A Review of Radio Frequency Fingerprinting Techniques

Naeimeh Soltanieh, Yaser Norouzi, *Member, IEEE*, Yang Yang, *Senior Member, IEEE*, and Nemai Chandra Karmakar, *Senior Member, IEEE*

***Abstract*—Radio frequency (RF) fingerprinting techniques have been used as an extra security layer for wireless devices. Unique fingerprints are used to identify wireless devices in order to avoid spoofing or impersonating attacks. These unique features can be extracted from imperfections of analog components during the manufacturing. This paper presents a general review of recent progress on RF fingerprinting techniques. Several studies are investigated for RF fingerprinting using different parts of a signal. The majority of these studies have been focused on the transient part of the signal. For this purpose, the transient signal must be extracted precisely. A number of common techniques of transient extraction are theoretically analyzed in this review. Then, some other approaches using the modulated part of the signal are also discussed. For all these approaches, the applied methodologies, the classification algorithms and a taxonomy of features are described. A comprehensive overview of the methods in RF fingerprinting is presented to demonstrate the state-of-the-art works.**

***Index Terms*—Radio frequency, PHY layer security, transient-based fingerprinting, steady-state based, transient detection.**

I. Introduction

WIRELESS devices are traditionally identified by some unique RF fingerprints caused by radio circuitry. There are several forms of attacks for the wireless network; an impersonation attack is one of the most important and threatening [1]. In this kind of attack, an attacker can copy most of the identification information like the password and Media Access Control (MAC) address to spoof devices [2]. The radio frequency fingerprinting (RFF) from the unique features of electromagnetic waves emitted by the transmitter is unique [3]–[5].

In this review, we focus on methods that identify wireless devices by unique fingerprints that are called physical layer device identification. Physical layer identification is the process of fingerprinting the wireless device by extracting features due to hardware imperfections in the analog circuitry [6]. These hardware imperfections appear during the manufacturing process. Physical layer device identification has been used for different purposes like intrusion detection [7]–[9], access control [3], [10], cloning detection [11], [12] and secure localization [13]. The most important merit of using physical imperfection as a signature for identification is that it is hard to spoof the signature by using other wireless devices [14]–[16]. Wireless platforms for device identification using physical layer include HF RFID transponders, UHF RFID transponders [17], VHF transmitters and IEEE 802.11 transceivers [18], [19].

The main stages of wireless device identification system based on RF fingerprinting are capturing signals, feature extraction, and classification. After capturing signals, it is necessary to extract unique features from different parts of the signal. RF feature extraction is a serious concern in related works. RF fingerprinting based on the steady-state part of signal extracts features from the modulated part of the signal and can exploit prior information about the known signals [20]. On the other hand, transient based RF fingerprinting extracts fingerprints from the transient part of signals. The essential part of transient based approaches is to detect the transient signal correctly.

The transient signal is generated from the change of the transmitter's status [21]. The challenge of transient detection is to find the exact position of the start point of the signal from channel noise. This survey investigates common techniques for transient extraction and their advantages and disadvantages in detail.

The most challenging work in practical deployment of RF fingerprinting is to use low-end devices instead of high-end devices. Researchers consider different aspects of this research such as: 1) analysis and discussion of the practical limits that low-end devices have for RFF, 2) understanding the effects of channel impairments on the classification efficiency [22].

The main goal of this paper is to provide a comprehensive review of radio frequency fingerprinting systems and methods. In this paper we discuss in depth classifications of radio frequency fingerprinting especially transient based algorithms. We also discuss important methods of transient extraction.

The rest of the paper is organized as follows: Section II provides a background of physical layer security and how physical layer identification systems work. In Section III, we classify

Manuscript received August 16, 2019; revised December 28, 2019; accepted January 2, 2020. Date of publication January 27, 2020; date of current version August 26, 2020. *(Corresponding author: Yaser Norouzi.)*

Naeimeh Soltanieh is with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran 1591634311, Iran, and also with the School of Electrical and Data Engineering, University of Technology Sydney, Ultimo, NSW 2007, Australia (e-mail: n_soltanieh@aut.ac.ir).

Yaser Norouzi is with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran 1591634311, Iran (e-mail: y.norouzi@aut.ac.ir).

Yang Yang is with the School of Electrical and Data Engineering, University of Technology Sydney, Ultimo, NSW 2007, Australia (e-mail: yang.yang-1@uts.edu.au).

Nemai Chandra Karmakar is with the Department of Electrical and Computer Systems Engineering, Monash University, Melbourne, VIC 3800, Australia (e-mail: nemai.karmakar@eng.monash.edu.au).

Digital Object Identifier 10.1109/JRFID.2020.2968369

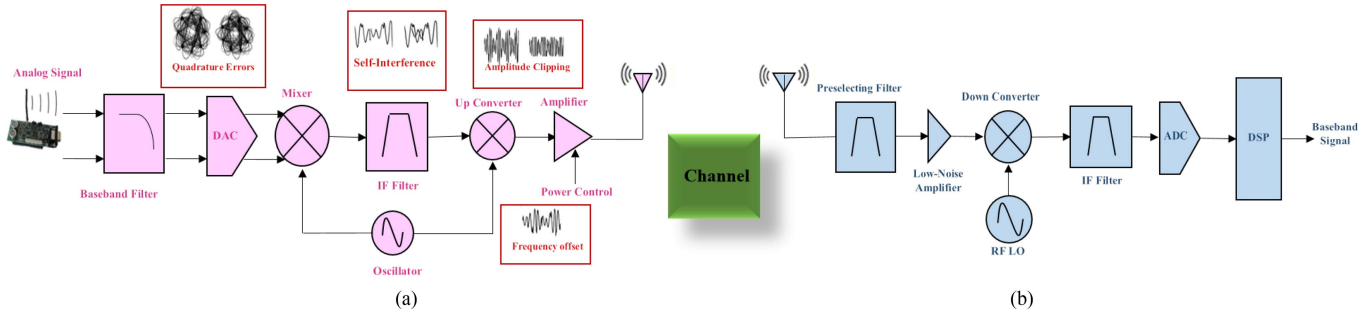


Fig. 1. Radiometric block diagram showing different sources of impairments in overall digital communication system. (a) Block diagram of transmitter and its impairments, (b) Block diagram of receiver.

RF fingerprinting methods and analyse both transient-based and steady state-based RFF algorithms. We also present other approaches that do not fit into those categories. In Section IV, we discuss features that are useful for both categories of RFF techniques. Finally, we present a classification methodology for transmitter identification in Section V and conclude the article in Section VI.

II. Physical Layer Security

Physical layer security is a new paradigm for securing the identity of wireless devices based on the unique features extracted from signals emitted by wireless devices [23], [24]. The uniqueness of features arises from analog element imperfections created in the manufacturing process [25]. Physical layer security that uses these unique features is known as Radio Frequency (RF) fingerprinting [26]. Transmitter imperfections that produce RF fingerprints are originated from its analog elements (phase noise, digital-to-analog converters, band-pass filters, frequency mixers, and power amplifiers) [12]. Fig. 1 shows physical imperfections of transceivers elements.

A physical layer identification system has three main tasks: 1) capture the identification signal, 2) extract proper features and 3) create fingerprints from captured signals and classify and identify fingerprints. A physical layer device identification system has two main modules: one for creating a library of enrolled devices and another for identification. Initially, signals are captured from a device or set of devices with different or same models and manufacturers [27]. Then the extracted features of RF fingerprints are, stored in a library as a database. In the second module, fingerprints extracted from a device are compared with the library of fingerprints in order to identify or verify the device.

As mentioned, fingerprints are sets of features that are extracted from the captured signal to identify and verify devices [28]. To achieve a high accuracy identification, the fingerprints need to have properties such as:

1) Universality, which means that every wireless device should have the features that are used for its identification;
2) Uniqueness, which indicates that no two devices should have the same fingerprints.
3) Permanence, which means that the fingerprints should be time-invariant and environment invariant.
4) Collectability, which indicates that it should be possible to measure the fingerprints quantitively and with existing equipment.
5) Robustness, which means that the fingerprints should be evaluated with respect to external environmental aspects like signal reflection, absorption, etc. and device-related aspects like temperature, power, and voltage level.

