang, H. Wu, and X. Wang, "Specific emitter identification based on Hilbert-Huang transform-based time-frequency-energy distribution features," *IET communications*, vol. 8, pp. 2404-2412, 2014.
- [47] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security," *Journal of Communications and Networks*, vol. 11, pp. 544-555, 2009.
- [48] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Micro-UAV detection and classification from RF fingerprints using machine learning techniques," in *2019 IEEE Aerospace Conference*, 2019, pp. 1-13.
- [49] C. Bertocini, K. Rudd, B. Noursain, and M. Hinders, "Wavelet fingerprinting of radio-frequency identification (RFID) tags," *IEEE Transactions on Industrial Electronics*, vol. 59, pp. 4843-4850, 2011.
- [50] G. Reus-Muns, D. Jaisinghani, K. Sankhe, and K. R. Chowdhury, "Trust in 5G open RANs through machine learning: RF fingerprinting on the POWDER PAWR platform," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, 2020, pp. 1-6.
- [51] L. Zong, C. Xu, and H. Yuan, "A rf fingerprint recognition method based on deeply convolutional neural network," in *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, 2020, pp. 1778-1781.
- [52] L. Ding, S. Wang, F. Wang, and W. Zhang, "Specific emitter identification via convolutional neural networks," *IEEE Communications Letters*, vol. 22, pp. 2591-2594, 2018.
- [53] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep learning based RF fingerprint identification using differential constellation trace figure," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 1091-1095, 2019.
- [54] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, *et al.*, "Deep learning for RF fingerprinting: A massive experimental study," *IEEE Internet of Things Magazine*, vol. 3, pp. 50-57, 2020.
- [55] N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis, and K. Chowdhury, "RF fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 15518-15531, 2020.
- [56] J.-H. Liang, Z.-T. Huang, and Z.-W. Li, "Method of empirical mode decomposition in specific emitter identification," *Wireless Personal Communications*, vol. 96, pp. 2447-2461, 2017.
- [57] P. H. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Transactions on communications*, vol. 42, pp. 2908-2914, 1994.
- [58] S. Kaur, C. Singh, and A. S. Sappal, "Effects and estimation techniques of symbol time offset and carrier frequency offset in OFDM system: Simulation and analysis," *International Journal of Electronics and Computer Science Engineering*, pp. 1188-1196, 2012.
- [59] S. Ellingson, "Correcting IQ imbalance in direct conversion receivers," *Argus Technical and Scientific Documents*, 2003.
- [60] L. Huang, M. Gao, C. Zhao, and X. Wu, "Detection of Wi-Fi transmitter transients using statistical method," in *2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013)*, 2013, pp. 1-5.
- [61] O. Ureten and N. Serinken, "Bayesian detection of Wi-Fi transmitter RF fingerprints," *Electronics Letters*, vol. 41, pp. 373-374, 2005.

- [62] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, pp. 27-33, 2007.
- [63] Y. Cao, W.-w. Tung, J. Gao, V. A. Protopopescu, and L. M. Hively, "Detecting dynamical changes in time series using the permutation entropy," *Physical review E*, vol. 70, p. 046217, 2004.
- [64] Y.-J. Yuan, X. Wang, Z.-T. Huang, and Z.-C. Sha, "Detection of radio transient signal based on permutation entropy and GLRT," *Wireless Personal Communications*, vol. 82, pp. 1047-1057, 2015.
- [65] C. Bandt and B. Pompe, "Permutation entropy: a natural complexity measure for time series," *Physical review letters*, vol. 88, p. 174102, 2002.
- [66] S. Kay, "Volume II: Detection Theory," *Fundamentals of Statistical Signal Processing; PTR Prentice Hall: Upper Saddle River, NJ, USA*, pp. 465-466, 1993.
- [67] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*: Prentice-Hall, Inc., 1993.
- [68] A. Candore, O. Kocabas, and F. Koushanfar, "Robust stable radiometric fingerprinting for wireless devices," in *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*, 2009, pp. 43-49.
- [69] S. M. Markalous, S. Tenbohlen, and K. Feser, "Detection and location of partial discharges in power transformers using acoustic and electromagnetic signals," *IEEE Transactions on Dielectrics and Electrical Insulation*, vol. 15, pp. 1576-1583, 2008.
