IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 17, 2018, accepted January 22, 2019, date of publication January 31, 2019, date of current version February 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2896696

RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum

MEMDUH KÖSE[1], SELÇUK TAŞCIOĞLU[2], AND ZİYA TELATAR[2]
[1]Computer Sciences Research and Application Center, Kır ehir Ahi Evran University, 40100 Kır ehir, Turkey
[2]Department of Electrical and Electronics Engineering, Ankara University, 06830 Ankara, Turkey

Corresponding author: Selçuk Ta cıo lu (selcuk.tascioglu@eng.ankara.edu.tr)

ABSTRACT Radio frequency (RF) fingerprinting is considered as one of the promising techniques to enhance wireless security in the Internet of Things (IoT) applications. In this paper, a low-complexity RF fingerprinting method for classification of wireless IoT devices is proposed. The method is based on the energy spectrum of the transmitter turn-on transient signals from which unique characteristics of wireless devices are extracted. The number of spectral components to be used is determined through a proposed approach based on the estimated transient duration value. Transient duration estimation is achieved from the smoothed versions of the instantaneous amplitude characteristics of transmitter signals, which are obtained through a sliding window averaging method. Classification performance of the proposed spectral fingerprints is assessed using experimental data and described by a confusion matrix. The discrimination effectiveness of the spectral fingerprints is quantified by a class separability criterion and evaluated for different noise levels through Monte Carlo simulations. It is demonstrated that the proposed fingerprints outperform the classification performance of two existing fingerprints especially at low signal-to-noise ratio. Additionally, computational complexity analysis of the classifier using the proposed fingerprints is provided.

INDEX TERMS Internet of Things (IoT) security, radio transmitter turn-on transient, RF fingerprinting, transient energy spectrum, wireless device identification.

I. INTRODUCTION

With the increasing use of Internet of Things (IoT) devices and technologies in critical applications such as smart healthcare, smart cities, and smart vehicles, efficient and low-complexity wireless security solutions are becoming more crucial. Traditional security techniques such as cryptographic methods cannot be directly applied to wireless IoT devices due to their limited energy and computing resources [1], [2]. RF fingerprinting has been an emerging security solution for IoT devices and employed in many IoT applications [3]–[6], since it relies only on intrinsic hardware characteristics without requiring additional hardware and computational cost.

RF fingerprinting is the process of analyzing the unique characteristics of wireless devices, which are induced by manufacturing tolerances of the physical layer components, for the aim of identifying wireless devices. A device identification system based on RF fingerprinting consists of detection, feature extraction, and classification stages. After detecting the transmitted signal which conveys the identifiable information, unique features are extracted to generate the fingerprints, and these fingerprints are classified. This approach has been proposed for various wireless devices so far, including very high frequency (VHF) transmitters [7]–[10], wireless fidelity (WiFi) transceivers [11]–[17], global system for mobile communications (GSM) transceivers [18], universal mobile telecommunications system (UMTS) transceivers [19], worldwide interoperability for microwave access (WiMAX) transceivers [16], [20], wireless personal area network (WPAN) transceivers [21]–[25].

RF fingerprints can be extracted from different regions of transmitted signals such as turn-on transient, preamble, and data regions. For example, RF fingerprints were extracted from WiFi preamble and WiMAX near transient signal regions by using discrete Gabor transform in [16]. For a selected signal region, distinctive features can be extracted from different signal characteristics. The most widely used signal characteristics are instantaneous amplitude, phase, and frequency. For example in [11],

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

instantaneous amplitude and phase profiles of transient signals were presented as candidate features, and classification performance of the instantaneous amplitude was evaluated for IEEE 802.11b signals. In [26], instantaneous amplitude characteristics were used as features to compare the performance of two different classifiers, the k-nearest neighbor classifier and probabilistic neural network classifier, in the problem of identification of WiFi devices. Additionally, several statistical features extracted from instantaneous signal attributes have been used to construct RF fingerprints of wireless devices, such as standard deviation, variance, skewness, and kurtosis [4], [14], [18], [20], [25], [27], [28]. In [27], features based on descriptive statistics were extracted from the transients of WiFi devices for classification purpose, and it was demonstrated that some of descriptive statistics, which measure the central tendency and dispersion of data, can be combined to generate more distinctive feature sets. For a systematic review of physical-layer identification systems, see [29].