III. Classification of RF Fingerprinting

RF fingerprinting is a well-known technique used to identify wireless devices by extracting unique structures in the electromagnetic waves emitted from the transmitters. In the past few years, many RF fingerprinting methods have been explored in commercial areas [24], [29]–[32]. For example, in the ADS-B system used in Air Traffic Control, RF fingerprinting techniques used to identify/classify aircraft [33]. Also, other wireless devices signal such as Bluetooth [34], [35], push-to-talk transmitters [29], RFID [5], [36], [37] are used to evaluate RF fingerprinting methods. According to [10], every transmitter has a unique RF fingerprint that this uniqueness arises from imperfections in analog components during the manufacturing process. The main step in RF fingerprinting is to extract useful features of a transmitted signal to identify the signal's transmitter [38]. Here we review important techniques for RF fingerprinting. Transmitter identification techniques are classified based on essential differences. These methods are divided into three categories, namely transient-based, steady state-based and other approaches based on different signal parts used for feature extraction. Fig. 2 shows the different parts of an actual signal that are used in the special category. A structure of wireless transmitter identification categories is shown in Fig. 3.

A. Transient-Based RF Fingerprinting

Transient-based RF fingerprinting techniques use the transition from the turn-off to the turn-on of a transmitter that is occurs before the transmission of the actual data of a signal. These approaches need accurate transient extraction (start point and duration) before feature extraction and identification [39]. Channel noise and hardware have an important effect on transient extraction methods. Fig. 3 shows different types of transient signals in the captured signal [40].

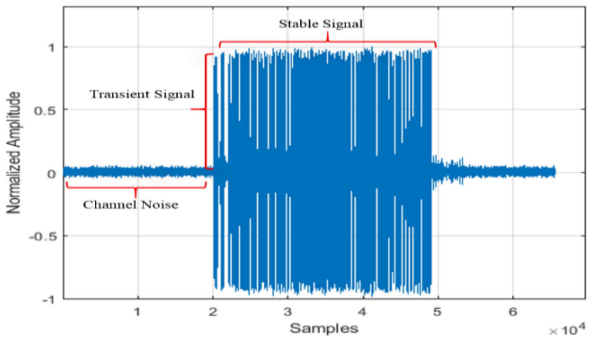


Fig. 2. Different parts of the mode S signal.

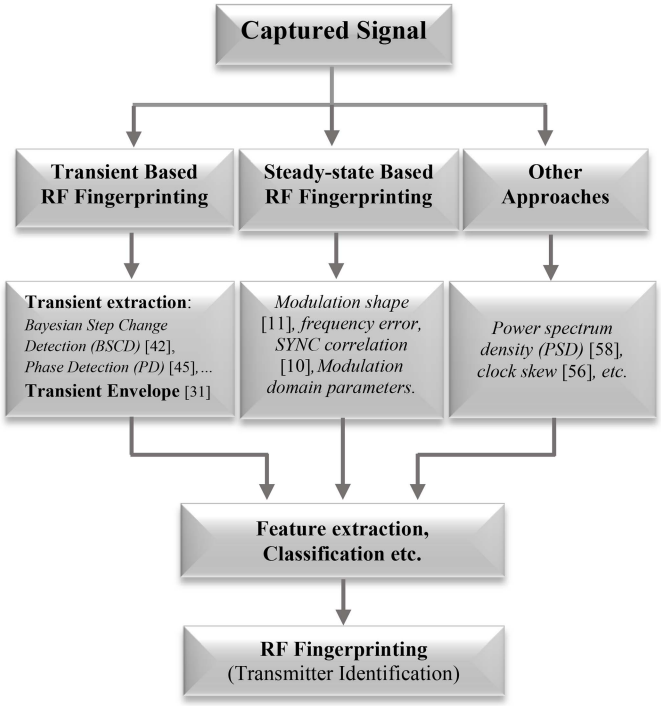


Fig. 3. A structure of wireless transmitter identification and classification of radio frequency fingerprinting techniques.

Equation (1) shows the modeled signal as follows:

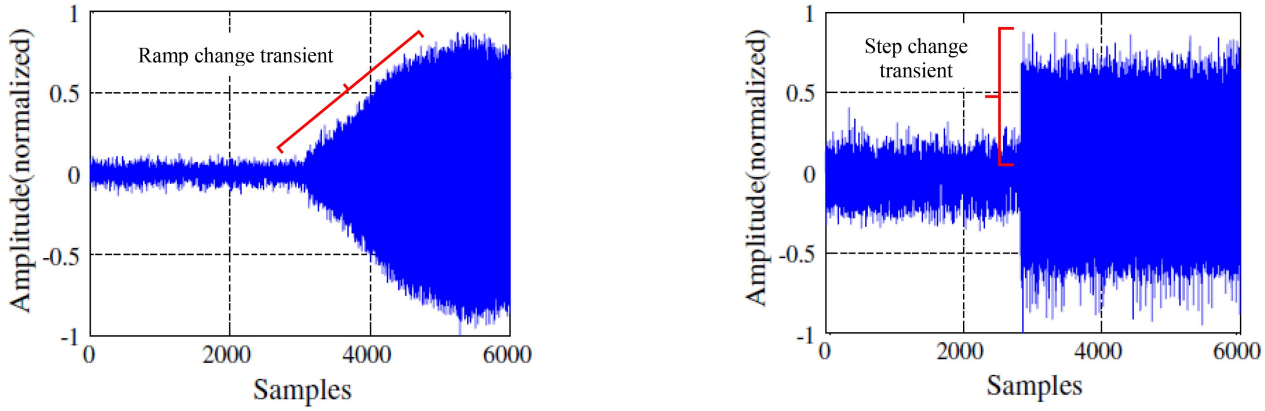
$$S_i = \begin{cases} n(i) & 1 \le i < m \\ X(i) + n(i) & n_0 \le n \le N_0 \end{cases} \quad (1)$$

where, S_i is the i-th sample; $X(i)$ is the discrete signal, when $i < m$; $n(i)$ is channel noise; N is the number of samples and m is the starting point of the transient signal.

The approaches to transient-based wireless device identification can be traced back to the early 90s. In [9], [29], seven VHF FM transmitters from different manufacturers but in the same model were identified using multi-resolution wavelet analysis to characterize the features in the transient signal. All the extracted features were classified using a genetic algorithm. To measure the noise sensitivity of the algorithm, Gaussian noise was added to the original transient signals. Choe *et al.* [7] proposed a robust and adaptive device identification system using a Daubechies-4 wavelet transform combined with ANN. Also, an example of identifier and classifier provided using transient signals of three different transmitters. Hippenstiel and Payal [30] also used Daubechies filter to obtain DWT coefficients of transients of 4 different transmitters. Ellis and Serinken [41] analyzed the amplitude and phase information of the transients of VHF FM transmitters. The authors used 28 transmitters from different manufacturers and the same models and showed that fingerprint profiles for devices from the same manufacturer and model is indistinguishable, making the identification process complex. Tekbas *et al.* [42], [43] tested transmission from 10 commercial VHF FM transmitters under ambient temperature, power supply, and additive channel noise. Amplitude and phase-based techniques were used to extract transient features. A probabilistic neural network (PNN) was used as a classifier and the results showed that classification accuracy of low SNR transients could be improved by estimating SNR and modifying its level during the training. Hall *et al.* used 14 different (manufacturers and models) IEEE 802.11 devices and 10 different (manufacturers and models) Bluetooth [43], [44]. The capturing process was performed from close proximity with a spectrum analyzer. The authors used amplitude, phase, in-phase, quadrature, power and DWT coefficients information to create a profile for each transient signal. The average classification error rate was 8% and was strongly dependent on the model and manufacturer. Ureten and Serinken [3] used the amplitude envelope as a feature of IEEE 802.11 transient signals for device classification and identification. The authors also used RF fingerprinting for enhancing the security of wireless networks. Signals were captured from 8 different manufacturers and models and classified using PNN. The proposed classifier could classify the signals with an error rate of 2%. In the above works, captured signals were from different models and manufacturers and at close distance with the fingerprinting antenna. In [45], Rasmussen and Capkun used RF fingerprinting techniques to identify 10 UHF (Mica2/CC1000) sensor devices from same manufacturers and models. Each device has a profile of fingerprints including transient length, amplitude variance, number of peaks of the carrier signal, the difference between normalized mean and the normalized maximum value of the transient power, and the first DWT coefficient. The feasibility of fingerprinting the radio of Wireless Sensor Node (Chipcon 1000 radio, 433MHz) was demonstrated in [45]. The duration of the transient signal, the number of peaks and the difference between the normalized mean normalized maximum values of the peaks are used to create an RF fingerprint for each signal.

In summary, transient based analysis offers high performance only whenever the transient is exactly extracted (the exact beginning and end point). The lack of transient analysis is the difficulty in distinguishing devices of same manufacturer (same model). Finally, very high sampling rates are needed for a good transient extraction, necessitating expensive receiver architectures.