- [70] C. Herold, T. Leibfried, S. Markalous, and I. Quint, "Algorithms for automated arrival time estimation of partial discharge signals in power cables," in *Proc. Int. Symp. High Volt. Eng.(ISH)*, 2007.
- [71] I. S. Mohamed, Y. Dalveren, and A. Kara, "Performance assessment of transient signal detection methods and superiority of energy criterion (EC) method," *IEEE Access*, vol. 8, pp. 115613-115620, 2020.
- [72] M. Barbeau, J. Hall, and E. Kranakis, "Detection of rogue devices in bluetooth networks using radio frequency fingerprinting," in *proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, CCN*, 2006, pp. 4-6.
- [73] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, 2007, pp. 331-340.
- [74] C. Zhao, T. Y. Chi, L. Huang, Y. Yao, and S.-Y. Kuo, "Wireless local area network cards identification based on transient fingerprinting," *Wireless Communications and Mobile Computing*, vol. 13, pp. 711-718, 2013.
- [75] T. Higuchi, "Approach to an irregular time series on the basis of the fractal theory," *Physica D: Nonlinear Phenomena*, vol. 31, pp. 277-283, 1988.
- [76] I. Mohamed, Y. Dalveren, F. O. Catak, and A. Kara, "On the Performance of Energy Criterion Method in Wi-Fi Transient Signal Detection," *Electronics*, vol. 11, p. 269, 2022.
- [77] R. M. Gerdes, T. E. Daniels, M. Mina, and S. Russell, "Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach," in *NDSS*, 2006.
- [78] Y. Shi and M. A. Jensen, "Improved radiometric identification of wireless devices using MIMO transmission," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 1346-1354, 2011.
- [79] 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.
- [80] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Radio frequency fingerprinting commercial communication devices to enhance electronic security," *International Journal of Electronic Security and Digital Forensics*, vol. 1, pp. 301-322, 2008.
- [81] E. J. Oughton, W. Lehr, K. Katsaros, I. Selinis, D. Bublely, and J. Kusuma, "Revisiting wireless internet connectivity: 5G vs Wi-Fi 6," *Telecommunications Policy*, vol. 45, p. 102127, 2021.



- [82] R. B. M. Abdelrahman, A. B. A. Mustafa, and A. A. Osman, "A Comparison between IEEE 802.11 a, b, g, n and ac Standards," *IOSR Journal of Computer Engineering (IOSR-JEC)*, vol. 17, pp. 26-29, 2015.
- [83] B. Mitchell, "Wireless Standards 802.11 a, 802.11 b/g/n, and 802.11 ac," *Verkköjulkaisu. Saatavissa: <http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm> [viitattu 8.4. 2015]*, 2015.
- [84] R. Khanduri and S. Rattan, "Performance Comparison Analysis between IEEE 802.11 a/b/g/n Standards," *International Journal of Computer Applications*, vol. 78, pp. 13-20, 2013.
- [85] B. Bellalta, "IEEE 802.11 ax: High-efficiency WLANs," *IEEE Wireless Communications*, vol. 23, pp. 38-46, 2016.
- [86] D.-J. Deng, K.-C. Chen, and R.-S. Cheng, "IEEE 802.11 ax: Next generation wireless local area networks," in *10Th international conference on heterogeneous networking for quality, reliability, security and robustness*, 2014, pp. 77-82.
- [87] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, "A tutorial on IEEE 802.11 ax high efficiency WLANs," *IEEE Communications Surveys & Tutorials*, vol. 21, pp. 197-216, 2018.
- [88] D. López-Pérez, A. Garcia-Rodriguez, L. Galati-Giordano, M. Kasslin, and K. Doppler, "IEEE 802.11 be extremely high throughput: The next generation of Wi-Fi technology beyond 802.11 ax," *IEEE Communications Magazine*, vol. 57, pp. 113-119, 2019.
- [89] E. Khorov, I. Levitsky, and I. F. Akyildiz, "Current status and directions of IEEE 802.11 be, the future Wi-Fi 7," *IEEE access*, vol. 8, pp. 88664-88688, 2020.