A. SPECTRAL FINGERPRINTS

Previous works have demonstrated that spectral fingerprints are useful for classifying wireless devices [7], [12], [14], [19]–[21], [24], [30]–[32]. Wavelet transforms of turn-on transients [7], [24] and preambles [14] of the transmitted signals have been used to extract spectral fingerprints. Besides, spectral fingerprints have been obtained by using Fourier transform of preambles [12], [19], [20], [30]–[32] and turn-on transients [21]. In [12], power spectral density values calculated using discrete Fourier transform of the preambles were used as fingerprints to classify IEEE 802.11a signals. The classification was accomplished by cross-correlating the extracted fingerprint of the unknown test signal with the fingerprints of the known reference signals and finding the maximum correlation value. Kennedy *et al.* employed steady state spectral features to identify UMTS devices [19], [30]. The authors investigated the effect of the number of spectral features on classification accuracy and observed that their method requires more spectral features for high classification accuracy at low SNR conditions. In [20], higher-order statistics such as standard deviation, variance, skewness, and kurtosis obtained from power spectral density of preamble signal regions were used as fingerprints for classification of WiMAX devices. Device classification was carried out by applying the statistical fingerprint vectors to a multiple discriminant analysis/maximum likelihood process. Danev and Capkun [21] proposed a transient-based fingerprinting technique to identify IEEE 802.15.4 radio transceivers and evaluated the robustness of the technique in dynamic environments. Spectral Fisher features were extracted from the relative differences between adjacent fast Fourier transform spectra of the transient data samples by using linear discriminant analysis. Mahalanobis distance was used to calculate the similarity between the test and template feature vectors. A summary of these works in terms of spectral features and signal parts employed for identification is provided in Table 1.

TABLE 1. Summary of device identification methods using spectral fingerprints.

Signal Part	Feature	Reference
Transient	FFT coefficients	[21]
Transient	Wavelet coefficients	[7], [24]
Preamble	FFT coefficients	[12], [19], [20], [30]–[32]
Preamble	Wavelet coefficients	[14]

B. CONTRIBUTIONS

The proposed fingerprinting method has two main contributions and differences compared to the previous spectral fingerprinting methods. First, unlike earlier spectral domain approaches using power spectral density of the preamble signals [12], [19], [20], [30]–[32], the proposed spectral fingerprints are achieved from energy spectrum of turn-on transient signals. Turn-on transients are emitted before the transmitter sends any information that can be decoded at the receiver therefore a classification system using turn-on transients has the potential to achieve the least latency compared to classification systems based on steady state characteristics. This feature is highly desirable in IoT applications, e.g. smart healthcare and smart vehicles, where the latency is of critical importance and the device authentication has to be performed before the actual data transmission starts.

Second, in contrast to the Fourier transform-based methods in [12], [19]–[21], and [30]–[32], the RF fingerprinting method proposed herein employs only small number of spectral components rather than the entire spectrum. In order to determine the number of spectral components, we propose an approach based on transient duration estimation. In this approach, the transient duration estimation is performed by using a sliding window averaging technique which is applied to instantaneous amplitude characteristics of transmitter signals. Moreover, in the proposed RF fingerprinting method, it is not required to reduce the input dimensionality unlike the methods in [19]–[21] and [30], since the number of spectral coefficients in feature vectors is small. These two advantages result in less computational complexity for feature extraction compared to the existing techniques using spectral fingerprints, which may contribute to the proliferation of cost-efficient commercial IoT applications.

The proposed fingerprinting method is evaluated using experimental data collected from eight different wireless IoT devices, IEEE 802.11b WiFi transceivers. The classification performance and computational complexity of the transmitter classifier using the proposed fingerprints are compared with those using two transient-based fingerprints introduced in [11] where the authors proposed to use instantaneous amplitude characteristics (hereafter called amplitude features) and their dimensionally reduced forms obtained by

using principal component analysis (hereafter called PCA features). Experimental results show that the proposed fingerprints have a better classification performance than the two existing fingerprints especially at low SNR conditions.

The outline of the paper is as follows: In Section II, turn-on transient behavior of WiFi devices is explained and visualized through instantaneous characteristics of signals. In Section III, the proposed RF fingerprinting method based on transient energy spectrum is presented. In Section IV, computational complexity of classification method using spectral fingerprints is analyzed. Effect of additive channel noise on the spectral features is investigated in Section V. The class separability criterion used to measure the classification capability of the feature sets is given in Section VI. The classification performance test results are presented in Section VII, and lastly, Section VIII concludes the paper.