Separating the transient signal and detecting the start point in channel noise are very difficult because of non-stationary characteristics [46]. In the rest of this section, a number of critical methods are theoretically analyzed for detecting the start point of transient signals.



(a) (b)

Fig. 4. Typical captured signal. (a) Ramp change signal from a Nokia 5230 mobile phone. (b) Step change signal from a VHF radio [35].

1) Method 1 (Bayesian Step Change Detection (BSCD)): This approach was proposed by Fourteen which transforms a change in variance into a change in the mean value based on the fractality of the sampled data to detect the start point of the transient. In this approach, Higuchi's method [47] was used to calculate the fractal dimension for successive segments of the signal. There is a close relation between the variance of fractal dimension and the probability density function of start point of transient, for example, the variance of fractal dimension between two sequences are related to the probability density function, so the maximum of the probability density function is the start point of the transient signal. A non-stationary signal like a transient is not a pure fractal because its fractality is time variant. Multi-fractality handles signals with local fractal dimensions. For calculating the local fractal dimensions of successive portions of the signal, a sliding window is used. The principle of this approach is provided as follows:

First, the fractal dimension of the transient is calculated by Higuchi's method. Higuchi defines the length of the curves for each subsets as follows:

$$L_m(k) = \left\{ \left(\sum_{i=1}^{\frac{N-m}{k}} |X(m+ik) - X(m-(i-1)k| \right) \times \frac{N-1}{\left[\frac{N-m}{k}\right]k} \right\} \Big/ k \tag{2}$$

where, m is the initial time and the starting point of each subset and k is the interval time and determines the number of subset and $X\ (m,k) : X(m), X(m+k), \ldots, X(m+[(N-m)/k] \times k)$ and $(N-1)/[(N-m)/k]k$ is assumed to be the normalization factor of curve length.

Second, $L_m(k)$ is plotted against k on a log-log scale, so the data should fall on an axis as k varies from N to zero.

Third, a curve is fitted to the points $(L_m(k))$ that calculated in the last step according to the least-square procedure, and then the slope of the curve is an estimation of the fractal dimension.

Fourth, the following *a posteriori* probability density function is used to detect transient. The maximum point of the function is the start point of the transient signal [47].

$$p(\{m\}|d) \propto \frac{1}{\sqrt{m(N-m)}} \times \left[\sum_{i=1}^{N} d_i^2 - \frac{1}{m}\left(\sum_{i=1}^{m} d_i \right)^2 - \left(\frac{1}{N-m} \right) \times \left(\sum_{i=m+1}^{N} d_i \right)^2 \right]^{\frac{N-2}{2}} \tag{3}$$

where, d is the fractal dimension, m is assumed to be the start point of transient and N is the number of samples in the sliding window. Although there is no need to define a threshold in the BSCD method, this approach has a complex computation and a poor detection for transient signals with small amplitude. Fig. 5 shows the detection result of BSCD algorithm on net-core transient.

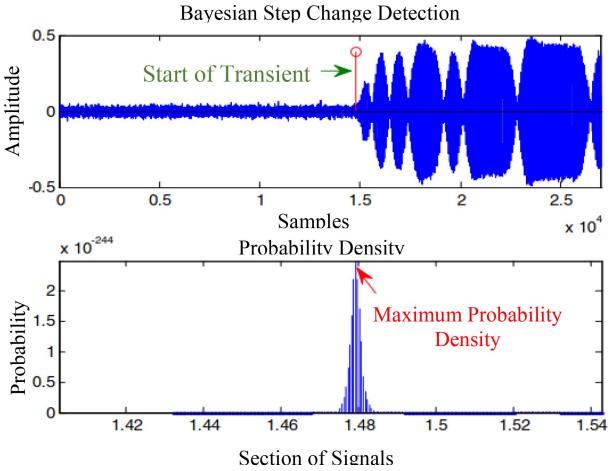


Fig. 5. Bayesian step change detection (signal of net-core). © [2013] IEEE. Reprinted, with permission, from [51].

2) Method 2 (Bayesian Ramp Change Detection (BRCD)): This method was proposed by Ureten and Serinken [48] and it is a modification to the BSCD scheme. In this approach, transient detection is achieved by estimating the time instant

when the power of signal gently increased. Its principals are provided as follows:

As mentioned before, typical transmission data contain channel noise before transmission of real data. The model of this signal can be written in the form of a matrix equation:

$$d = Gb + e \tag{4}$$

where d is an $N \times 1$ matrix of data samples, e is a matrix of Gaussian noise samples with dimensions of $N \times 1$, the matrix G is of size $N \times M$ that each column of G is a basis function estimated at each sample in the time series and b is an $M \times 1$ matrix of linear coefficients. The next step is to detect the change point with a posteriori probability density which is calculated as in the following equation [48]:

$$p(\{m\}|d, I) \propto \frac{\left[d^T d - d^T G\left(G^T G\right)^{-1} G^T d\right]^{-(N-m)/2}}{\sqrt{\det\left(G^T G\right)}} \tag{5}$$

where I defines the signal model. The start point position can be found in the structure of the matrix G that is given in equation (6).

$$G^T = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 2 & 3 & \cdots & N-m \end{bmatrix} \tag{6}$$

A Bayesian ramp change detector is a better candidate for transient extraction for Wi-Fi radios in comparison with Bayesian step change detector because of the lags behind the start point of the transient signal and because the standard deviation of the detection error for BSCD is three times higher than BRCD [48].

3) Method 3 (Variance Fractal Dimension Threshold Detection): This approach was proposed by Shaw and Kinser [49]. The main idea is to calculate the fractal dimension from the variance of signal amplitude to detect the transient part of a signal.

The first step is to calculate the fractal dimension for each portion of the signal in the sliding window by equation (7).

$$D(t) = 2 - H \tag{7}$$

where H is a value called the Hurst index that is the correlation between $\Delta X(t_i, \Delta t)$ and Δt that is the amplitude difference between data samples and Δt. By setting $\Delta X(t_i, \Delta t) = X(t_i, \Delta t) - X(t_i)$ and $\Delta t = |t_{i+1} - t_i|$, the Hurst index can be calculated by equation (8) based on the least squares regression (LSR) scheme [49].

$$2H = \frac{N\sum_{i=1}^{N} x_i y_i - \left(\sum_{i=1}^{N} x_i\right)\left(\sum_{i=1}^{N} y_i\right)}{N\left(\sum_{i=1}^{N} x_i^2\right)\left(\sum_{i=1}^{N} x_i\right)^2} \tag{8}$$

where $(x_i, y_i) = (\log(\Delta t_i), \log(var(\Delta X(t_i, \Delta t_i))))$. It is necessary to ensure that there are a sufficient number of the pairs (x_i, y_i) and selecting a suitable sequence of time is very important.

The next step is to detect the start point of the transient signal from the fractal dimension obtained from the first step. The mean of the fractal dimension of channel noise is considered as a threshold. The threshold needs to be determined based on experiments. The variance fractal dimension of wireless network card net-core is shown in Fig. 6. For example, if the value of n-th point and its m successive points are less than the threshold, then n is considered to be the start point of the transient. It must contain at least $T/4$ samples of channel noise before the start of the transmission. It is proved that there is a remarkable difference between the fractal dimension of ambient channel noise and the actual data. This method is simple and fast, but the threshold needs to be determined by trial and error and it is very sensitive to noise.

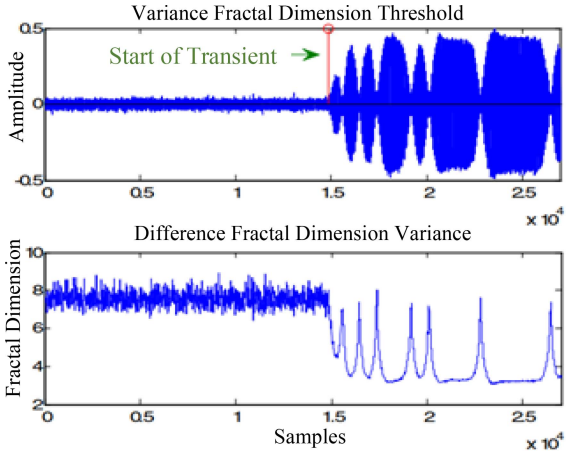


Fig. 6. Variance fractal dimension threshold detection (signal of net-core). © [2013] IEEE. Reprinted, with permission, from [51].