- [90] Y. Li, Y. Lin, Z. Dou, and Y. Chen, "Research on RF Fingerprint Feature Selection Method," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1-5.
- [91] J. Yu, A. Hu, F. Zhou, Y. Xing, Y. Yu, G. Li, et al., "Radio frequency fingerprint identification based on denoising autoencoders," in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2019, pp. 1-6.
- [92] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE transactions on Mobile Computing*, vol. 9, pp. 449-462, 2009.
- [93] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, pp. 93-108, 2005.
- [94] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet denoising to improve OFDM-based signal detection and classification," *Security and Communication Networks*, vol. 3, pp. 71-82, 2010.
- [95] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, 2008, pp. 1-5.
- [96] D. Zanetti, B. Danev, and S. Capkun, "Physical-layer identification of UHF RFID tags," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, 2010, pp. 353-364.
- [97] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID tags," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, pp. 938-943, 2010.
- [98] S. Chinnappa Gounder Periaswamy, D. R. Thompson, H. P. Romero, and J. Di, "Fingerprinting radio frequency identification tags using timing characteristics," in *Radio Frequency Identification System Security*, ed: IOS Press, 2010, pp. 73-81.
- [99] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improved wireless security for GMSK-based devices using RF fingerprinting," *International Journal of Electronic Security and Digital Forensics*, vol. 3, pp. 41-59, 2010.
- [100] J. Padilla, P. Padilla, J. Valenzuela-Valdés, J. Ramírez, and J. Górriz, "RF fingerprint measurements for the identification of devices in wireless communication networks based on feature reduction and subspace transformation," *Measurement*, vol. 58, pp. 468-475, 2014.
- [101] S. KARASU and Z. SARAÇ, "Güç kalitesi bozulmalarının hilbert-huang dönüşümü, genetik algoritma ve yapay zeka/makine öğrenmesi yöntemleri ile sınıflandırılması," *Politeknik Dergisi*, vol. 23, pp. 1219-1229, 2020.

- [102] M. Tosun and O. Çetin, "Ampirik Mod Ayırıştırması ve Welch Yöntemini Kullanarak Dört Sınıflı Motor Hayali EEG Sinyallerinin Derin Öğrenme ile Sınıflandırılması," *Avrupa Bilim ve Teknoloji Dergisi*, pp. 284-288, 2021.
- [103] F. Chen, Q. Yan, C. Shahriar, C. Lu, W. Lou, and T. C. Clancy, "On passive wireless device fingerprinting using infinite hidden markov random field," *submitted for publication*, 2017.
- [104] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Communications Magazine*, vol. 56, pp. 146-152, 2018.
- [105] J. A. Van Randwyk, J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, and D. Sicker, "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting," Sandia National Lab.(SNL-CA), Livermore, CA (United States)2006.
- [106] K. Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, 2010, pp. 383-392.
- [107] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, "GTID: A technique for physical device and device type fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, pp. 519-532, 2014.
- [108] T. J. O'Shea, J. Corgan, and T. C. Clancy, "Convolutional radio modulation recognition networks," in *International conference on engineering applications of neural networks*, 2016, pp. 213-226.
- [109] T. J. O'Shea and J. Hoydis, "An introduction to machine learning communications systems," *arXiv preprint arXiv:1702.00832*, 2017.
- [110] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio Frequency Fingerprint Identification for LoRa Using Deep Learning," *IEEE Journal on Selected Areas in Communications*, 2021.
- [111] G. A. Kale and C. Karakuzu, "Multilayer extreme learning machines and their modeling performance on dynamical systems," *Applied Soft Computing*, vol. 122, p. 108861, 2022.
- [112] Z. Katılmış and C. Karakuzu, "ELM based two-handed dynamic turkish sign language (TSL) word recognition," *Expert Systems with Applications*, vol. 182, p. 115213, 2021.
- [113] S. Ding, N. Zhang, X. Xu, L. Guo, and J. Zhang, "Deep extreme learning machine and its application in EEG classification," *Mathematical Problems in Engineering*, vol. 2015, 2015.