II. TURN-ON TRANSIENT BEHAVIOR OF WiFi DEVICES

The IEEE 802.11b standard specifies the limits for transmit power-on and power-down ramp durations to avoid spreading power to adjacent channels [33]. Transmitters from various manufacturers have a variety of power-on duration within the value defined by the standard. Furthermore, this duration differs for the devices of the same model and type due to manufacturing tolerances of the physical layer components [11]. The signal within power-on duration has a transient behavior and continues until the transmitter generates a stable carrier signal. Transient signals have unique characteristics attributed to combination of hardware imperfections in the analog circuitry, which can be exploited to identify the wireless devices [11], [29].

Transient behavior of the transmitter signals can be represented by means of instantaneous characteristics of signals, such as instantaneous amplitude, phase, and frequency. These characteristics have been used in wireless device identification systems [11], [14], [18], [20]. In Fig. 1, an intermediate frequency signal from an IEEE 802.11b transmitter and corresponding instantaneous amplitude are shown. For this transmitter, instantaneous amplitude data has a ramp-like structure. In order to show the differences in characteristic behavior of transient signals, instantaneous amplitude profiles of captured transients from three different IEEE 802.11b WiFi transmitters (Tx) are given in the left panel of Fig. 2. Real and imaginary parts of the captured transients are also plotted in the middle panel of the same figure.

III. EXTRACTING RF FINGERPRINTS BASED ON ENERGY SPECTRUM OF TRANSIENT SIGNAL

The block diagram of the device identification procedure based on the proposed spectral fingerprints is given in Fig. 3. Captured real valued intermediate frequency (IF) signals are first transformed to analytic signals by using the Hilbert transform [34]. The analytic IF signal is down-converted to baseband by multiplying with a complex exponential. Since the analytic IF signal has a single sided spectrum, complex baseband signal centered at 0 Hz is obtained without the need to suppress the unwanted spectral images. The received complex-valued baseband signal can be modeled as:

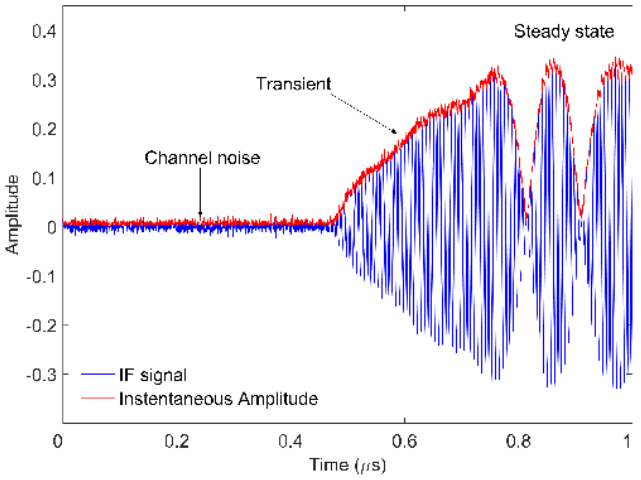

FIGURE 1. A captured IF signal from IEEE 802.11b transmitter (blue) and corresponding instantaneous amplitude (red).

$$x(n) = \begin{cases} v(n) & \text{if } 1 \le n \le m \\ s_t(n-m) + v(n) & \text{if } m < n \le p \\ s_s(n-p) + v(n) & \text{if } p < n \le L \end{cases} \quad (1)$$

where $s_t(n)$ and $s_s(n)$ are the transient and steady state signals, respectively, $v(n)$ is complex Gaussian noise, n is the discrete time index, m and p are start and end points of transients, respectively, and L is the total number of samples.

The details of transient detection and fingerprint generation stages are given in the following sections. Lastly, generated spectral fingerprints are classified by using a probabilistic neural network (PNN) classifier.

A. TRANSIENT DETECTION

Accurate separation of the transient signal from the noise and the steady state part of the received signal is important to extract actual fingerprints. In this study, transient detection is performed on instantaneous amplitude profiles. For the received baseband signal of the form

$$x(n) = x_I(n) + jx_Q(n) \quad (2)$$

where $x_I(n)$ and $x_Q(n)$ denote real and imaginary parts, respectively, the instantaneous amplitude can be calculated by

$$a(n) = \sqrt{x_I{}^2(n) + x_Q{}^2(n)}. \quad (3)$$

The instantaneous amplitude of the complex baseband signal, $a(n)$, is the same with that of the analytic IF signal. Note that shifting the frequency of the analytic signal by multiplying by a complex exponential does not change the instantaneous amplitude profile, since $|exp(-jw_c n)| = 1$, where w_c is the IF carrier frequency.