4) Method 4 (Phase Detection (PD)): Phase Detection method was proposed by Hall *et al.* [50] and unlike the previous approaches which used the amplitude characteristics of the signal for transient extraction, this approach used phase characteristics to extract transient signals. This approach has advantages against the methods using amplitude characteristics because the phase of the signal does not represent the same degree of variation because the phase is less sensitive to noise. Moreover, the implementation of PD is as follows:

The instantaneous phase of the signal $(X(t) = I(t) + jQ(t))$ can be calculated using equation (9) as follows:

$$\theta(t) = \tan^{-1}\left[\frac{Q(t)}{I(t)}\right] \tag{9}$$

where, $\theta(t)$ is unwrapped to remove the discontinuities that result at multiples of 2π radians. The absolute value of each element in the unwrapped vector AV which is shown in equation (10):

$$AV = \begin{cases} \theta(t) & |\theta(t) - \theta(t-1)| \le \pi \\ \theta(t) \pm 2\pi & others. \end{cases} \tag{10}$$

To detect the start point of the transient signal and magnify the variation between channel noise and turn-on transient signal, the variance of the phase characteristics is calculated for each consecutive portion of AV [50].

$$TV(i) = \text{var}\left(A\vec{V}(d+1),\ A\vec{V}(d+2), \ldots, A\vec{V}(d+g)\right) \tag{11}$$

where $i = 1, 2, \ldots, N/S$, $g = i \times S$, $d = g - S, S$ is non-overlapping window size and *var* represents the variance of the phase.

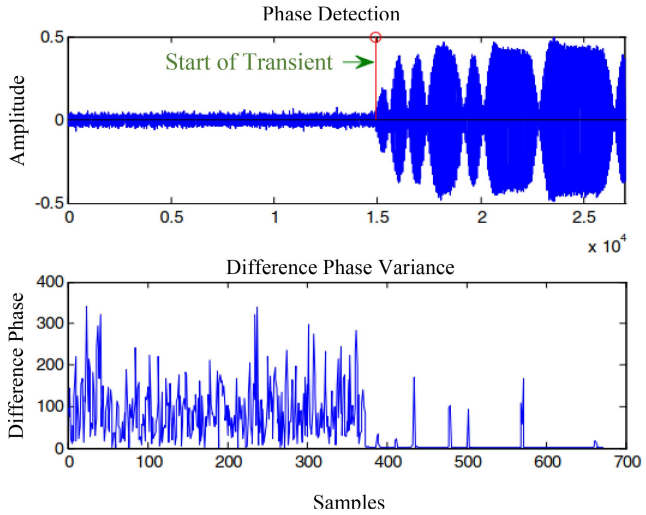


Fig. 7. Phase detection (signal of net-core). © [2013] IEEE. Reprinted, with permission, from [51].

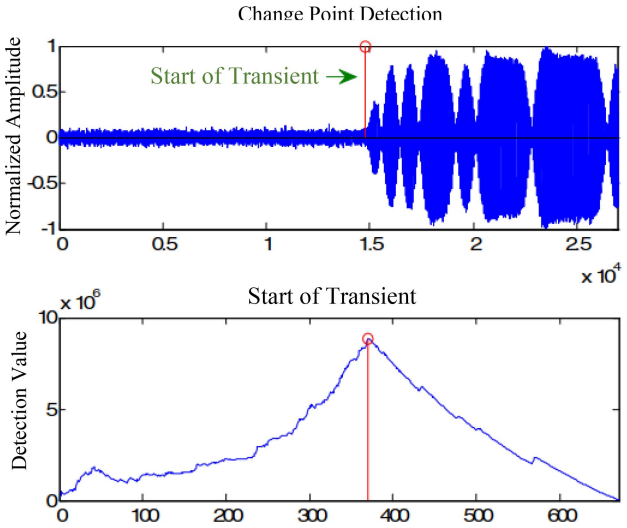


Fig. 8. Mean change point detection (signal of net-core). © [2013] IEEE. Reprinted, with permission, from [51].

The last step is to create the fractal trajectory (FT) from the difference of the phase variance. The start point of the turn-on transient is when the fractal trajectory becomes near to zero because the phase variance of the transient signal changes more slowly than channel noise. The start point detection of net-core signal using PD algorithm is shown in Fig. 7.

5) Method 5 (Mean Change Point Detection (MCPD)): The mean Change Point Detection approach detects the start point of the transient signal by statistical calculation [51]. There is no need to define a threshold and nonparametric estimation for the hypothesis test [52].

Assuming fractal trajectory as the sample sequence, e.g., $x_1, x_2, \ldots, x_N$, the process of the algorithm is provided as follows.

The first step is to divide the sample sequence into two sections $x_1, x_2, \ldots, x_{i-1}$ and $x_i, x_{i+1}, \ldots, x_N$, then calculate the mean and the following statistics of each section for $i = 2, 3, \ldots, N$.

$$S_i = \sum_{t=1}^{i-1} \left(x_t - \bar{X}_{t1}\right)^2 + \sum_{t=i}^{N} \left(x_t - \bar{X}_{t2}\right)^2 \tag{12}$$

where $\bar{X}$ is average of original samples. Statistics (S) of samples calculated according to equation (13).

$$S_i = \sum_{t=1}^{N} \left(x_t - \bar{X}\right)^2 \tag{13}$$

The last step is to define the position of the start point of the transient signal by calculating the maximum point of $S - S_i$. The main idea of this approach is to magnify the difference between static of samples before and after the section. As shown in Fig. 8, the start point of the transient part of net-core signal is accurately detected.

6) Method 6 (Permutation Entropy (PE) and Generalized Likelihood Ratio Test (GLRT) Detector): This method detects a transient signal based on permutation entropy (PE) and a generalized likelihood ratio test (GLRT) detector [40].

Permutation Entropy (PE) is introduced by Bandt-Pompe and can evaluate the irregularity and complexity of time series [53]. PE is simple, structurally robust and fast. Assume we have a given time series $X = \{x(i), i = 1, 2, \ldots, N\}$, to calculate PE of it, the time series are embedded into an m-dimensional space:

$$X_i = [x(i), x(i+1), \ldots, x(i+(m-1))], \tag{14}$$

where m is the embedding dimension and determines how much information is contained in each vector, l is time delay and X_i is the i-th point in m-dimensional space; $1 \le i \le N - (m-1)l$.

In the next step, the values of X_i are sorted in ascending order, so it can be written as follows:

$$X_i = \left[x(i+(j_1-1)l) \le x(i+(j_2-1)l) \le \cdots \le x(i+(j_m-1)l)\right], \tag{15}$$

The vector X_i can be mapped onto a permutation pattern π:

$$\pi_i = \left[j_1, j_2, \ldots, j_m\right], \tag{16}$$

where, π_i is one of $m!$ possible permutations of m different symbols and j is the time index of the element in the reconstruction vector. Let the occurrence number of π be $f(\pi_i)$, then the occurrence probability of π_i is $p(\pi_i) = f(\pi_i)/(N-(m-1)l)$. Finally, the PE is computed as Shannon Entropy [54]:

$$0 \le H_P = -\sum p_j \ln\left(p_j\right) / \ln(m!) \le 1 \tag{17}$$

where, K is the number of distinct symbols in $[\pi_1, \pi_2, \ldots, \pi_{N-(m-1)l}]$. Using above knowledge about PE, the start point of transient signal can be detected.

In the first step, the PE trajectory of transient is calculated using a rectangular window with the length of L_{wnd} that slides one sample each time. The PE of a noise series is bigger than the PE of a signal because there is no regularity in noise. PE

trajectory can be modeled by the following equation:

$$H_P(n) = \begin{cases} H_{pn}(n) & 1 \le n \le n_0 \\ H_{pt}(n) & n_0 \le n \le n_1 \\ H_{ps}(n) & n_1 + 1 \le n \le N \end{cases} \tag{18}$$

where n is the number of slides; $H_{pn}(n)$ is the PE of noise; $H_{ps}(n)$ is the PE of stable signal; $H_{pt}(n)$ is the PE of slides that contains transient signal. When the transient is in the sliding window, the PE starts to decrease and when the stable signal is in the sliding window, the PE changes a little. The PE for the slides that contains transient signal can be modelled as follows [40]:

$$H_P(n) = \begin{cases} A_0 + w(n) & 1 \le n \le n_0 \\ A_0 + k \times (n - n_0) + w(n) & n_0 \le n \le N_0 \end{cases} \tag{19}$$

where, $w(n)$ is a Gaussian noise with a standard deviation of $\sigma$and zero mean; A_0 is the average of $H_{pn}(n)$; k is the slope of decreasing after the n_0. n_0 is the first slide that contains the transient signal; N_0 is the changing point when $n \le N_0$, $H_{pn}(n) > T_0$ and $H_{pn}(N_0 + 1) \le T_0$ and T_0 is the average PE, calculated as follows:

$$T_0 = \frac{\max(H_P) + \min(H_P)}{2}. \tag{20}$$

The transient detection problem can be solved in terms of the binary hypotheses test:

$$\begin{aligned} H_0 &: A_0 + w(n) \\ H_1 &: \begin{cases} A_0 + w(n) & 1 \le n \le n_0 \\ A_0 + k \times (n - n_0) + w(n) & n_0 \le n \le N_0 \end{cases} \end{aligned} \tag{21}$$

In the second step, the GLRT detector of $H_p(n)$ can be represented as follows [55]:

$$\begin{aligned} L_G(x) &= \frac{p(x; n_0, H_1)}{p(x; H_0)} \\ &= \frac{p\left(x; A_1 = \hat{A}_0, A_2 = \hat{A}_0 + \hat{k} \times (n - n_0), H_1\right)}{p\left(x; A_1 = \hat{A}_0\right)}, \end{aligned} \tag{22}$$

where $p(x; n_0, H_1)$ and $p(x; A_1)$ are represented as in the following equations; A_0 and k are unknown can be estimated by maximum likelihood (MLE) [40].

$$p(x; A_1, A_2) = \frac{1}{\left(2\pi\sigma^2\right)^{N_0/2}} exp\left[-\frac{1}{2\sigma^2} \left(\sum_{n=1}^{n_0} (x(n) - A_1)^2 + \sum_{n=n_0+1}^{N_0} (x(n) - A_2)^2 \right) \right] \tag{23}$$

$$p(x; A_1) = \frac{1}{\left(2\pi\sigma^2\right)^{N_0/2}} exp\left[-\frac{1}{2\sigma^2} \left(\sum_{n=1}^{N_0} (x(n) - A_1)^2 \right) \right], \tag{24}$$

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.

$$\hat{A}_{00} = \hat{A}_0 = \frac{1}{N_0} \sum_{n=1}^{N_0} H_p(n) \tag{25}$$

$$\hat{A}_{01} = \hat{A}_0 = \frac{1}{n_0} \sum_{n=1}^{n_0} H_p(n) \tag{26}$$

The MLE of the slope k can be estimated by the least-squares fitting algorithm as in the following equation [54]:

$$\hat{k} = \frac{(N_0 - n_0) \sum_{n=1}^{N_0 - n_0} n H_p(n + n_0) - \sum_{n=1}^{N_0 - n_0} n \sum_{n=1}^{N_0 - n_0} H_p(n + n_0)}{(N_0 - n_0) \sum_{n=1}^{N_0 - n_0} n^2 - \left(\sum_{n=1}^{N_0 - n_0} n \right)^2} \tag{27}$$

According to the above equations, the GLRT detector defines as follows [40]:

$$\begin{aligned} &Ln\left(L_G\left(H_p(n)\right)\right) \\ &= \frac{1}{2\sigma^2} \left[\sum_{n=1}^{N_0} \left(H_p(n) - \hat{A}_{00} \right)^2 - \sum_{n=1}^{n_0} \left(H_p(n) - \hat{A}_{01} \right)^2 \right. \\ &\qquad \left. - \sum_{n=n_0+1}^{N_0} \left(H_p(n) - \hat{A}_{01} - \hat{k} \times (n - n_0) \right)^2 \right], \end{aligned} \tag{28}$$

The estimated start point of transient signal $\hat{n}_0$ is the maximum of the GLRT detector, defined in equation [40]:

$$\hat{n}_0 = \arg\max_n \left[Ln\left(L_G\left(H_p(n)\right)\right) \right], \tag{29}$$

According to the explanations about transient extraction methods, a table of performance comparison is provided. Table I shows the advantages and disadvantages of common algorithms in transient extraction.

B. Steady State-Based RF Fingerprinting

Steady-state based approaches focus on the unique features extracted from the modulated part of the signal. Brike *et al.* [10] proposed a Passive RAdiometric Device Identification System (PARADIS) using five specific features of the modulated signal such as: the frequency error, SYNC (synchronized) correlation, I/Q origin offset, and magnitude and phase errors for physical-layer identification. These features were used to make an RF fingerprint profile that is classified with an SVM and k-NN classifier. The system used 138 same model IEEE 802.11b signals, captured by a high-end vector signal analyzer and at distance from 3 to 15m from the antenna, to test the accuracy of the classifiers. Shi and Jensen [56] proposed a similar approach to PARADIS and use radiometric features in the modulation domain to identify Multiple Input Multiple Output devices. Modulation-based methods were also used to classify RFID devices. Danev *et al.* [11] also used the features extracted from modulation shape and spectral features from RFID transponders. The proposed method was tested on 4 different classes and different models of ISO 14443 RFID transponder. In number of researches like [57] frequency domain features were used to perform transmitter identification. Eight Universal Radio Peripherals (USRP) transmitters were used for laboratory experiments. This paper offers an excellent performance improvement by using flexible feature selection with a traditional discriminatory classifier (k-NN). The approach performs well with 97% accuracy rate at 30 dB SNR

TABLE I
PERFORMANCE COMPARISON OF TRANSIENT EXTRACTION ALGORITHMS

Algorithms	Advantages	Disadvantages	Success Rate
BSCD [44]	High detection rate for signals with suitable amplitude, no need to define a threshold	Complex computation, poor detection for transient signal with small amplitude	80-85% 802.11b transceiver
BRCD [45]	Perform better than BSCD specially for Wi-Fi radios , no need to define a threshold	Complex computation, effective on signal models with linear power increase	95% 802.11b transceiver
VFDTD [46]	High detection rate	Complex computation, need to define a threshold practically, very sensitive against noise	Not Available
PD [47]	Simple and fast	Less sensitive to noise, need to define a start point practically	85-90% 802.11b transceiver
MCPD [48]	Simple, high detection rate, no need to define a threshold	Need a long computation time	90-92.5% 8 different transmitters including 3 Kenwood, 3 Force and 2 Yaesu models
PE & GLRT [37]	High detection rate, extremely accurate detection of start point, no need to define a threshold	Complex computation	Not Available

and the performance is still good with accuracy of 66% at 0dB SNR. Suski *et al.* [58] used the Power Spectral Density (PSD) coefficients as unique features from the preamble part of IEEE 802.11a/g signal.

Initially, research was more about transient-based RF fingerprinting because the steady-state part of the signal is not common to all transmitters. The transient signal always occurs in a transmission, so the research focused on transient-based approaches. However, a higher sampling rate is required to extract the transient signal due to its short period and reliability of the phase and amplitude information is a serious challenge in this area [57]. Nowadays, there is no need to have a steady-state signal for these approaches because almost all wireless local area network (WLAN), RFID, etc. have a preamble at the start of data transmission to make the receiver design simple [59]. Gerdes *et al.* [60] proposed a steady state-based RFF technique which is able to identify cards with same model and same manufacturer. The preamble part of IEEE Ethernet 802.3 (16 devices with 3 different models) was used to provide a device fingerprint profile, which help to identify the device the signal emitted from. A matched filter implementation and a simple threshold were used to provide classification. They have shown that the characteristics of analog signals for these devices are track able and also it is appropriate for network access control schemes.

C. Other Approaches

Some of the proposed physical-layer identification techniques could not be related to the mentioned classification [61], [62]. These approaches usually use a special wireless technology and/or extract other attributes of the signal and logical layer. Suski *et al.* [63] create an RF fingerprint profile by measuring the power spectrum density (PSD) of the preamble of IEEE 802.11a to uniquely identify wireless devices. This approach was tested on 3 devices and achieved an average classification error rate of 20% for packet frames that were captured with SNR greater than 6 dB. In [62], [64], a complex wavelet transformation was applied to identify IEEE 802.11a (OFDM) devices. Multiple Discrimination Analysis (MDA) used to classify extracted features and the classification performance for this approach was tested on 4 same model Cisco wireless devices. The results showed a classification error rate of 20% for SNR improvement of 8 dB. Recent research targeted different class of RFID for physical-layer identification [36], [65]. Periaswamy *et al.* [65], [66] used UHF RFID tags for device identification. The authors showed that the minimum power response characteristic can be used to identify devices two independent sets of 50 tags from two different manufacturers with an accuracy of 94.4% (with False Acceptance Rate (FAR) of 0.1%) and 90.7% (with FAR of 0.2%).