In this work, turn-on transient starting point estimation is carried out by using a Bayesian ramp change detector [35],

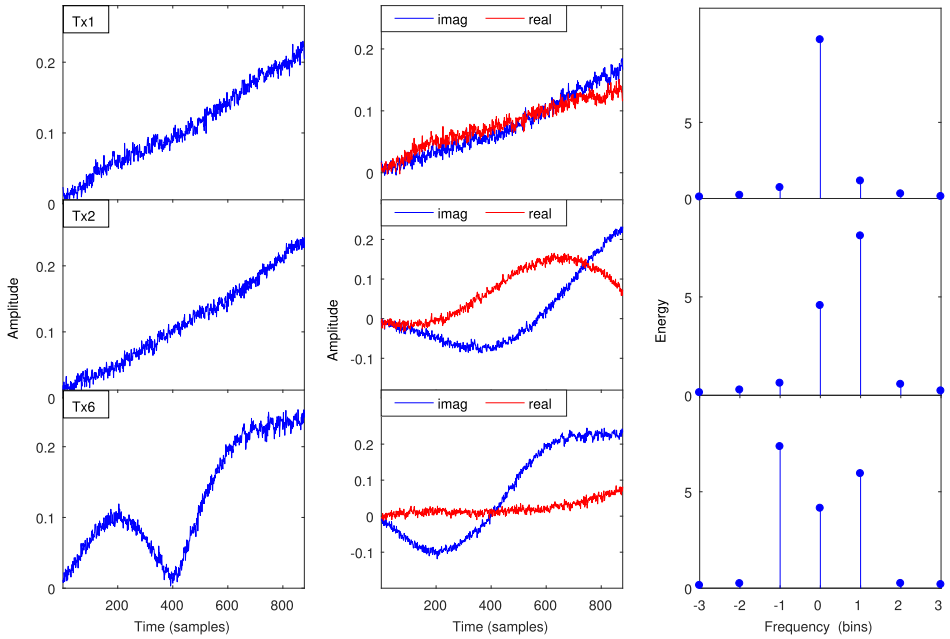

FIGURE 2. Instantaneous amplitude profiles (left panel), real and imaginary parts (middle panel), and energy spectral coefficients (right panel) of complex transient signals for three different WiFi transmitters.

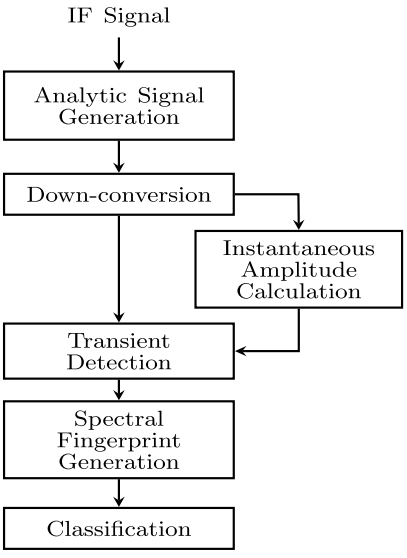

FIGURE 3. Spectral RF fingerprinting system block diagram.

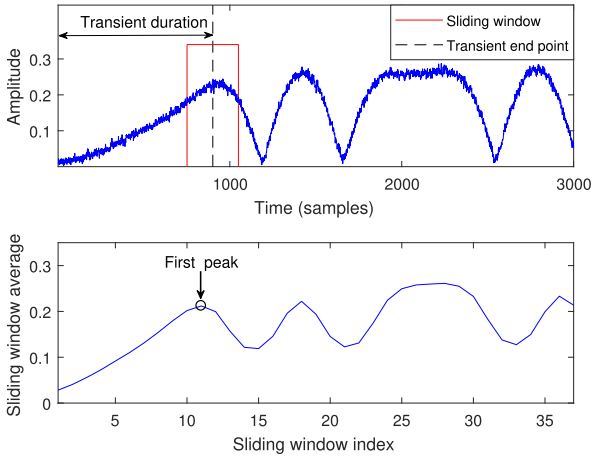

FIGURE 4. Instantaneous amplitude (top) of a received WiFi signal and the corresponding average values (bottom) obtained through a sliding window.

in which the instantaneous amplitude data of a WiFi radio is modeled as a ramp function. Within this approach, detection of the transient starting point is considered as a change point detection problem and solved in a Bayesian framework. In [36], the performance of this detector for different SNR conditions was evaluated, and also the effect of transient detection errors on the performance of a transient-based identification system was investigated.