Danev *et al.* [11], used timing, modulation shape and spectral features of device response signals for physical layer identification. The authors showed that of these features, timing and modulation-shape only distinguished devices from different manufacturers, but spectral features would be a preferred fingerprint to identify devices from the same manufacturer and same model. Jana and Kasera [61] used clock skews as a unique feature to identify access points (Aps) in a wireless local area network. The effectiveness of this technique has been shown in [67] for complex networks. The results showed that different Aps are distinguishable with high accuracy. Recently, researchers investigated variety of signal characteristics, signal parts on GSM devices [68]–[70]. They used midamble and the near-transient part of GSM-GMSK burst signals for the aim of identification and classification of devices from 4 different manufacturers. The results showed that the accuracy of classification sharply decreases when the midable part is used but the near-transient part is suitable for identifying GSM signals.

IV. TAXONOMY OF FEATURES FOR RF FINGERPRINTING

A large variety of features can be used for physical layer identification. In this section, we investigate useful features in the physical layer, whether they are active or passive. Physical layer features are extracted from the received RF waveform and generally divided into two categories: location dependent features and location independent features or radiometrics. In this paper, we focused on location independent features.

A. Location-Independent Features

Extracting radiometric features depend on the hardware implementation of wireless devices. It has been shown that even with significant advancement in circuit design and manufacturing, every transmitter has a unique RF fingerprint owing to imperfections in its analog components and manufacturing process [71]. Imperfections such as channel width, channel doping and oxide thickness, which are small enough to meet specifications of communication, can allow us to detect unique features from devices and provide device fingerprints [72].

The main purpose of feature extraction is to create a unique RF fingerprint profile to make a transmitter distinguishable from the rest of the transmitters. Previously, researchers [59] used the coefficients of Power Spectral Density (PSD) and normalized PSD to create an RF fingerprint.

Hall *et al.* [50] use unique features such as phase, amplitude, phase angle and frequency that are extracted using the Discrete Wavelet Transform (DWT), from the turn-on transient portion of signals.

Polak *et al.* [73] used the imperfection of the power amplifier for physical layer identification because power amplifiers are the last elements in the circuit of transmitters and it is hard for attackers to modify with software. Volterra series were used to model the nonlinear characteristics of power amplifiers.

As mentioned, Brik *et al.* [10] proposed a system called PARADIS that used features such as magnitude and phase errors, I/Q origin offset and SYNC correlation of the frame. Nguyen *et al.* [74] used carrier frequency differences (CFD) and phase shift differences (PSD) as fingerprints for transmitters. PSD is determined as the phase shift from one constellation to another in the neighborhood that may vary because of the different amplifier for I-phase and Q-phase in each transmitter. Nguyen *et al.* also proposed a second-order cyclostationary feature (SOCF) in addition to PSD and CFD to identify devices.

In radiometric techniques, feature extracting can be classified into transient-based and steady state-based features because of the way they treat signals [10]. Transient-based methods [75], [76] use time- and frequency-based features which are flexible but complex while steady state-based methods represent features in terms of I/Q samples. Modulation based methods have better structure but the important issue is the fact that we should know the respective modulation scheme.

B. Location-Dependent Features

RF fingerprinting techniques usually have two aims: 1) find the device which emitted the signal and 2) find the location of the device which the signal originated from [77]. The most common feature which is used in location based RFF techniques is radio signal strength (RSS) [78]. The value of RSS depends on the attenuation of the channel and the transmission power at the transmitter. For example, two distant locations have different values of average signal power (RSS) at the receiver with the same transmitter. However, if the two devices are close, their RSS will be similar. The other feature in this classification is Channel State Information at the Receiver (CSIR). This feature is very sensitive to moving. If we consider small-scale fading, CSIR can have very different values by only a little movement of a receiver. Location-dependent features cannot be used separately as a fingerprint because they are very sensitive to environmental changes [72].

V. Classification Of Extracted Features

Classification algorithms can be divided into two categories: supervised algorithms and unsupervised algorithms. Supervised algorithms represent the category that a set of observations is available, and classifiers are built based on a set of labeled data and the algorithms learn to be predicted [79]. In supervised algorithms, a set of labeled observations is available for training In supervised algorithms, a set of labeled observations is available for training.

The K Nearest Neighbors algorithm (KNN) is one of the supervised methods [53]. This algorithm classifies a data set based on the distance to the nearest samples in the training set. A variety of functions can be used to determine the distance between samples such as Euclidean distance, Mahalanobis and Minkowski; Euclidean distance is the most common [80]. The KNN algorithm is very simple and computationally efficient in the training phase but the classification phase could be computationally intensive in comparison with other algorithms. In addition, high dimension, KNN is less effective method for classification.

SVM is also a supervised algorithm that learns to classify observation samples from the reference samples. SVM uses a function from different types such as: linear, Radial Basis Function (RBF), polynomial, sigmoidal to divide the labeled set into several groups, depending on the problem, on a multi-dimensional surface [81]. This method provides a high level of accuracy and robustness and it is also efficient for binary classification.

A neural network is a supervised method that contains a set of connected input and output and each connection has a specific weight. The network predicts the class labels during the process of adjusting the weight to each connection [82]. The most important advantage of neural networks is the tolerance of noisy data in RF fingerprints. This algorithm could be able to classify patterns without a training phase that is a very useful point for identifying new devices.

Unsupervised learning algorithms do not have a training set and the algorithm must find the function from unlabeled data. For wireless device identification, unsupervised algorithms mean that we have similar fingerprints from different devices which are grouped together and belong to the same cluster. These methods are very useful for identifying devices from the same models and the same manufacturers. In these approaches, there is no need to create a reference library because the presence of valid phones is used for this purpose [83]. There are various unsupervised algorithms. Here we described only the methods applied to fingerprint identification.

K-Means clustering is an unsupervised algorithm in which the observations are divided into a number of clusters and each sample of observation is assigned to the cluster with the nearest mean.

PCA (Principal Component Analysis) is a multivariate method which is useful for data compression and dimensionality reduction. The main purpose in PCA is to extract important information from data and construct a set of orthogonal variables called principal components. This feature is very useful in phone identification to reduce a large set of features [84].

VI. Conclusion

This survey has reviewed RF fingerprinting methods for wireless devices. Physical-layer identification has been studied for a variety of wireless applications, but the primary usage of this technology is in wireless security enhancement. In this paper, we provide a comprehensive overview of physical-layer identification and state-of-the-art techniques in RFF. The detection of transients is considered one of the key steps in the fingerprint detection of wireless devices; its accuracy directly affects the success of identification. This review has investigated some of the common approaches in transient detection and their advantages and disadvantages. The most important problem in transient based algorithms is the dependency of the extraction method on the sampling rate of signals. Signal with high sampling rate could have a precise transient extraction which is needed to have a high-end devices for capturing the signal. The main gap in this area is the lack of a reliable approach to optimize the sampling rate which can reduce the costs.

The feature profiles used for different types of fingerprinting methods have been elaborated in this review. The main idea is to extract unique features from wireless devices to generate non-forgeable signatures. Finally, the paper has taken into consideration the classification process and methods.

Acknowledgment

The authors are particularly grateful for the assistance given by Dr. M. Pauly for English language editing.

References

[1] Q. Li and W. Trappe, "Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 793–808, Dec. 2007.

[2] J. Hall, M. Barbeau, and E. Kranakis, "Radio frequency fingerprinting for intrusion detection in wireless networks," *IEEE Trans. Depend. Secure Comput.*, vol. 12, pp. 1–35, Jul. 2005. [Online]. Available: https://www.researchgate.net/publication/221425652_Radio_frequency_fingerprinting_for_intrusion_detection_in_wireless_networks

[3] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Can. J. Elect. Comput. Eng.*, vol. 32, no. 1, pp. 27–33, 2007.

[4] K. D. Hawkes, "Transient analysis system for characterizing RF transmitters by analyzing transmitted RF signals," Google Patent WO1 998 012 895 A1, 1998.

[5] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet fingerprinting of radio-frequency identification (RFID) tags," *IEEE Trans. Ind. Electron.*, vol. 59, no. 12, pp. 4843–4850, Dec. 2012.

[6] H. L. Yuan and A. Q. Hu, "Preamble-based detection of Wi-Fi transmitter RF fingerprints," *Electron. Lett.*, vol. 46, no. 16, pp. 1165–1167, Aug. 2010.

[7] H. C. Choe, C. E. Poole, M. Y. Andrea, and H. H. Szu, "Novel identification of intercepted signals from unknown radio transmitters," in *Proc. SPIE*, 1995, pp. 504–518.

[8] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Communications, Internet, and Information Technology*. Anaheim, CA, USA: ACTA Press, 2004, pp. 201–206.

[9] J. Toonstra and W. Kinsner, "Transient analysis and genetic algorithms for classification," in *Proc. Conf. Commun. Power Comput. (IEEE WESCANEX)*, 1995, pp. 432–437.

[10] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, 2008, pp. 116–127.

[11] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of RFID devices," in *Proc. USENIX Security Symp.*, 2009, pp. 199–214.

[12] D. Kaplan and D. M. Stanhope, "Waveform collection for use in wireless telephone identification," U.S. Patent 5 99 980 6A, 1999.

[13] N. O. Tippenhauer, K. B. Rasmussen, C. Pöpper, and S. Èapkun, "Attacks on public WLAN-based positioning systems," in *Proc. 7th Int. Conf. Mobile Syst. Appl. Services*, 2009, pp. 29–40.

[14] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.

[15] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. IEEE Int. Conf. Commun.*, 2008, pp. 1520–1524.

[16] P. V. Nikitin, R. Martinez, S. Ramamurthy, H. Leland, G. Spiess, and K. Rao, "Phase based spatial identification of UHF RFID tags," in *Proc. IEEE Int. Conf. RFID (IEEE RFID)*, 2010, pp. 102–109.

[17] A. A. Larionov, R. E. Ivanov, and V. M. Vishnevsky, "UHF RFID in automatic vehicle identification: Analysis and simulation," *IEEE J. Radio Freq. Identification*, vol. 1, no. 1, pp. 3–12, Mar. 2017.

[18] *Wireless LAN Medium Access Control and Physical Layer Specifications*, IEEE Standard 802.11, Aug. 1999.

[19] B. Kauffmann, F. Baccelli, A. Chaintreau, V. Mhatre, K. Papagiannaki, and C. Diot, "Measurement-based self organization of interfering 802.11 wireless access networks," in *Proc. INFOCOM*, 2007, pp. 1451–1459.

[20] A. Candore, O. Kocabas, and F. Koushanfar, "Robust stable radiometric fingerprinting for wireless devices," in *Proc. IEEE Int. Workshop Hardw. Orient. Security Trust*, 2009, pp. 43–49.

[21] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proc. Int. Conf. Inf. Process. Sensor Netw.*, 2009, pp. 25–36.

[22] M. Debbah, "Mobile flexible networks: The challenges ahead," in *Proc. Int. Conf. Adv. Technol. Commun.*, 2008, pp. 3–7.

[23] N. Hu and Y.-D. Yao, "Identification of legacy radios in a cognitive radio network using a radio frequency fingerprinting based method," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2012, pp. 1597–1602.

[24] M. Marcus, "Progress in VHF/NHF mobile transmitter identification," Dept. Elect. Comput. Eng., Univ. Manitoba, Winnipeg, MB, Canada, Rep. 33, 1992.

[25] K. G. Gard, L. E. Larson, and M. B. Steer, "The impact of RF front-end characteristics on the spectral regrowth of communications signals," *IEEE Trans. Microw. Theory Techn.*, vol. 53, no. 6, pp. 2179–2186, Jun. 2005.

[26] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. 3rd ACM Conf. Wireless Netw. Security*, 2010, pp. 89–98.

[27] B. Danev, A. D. Spindler, H. Luecken, and S. Capkun, "Physical-layer identification: Secure or not?" Dept. Comput. Sci., ETH Zürich, Zürich, Switzerland, Rep. 634, 2009.

[28] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*. New York, NY, USA: Springer, 2013.

[29] J. Toonstra and W. Kinsner, "A radio transmitter fingerprinting system ODO-1," in *Proc. Can. Conf. Elect. Comput. Eng.*, 1996, pp. 60–63.

[30] R. D. Hippenstiel and Y. Payal, "Wavelet based transmitter identification," in *Proc. 4th Int. Symp. Signal Process. Appl.*, 1996, pp. 740–742.

[31] S. Xu, L. Xu, Z. Xu, and B. Huang, "Individual radio transmitter identification based on spurious modulation characteristics of signal envelop," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, 2008, pp. 1–5.

[32] G. O. M. Zamora, S. Bergin, and I. O. Kennedy, "Using support vector machines for passive steady state RF fingerprinting," in *Novel Algorithms and Techniques in Telecommunications and Networking*. Dordrecht, The Netherlands: Springer, 2010, pp. 183–188.

[33] M. Leonardi, L. Di Gregorio, and D. Di Fausto, "Air traffic security: Aircraft classification using ADS-B message's phase-pattern," *Aerospace*, vol. 4, no. 4, p. 51, 2017.

[34] M. Woelfle, M. Temple, M. Mullins, and M. Mendenhall, "Detecting identifying and locating Bluetooth devices using RF fingerprints," in *Proc. Mil. Commun. Conf. (MILCOM)*, 2009. [Online]. Available: https://scholar.google.com/scholar?hl=en&q=WoelfleM.TempleM.Mull

insM.MendenhallM.+2009.+Detecting%2C+identifying+and+locating+bluetooth+devices+using+rf+fingerprints.+In+2009+Military+Communications+Conference+MILCOM+2009.+Boston%2C+USA

[35] S. U. Rehman, K. W. Sowerby, and C. Coghill, "RF fingerprint extraction from the energy envelope of an instantaneous transient signal," in *Proc. Aust. Commun. Theory Workshop (AusCTW)*, 2012, pp. 90–95.

[36] D. Zanetti and B. Danev, "Physical-layer identification of UHF RFID tags," in *Proc. 16th Annu. Int. Conf. Mobile Comput. Netw.*, 2010, pp. 353–364.

[37] X. Li, Y. Zhang, and M. G. Amin, "Multifrequency-based range estimation of RFID tags," in *Proc. IEEE Int. Conf. RFID*, 2009, pp. 147–154.

[38] K. I. Talbot, P. R. Duley, and M. H. Hyatt, "Specific emitter identification and verification," *Technol. Rev.*, vol. 11, pp. 113–133, 2003.

[39] Y. Honglin and H. Aiqun, "Fountainhead and uniqueness of RF fingerprint," *J. Southeast Univ. Nat. Sci. Ed.*, vol. 39, no. 2, pp. 230–233, 2009.

[40] Y.-J. Yuan, X. Wang, Z.-T. Huang, and Z.-C. Sha, "Detection of radio transient signal based on permutation entropy and GLRT," *Wireless Pers. Commun.*, vol. 82, pp. 1047–1057, Jan. 2015.

[41] K. Ellis and N. Serinken, "Characteristics of radio transmitter fingerprints," *Radio Sci.*, vol. 36, no. 4, pp. 585–597, 2001.

[42] O. H. Tekbas, N. Serinken, and O. Ureten, "An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions," *Can. J. Elect. Comput. Eng.*, vol. 29, no. 3, pp. 203–209, Jul. 2004.

[43] Ö. H. Tekbas, O. Üreten, and N. Serinken, "Improvement of transmitter identification system for low SNR transients," *Electron. Lett.*, vol. 40, no. 3, pp. 182–183, Feb. 2004.

[44] M. Barbeau, J. Hall, and E. Kranakis, "Detection of rogue devices in Bluetooth networks using radio frequency fingerprinting," in *Proc. 3rd IASTED Int. Conf. Commun. Comput. Netw. (CCN)*, 2006, pp. 4–6.

[45] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Proc. 3rd Int. Conf. Security Privacy Commun. Netw. Workshops (SecureComm)*, 2007, pp. 331–340.

[46] C. Zhao, T.-Y. Chi, L. Huang, Y. Yao, and S.-Y. Kuo, "Wireless local area network cards identification based on transient fingerprinting," *Wireless Commun. Mobile Comput.*, vol. 13, no. 7, pp. 711–718, 2013.

[47] T. Higuchi, "Approach to an irregular time series on the basis of the fractal theory," *Physica D Nonlinear Phenom.*, vol. 31, no. 2, pp. 277–283, 1988.

[48] O. Ureten and N. Serinken, "Bayesian detection of Wi-Fi transmitter RF fingerprints," *Electron. Lett.*, vol. 41, no. 6, pp. 373–374, 2005.

[49] D. Shaw and W. Kinsner, "Multifractal modeling of radio transmitter transients for classification," in *Proc. Conf. Commun. Power Comput. (IEEE WESCANEX)*, 1997, pp. 306–312.

[50] J. Hall, M. Barbeau, and E. Kranakis, "Detection of transient in radio frequency fingerprinting using signal phase," in *Proc. Wireless Opt. Commun.*, 2003, pp. 13–18.

[51] L. Huang, M. Gao, C. Zhao, and X. Wu, "Detection of Wi-Fi transmitter transients using statistical method," in *Proc. IEEE Int. Conf. Signal Process. Commun. Comput. (ICSPCC)*, 2013, pp. 1–5.