For the transient end point estimation, a method is proposed based on average instantaneous amplitude samples. In this method, averaging process is performed by using a sliding window approach. Instantaneous amplitude values in the sliding window are averaged to produce a smoothed amplitude signal. Estimation procedure can be explained by Fig. 4, where instantaneous amplitude (top) of a received WiFi signal and the corresponding sliding window average (bottom) are given. Initial sample for the sliding window is taken as the estimated start point of the transient. As can be seen from this figure, sliding window average in the steady state region fluctuates around a value of approximately half the maximum value. In order to determine the point where transient signal ends and steady state signal starts,

the first peak above half the maximum value is found in the smoothed amplitude signal, which is shown with a circle marker in Fig. 4 (bottom). The sliding window position from which this average value is obtained is shown with red lines in Fig. 4 (top). The center point of this window is taken as the estimate of the transient end point.

Transient duration (in samples) can now be determined by

$$N = \hat{p} - \hat{m} \tag{4}$$

where $\hat{m}$ and $\hat{p}$ denote the estimated start and end points of the transient, respectively. Then, transient signal is obtained as follows:

$$x_t(i) = x(\hat{m} + i), \quad \text{for } 1 \leq i \leq N \tag{5}$$

where $x(\cdot)$ denotes the complex baseband signal in the interval $(\hat{m}, \hat{p}]$.

B. GENERATING SPECTRAL RF FINGERPRINTS

As opposed to steady state parts of the transmitted signals such as preambles and data, transient signals do not have periodic structure and are widely scaled by their energy instead of power in the signal [37]. Therefore the energy spectrum is the most commonly used function for transient signals and can be approximated by using discrete Fourier transform (DFT) as

$$E(k) = \frac{1}{N}\left|\sum_{n=0}^{N-1}\left(x_t(n)\exp\left(-j2\pi kn/N\right)\right)\right|^2 \tag{6}$$

where $x_t(n)$ stands for the complex samples of transient signal, n and k denote the discrete time and frequency indices, respectively.

The energy spectrums of the transients from three different IEEE 802.11b WiFi transmitters are given in the right panel of Fig. 2. In this figure, the frequency-domain signals are plotted such that the direct current (DC) component is in the center of the spectrum. The negative frequency bins between $N/2+1$ and $N-1$ are represented with negative index, e.g. DFT frequency bins $k = N-2$ and $k = N-1$ are represented as $k = -2$ and $k = -1$, respectively.

Distinct characteristics of the transients can be seen from both time and frequency domain representations of the transients in Fig. 2. For example, the transient from Tx6 has a quasi-periodic structure in time domain with a spectrum containing strong peaks at the first positive and negative frequency bins. The transient from Tx1 on the other hand has a ramp structure in the time domain, which has a spectrum composed of large DC and small harmonic components. The right panel of this figure also demonstrates that the information in energy spectrum is concentrated in a few low-frequency components. This can be explained by the fact that the practical radios are implemented using image rejection filters with high out-of-band rejection to prevent interference between adjacent channels. This figure also shows that the distribution of the transient energy over these spectral components carries the information about the characteristic behavior of the transients. The main idea of this paper is to use these observations in identifying wireless devices.

Based on these observations, the number of energy spectral coefficients carrying characteristic information is calculated as

$$K = \left[\frac{W}{\Delta f}\right] \tag{7}$$

where $[\cdot]$ denotes the integer part of a number, W is the transmission bandwidth, Δf is the frequency resolution of the DFT and is defined by

$$\Delta f = \frac{1}{T_d} = \frac{1}{NT_s} = \frac{f_s}{N} \tag{8}$$

where T_d is the average transient duration in seconds, T_s and f_s denote sampling period and sampling frequency, respectively.

Since the analyzed complex signals are centered at 0 Hz, spectral fingerprints are defined as sets of energy spectral coefficients consisting of the DC component, K_p lowest positive and K_n lowest negative frequency components. The number of positive and negative frequency components are calculated as follows

$$K_n = [(K-1)/2] \tag{9}$$

$$K_p = K - K_n - 1. \tag{10}$$

Note that $K_p = K_n$ for odd values of fingerprint length K, and $K_p = K_n + 1$ for even values of K.

IV. COMPUTATIONAL COMPLEXITY

In device identification process, feature extraction is carried out prior to classification. For the proposed spectral features, the computational complexity of feature extraction using (6) is $O(N)$, since only three spectral coefficients (for $k = 0$, 1, and $N-1$) need to be calculated as will be explained in Section VII-A. This provides an advantage in terms of computational complexity over the methods using the entire spectrum such as [12], [19]–[21], [30], and [31], which have the usual $O(N\log(N))$ complexity. Besides, these methods have an additional computational complexity resulting from dimension reduction procedures such as linear discriminant analysis [20], multiple discriminant analysis [21], and averaging [19], [30]. On the other hand, dimension reduction is not a requirement for our proposed fingerprinting approach since the fingerprints are generated from a small number of spectral components.

For the compared transient-based fingerprints, principal component analysis (PCA) features are obtained by projecting the test vectors onto a lower dimensional subspace. This projection is performed using a projection matrix which is calculated during training stage. In [11], feature dimension was reduced from N to 5 using principal component analysis. Therefore, computational complexity of PCA feature extraction is $O(N)$ due to the multiplication of $1 \times N$ test vector and $N \times 5$ projection matrix. Amplitude features proposed in the

same study do not require any additional computations therefore yields a computational complexity of $O(1)$ for feature extraction stage.

In this work, the fingerprints of WiFi transmitters are classified by using a probabilistic neural network (PNN) classifier to evaluate the classification performance. PNN classifier has a computational complexity of $O(MN)$ where M and N denote the number of training vectors and feature size, respectively. For a detailed description of the PNN classifier and the issues of its computational complexity, see [38]. Classification with the amplitude features proposed in [11] has this computational complexity value, since the entire instantaneous amplitude data of length N is used as feature vectors. For the PCA features, the computational complexity of the classification process reduces to $O(M)$ due to dimension reduction (from N to 5). Similarly, the computational complexity of the PNN classifier using the proposed spectral fingerprints is $O(M)$, since only three spectral components are employed as features.

The total computational complexities in testing stage, including feature extraction process, for the spectral, PCA, and amplitude features are presented in Table 2. These results show that computational complexities in testing stage for spectral and PCA features are the same, which is lower than the complexity of the amplitude features.

TABLE 2. Computational complexities in testing stage, including feature extraction, for three different features.

Features	Computational Complexity
Spectral(proposed)	$O(M+N)$
PCA	$O(M+N)$
Amplitude	$O(MN)$

Training stage of the classifier using the spectral features has a computational complexity of $O(MN)$, since three spectral coefficients are calculated by using (6) for M training vectors. On the other hand, the computational complexity in training stage for eigenvalue decomposition based PCA is $O(MN^2+N^3)$ [39]. In training stage, low computational complexity of the classifier using the spectral features can provide an advantage over that using the PCA features for mobile systems which have ability to learn in the field, such as cognitive radios. In such a system, the extracted spectral fingerprints consisting of a small number of spectral coefficients in mobile IoT devices can be exchanged in a cooperative network. Thus an enhanced transmitter identification system can be achieved using space diversity advantage of cooperative systems.

V. ADDITIVE NOISE EFFECT ON THE SPECTRAL FEATURES

The effect of additive noise on the proposed features is investigated by adding recorded channel noise samples to captured transients to reduce SNR of the transients. SNR estimation of noisy transient signal is obtained by

$$SNR = 10\log_{10}\left(\frac{E_{SN}}{E_N} - 1\right) \tag{11}$$

where E_{SN} is the average energy of the noisy transient, and E_N is the average energy of the noise signal. The average noise energy at the collected SNR level is estimated by using the channel noise samples prior to the start of the transient. In [40], it was shown by simulations that this estimator can be used for the SNR values encountered in many practical applications.

Instantaneous amplitude profiles of a captured IEEE 802.11b transmitter signal for transient SNR levels of 24 dB (top) and 12 dB (bottom) are shown in Fig. 5. As seen from this figure, noise corrupts the instantaneous amplitude profile of the transient signal, which leads to classification performance degradation for the features extracted from this profile, e.g. amplitude features. In order to visualize the additive noise effect on the proposed spectral features, three dimensional spectral features obtained from eight WiFi transmitters at the collected SNR (approximately 25 dB) and 0 dB SNR levels are presented in Fig. 6. PCA features are also shown for the same SNR levels in Fig. 7. The number of principal components was set to 3 in order to visually compare the noise effect on separability of these two features in the three dimensional feature space. Fig. 6(a) and Fig. 7(a) show that both spectral and PCA features are visually distinctive at the collected SNR. As the SNR level decreases to 0 dB, the spread of both the features increases (see Fig. 6(b) and Fig. 7(b)). It is visually observed from these figures that, at 0 dB SNR, PCA features substantially lose their distinctiveness whereas the spectral features keep their ability to separate the classes with a relatively small degradation in performance. Quantitative evaluation of the additive noise effect on discrimination effectiveness of the spectral, PCA, and amplitude features is performed through Monte Carlo simulations in Section VII-C.