[52] R. W. Klein, M. A. Temple, M. J. Mendenhall, and D. R. Reising, "Sensitivity analysis of burst detection and RF fingerprinting classification performance," in *Proc. IEEE Int. Conf. Commun.*, 2009, pp. 1–5.

[53] Y. Cao, W.-W. Tung, J. Gao, V. A. Protopopescu, and L. M. Hively, "Detecting dynamical changes in time series using the permutation entropy," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 70, no. 4, 2004, Art. no. 046217.

[54] C. Bandt and B. Pompe, "Permutation entropy: A natural complexity measure for time series," *Phys. Rev. Lett.*, vol. 88, no. 17, 2002, Art. no. 174102.

[55] S. M. Kay, *Fundamentals of Statistical Signal Processing*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[56] Y. Shi and M. A. Jensen, "Improved radiometric identification of wireless devices using MIMO transmission," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1346–1354, Dec. 2011.

[57] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau, "Radio transmitter fingerprinting: A steady state frequency domain approach," in *Proc. IEEE 68th Veh. Technol. Conf.*, 2008, pp. 1–5.

[58] W. C. Suski, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Radio frequency fingerprinting commercial communication devices to enhance electronic security," *Int. J. Electron. Security Digital Forensics*, vol. 1, no. 3, pp. 301–322, 2008.

[59] P. Scanlon, I. O. Kennedy, and Y. Liu, "Feature extraction approaches to RF fingerprinting for device identification in femtocells," *Bell Labs Tech. J.*, vol. 15, no. 3, pp. 141–151, Dec. 2010.

[60] R. M. Gerdes, T. E. Daniels, M. Mina, and S. Russell, "Device identification via analog signal fingerprinting: A matched filter approach," in *Proc. NDSS*, 2006. [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=R.+M.+Gerdes%2C+T.+E.+Daniels%2C+M.+Mina%2C+and+S.+Russell%2C+%22Device+identification+via+analog+signal+fingerprinting%3A+a+matched+filter+approach%2C%22+in+NDSS%2C+2006&btnG=

[61] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, pp. 449–462, Mar. 2010.

[62] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security," *J. Commun. Netw.*, vol. 11, no. 6, pp. 544–555, Dec. 2009.

[63] W. C. Suski, II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *Proc. IEEE Glob. Telecommun. Conf. (IEEE GLOBECOM)*, 2008, pp. 1–5.

[64] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet denoising to improve OFDM-based signal detection and classification," *Security Commun. Netw.*, vol. 3, no. 1, pp. 71–82, 2010.

[65] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID tags," *IEEE Trans. Depend. Secure Comput.*, vol. 8, no. 6, pp. 938–943, Nov. 2011.

[66] S. C. G. Periaswamy, D. R. Thompson, H. P. Romero, and J. Di, "Fingerprinting radio frequency identification tags using timing characteristics," in *Proc. Workshop RFID Security (RFID-Sec) Asia*, 2010, pp. 73–82.

[67] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Trans. Depend. Secure Comput.*, vol. 2, no. 2, pp. 93–108, Apr.–Jun. 2005.

[68] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improved wireless security for GMSK-based devices using RF fingerprinting," *Int. J. Electron. Security Digit. Forensics*, vol. 3, no. 1, pp. 41–59, 2010.

[69] M. D. Williams, M. A. Temple, and D. R. Reising, "Augmenting bit-level network security using physical layer RF-DNA fingerprinting," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2010, pp. 1–6.

[70] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improving intra-cellular security using air monitoring with RF fingerprints," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2010, pp. 1–6.

[71] S. Dolatshahi, A. Polak, and D. L. Goeckel, "Identification of wireless users via power amplifier imperfections," in *Proc. Conf. Rec. 44th Asilomar Conf. Signals Syst. Comput.*, 2010, pp. 1553–1557.

[72] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 1st Quart., 2016.

[73] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.

[74] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," in *Proc. IEEE INFOCOM*, 2011, pp. 1404–1412.

[75] K. Remley *et al.*, "Electromagnetic signatures of WLAN cards and network security," in *Proc. 5th IEEE Int. Symp. Signal Process. Inf. Technol.*, 2005, pp. 484–488.

[76] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proc. 27th Conf. Comput. Commun. (IEEE INFOCOM)*, 2008, pp. 1768–1776.

[77] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proc. 13th Annu. ACM Int. Conf. Mobile Comput. Netw.*, 2007, pp. 111–122.

[78] R. S. Campos and L. Lovisolo, "RF fingerprinting location techniques," in *Handbook of Position Location: Theory, Practice, and Advances*. Hoboken, NJ, USA: Wiley, 2011, pp. 487–520.

[79] S. Theodoridis and K. Koutroumbas, "Pattern recognition," *IEEE Trans. Neural Netw.*, vol. 19, no. 2, p. 376, Jul. 2008.

[80] Z. Prekopcsák and D. Lemire, "Time series classification by class-specific Mahalanobis distance measures," *Adv. Data Anal. Classification*, vol. 6, no. 3, pp. 185–200, 2012.

[81] G. Baldini and G. Steri, "A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1761–1789, 3rd Quart., 2017.

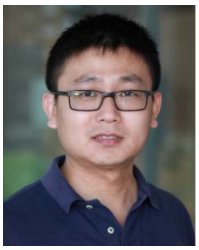
[82] B. Widrow and M. A. Lehr, "30 years of adaptive neural networks: Perceptron, madaline, and backpropagation," *Proc. IEEE*, vol. 78, no. 9, pp. 1415–1442, Sep. 1990.

[83] G. X. Zhang, W. Jin, and L. Hu, "Resemblance coefficient based intra-pulse feature extraction approach for radar emitter signals," *Chin. J. Electron.*, vol. 14, no. 2, pp. 337–341, 2005.
[84] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1180–1192, Jun. 2015.

Naeimeh Soltanieh was born in Zanjan, Iran, in 1991. She received the B.Sc. degree in electronics engineering from Zanjan University in 2012, and the M.Sc. degree in telecommunication engineering from the Sahand University of Technology in 2014. She is currently pursuing the Ph.D. degree in telecommunication engineering with the Amirkabir University of Technology, focusing on radio frequency fingerprinting.

She has completed one year visitor student program with Melbourne University. She is currently attending same program with the University of Technology Sydney, researching about transient based radio frequency identification and verification. Her research interests include signal processing, radio frequency identification, information theory, and communication systems.

Yaser Norouzi (Member, IEEE) was born in Tafresh, Iran, in 1981. He received the B.S., M.S., and Ph.D. degrees in communication engineering from the Sharif University of Technology, Tehran, Iran, in 2002, 2004, and 2008, respectively. He is currently with the Department of Electrical Engineering, Amirkabir University of Technology (Tehran Polytechnique). His fields of research include radar waveform design, signal detection, and parameter estimation.



Yang Yang (Senior Member, IEEE) was born in Bayan Nur, China. He received the Ph.D. degree from Monash University, Melbourne, VIC, Australia, in 2013.

He has three years of industry experience with Rain Bird Australia serving as an Asia-Pacific GSP Engineer, from 2012 to 2015. In April 2015, he returned to academia working in the field of microwave and antenna technologies, with the Centre for Collaboration in Electromagnetic and Antenna Engineering, Macquarie University. In April 2016, he was appointed a Research Fellow with the State Key Laboratory of Terahertz and Millimeter Waves, City University of Hong Kong. In December 2016, he joined University of Technology Sydney, Australia. He is currently a Senior Lecturer and a Team Leader of millimetre-wave integrated circuits and antennas. He has over 150 international peer reviewed publications in microwave and millimetre-wave circuits and antennas.

Dr. Yang received the Corporate 2014 Global GSP Success Award (one globally). He is a Global Winner of the CST University Publication Award 2018, by CST, Dassault Systèmes. He is currently an Associate Editor of IEEE ACCESS, and an Area Editor of *Microwave and Optical Technology Letters*.

Nemai Chandra Karmakar (Senior Member, IEEE) received the Ph.D. degree in information technology and electrical engineering from the University of Queensland, St. Lucia, QLD, Australia, in 1999. He has 20 years of teaching, design, and research experience in smart antennas, microwave active and passive circuits, and chipless RFIDs in both industry and academia in Australia, Canada, Singapore, and Bangladesh. He is currently an Associate Professor with the Department of Electrical and Computer Systems Engineering, Monash University, Melbourne, VIC, Australia. He has authored and coauthored over 230 referred journal and conference papers, 24 referred book chapters and 3 edited and 1 coauthored book in the field of RFID. He has two patent applications for chipless RFIDs.