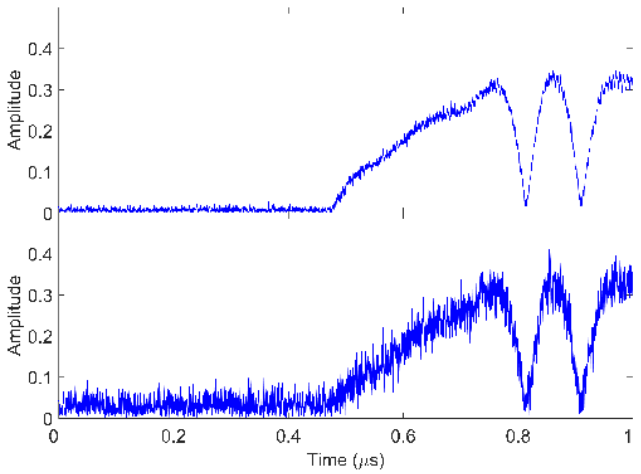

FIGURE 5. Instantaneous amplitude profiles of a captured IEEE 802.11b transmitter signal for transient SNR levels of 24 dB (top) and 12 dB (bottom).

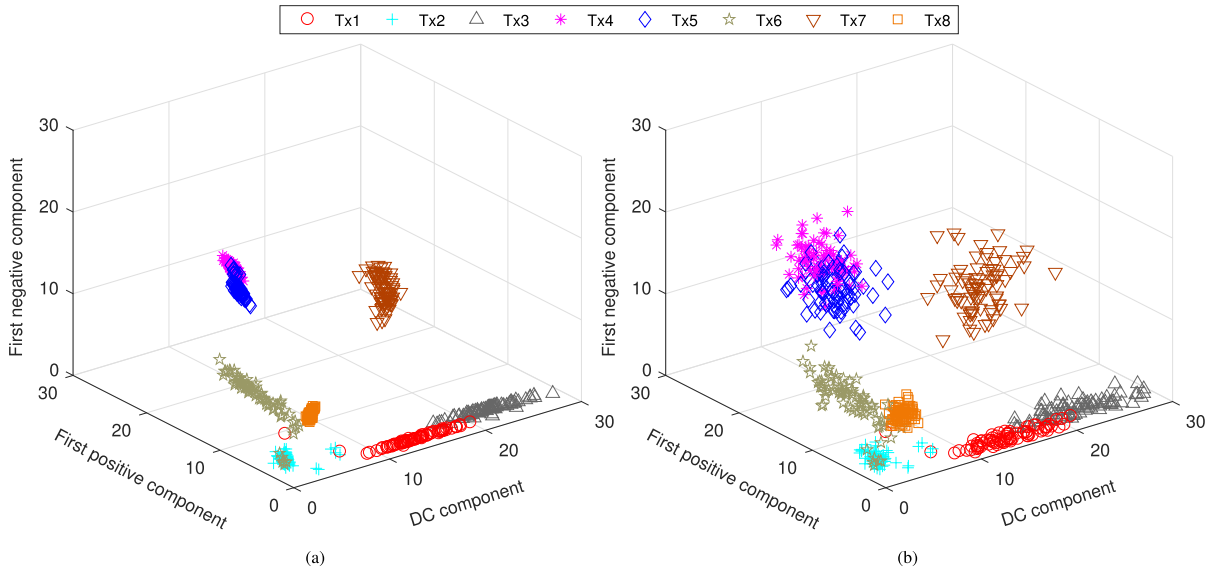

FIGURE 6. Spectral features at (a) the collected SNR and (b) 0 dB SNR.

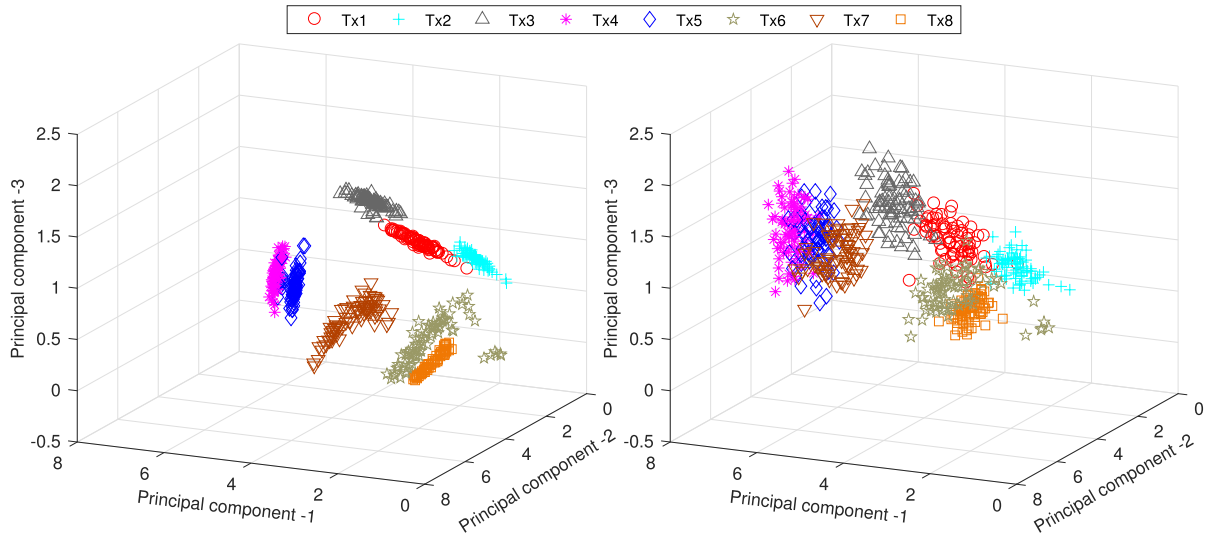

FIGURE 7. PCA features at (a) the collected SNR and (b) 0 dB SNR.

VI. CLASSIFICATION CAPABILITY OF THE FEATURE SETS

In order to quantify the classification capability of the feature vectors and analyze the detrimental effect of additive noise on classification performance, a class separability criterion based on scatter matrices was calculated. The scatter matrices, including with-in class scatter matrix S_w, between class scatter matrix S_b, and total scatter matrix S_t, are defined as [38]

$$S_w = \sum_{i=1}^{M} \sum_{x \in C_i} (x - \mu_i)(x - \mu_i)^T \tag{12}$$

$$S_b = \sum_{i=1}^{M} n_i (\mu_i - \mu_0)(\mu_i - \mu_0)^T \tag{13}$$

$$S_t = S_w + S_b \tag{14}$$

where x is a sample in the feature space, C_i is the i*th* subset in the set of all classes (C), n_i is the number of samples in class C_i, M is the number of classes, μ_i is the mean vector of the i*th* class, μ_0 is the global mean vector over all classes, and $(\cdot)^T$ denotes the transpose of a matrix. A class separability criterion J can be defined as [41]

$$J = \mathrm{tr}(S_w^{-1} S_t) \tag{15}$$

where $\mathrm{tr}(\cdot)$ represents the trace of a matrix. Large values of J indicate that samples of each class are closely clustered around their mean, and the clusters are well separated from each other [41]. J values for the feature sets extracted from experimental data are given in Sections VII-B and VII-C.

VII. CLASSIFICATION PERFORMANCE EVALUATION

The classification performance of the spectral fingerprints was tested using a data set collected from eight different IEEE 802.11b WiFi devices and compared with those of amplitude and PCA fingerprints. The data set contains

100 transmissions from each of the devices operating in the 2.4 GHz ISM band, which were first down-converted to the intermediate frequency of 160 MHz and then digitized at a rate of 5 GSamples/s by using a digital oscilloscope. In order to classify devices, digitized IF signals were applied to the spectral RF fingerprinting system given in Fig. 3. Classification performances of the three different fingerprints were evaluated using Monte Carlo cross-validation where, in each trial, 20 of 100 transients were selected randomly from each WiFi transmitter for training set, and the remaining 80 transients were employed as a test set. Therefore, 640 test signals were classified at each trial. The sizes of the training and test sets were determined by using the experimental results in [26], in which the impact of the size of the training set on the classification performance was analyzed and it was shown that increasing the training sample size above 20 had a negligible effect on the classification performance. Classification was carried out using a PNN classifier [38].

A. TRANSIENT DURATION AND FEATURE LENGTH

In classification tests, transient detection was first performed using the procedure defined in Section III-A. For the transient end point estimation, a sliding window with a size of 300 samples and %75 overlap was used in order to ensure sufficient smoothing for data. The details of transient starting point estimation using the Bayesian ramp change method can be found in [35]. Once the start and end points of a transient signal were estimated, the transient duration was calculated by using (4). In training stage, an average transient duration was calculated over the estimated transient durations of the training vectors. In the testing stage, this average value was used as the transient duration of the test vectors.

As an example calculation, consider the average transient duration of 878 samples obtained from the entire data set, which corresponds approximately to 176 ns for the sampling rate of 5 GSamples/s. As the training vectors were selected randomly in each test, the average transient duration was found to be approximately in an interval of [850, 900] samples, corresponding to the interval of [170, 180] ns. The values in this interval are close to the value reported in [11], in which transient duration for IEEE 802.11b signals was empirically found to be around 200 ns. For the calculated average transient duration values and the transmission bandwidth of 22 MHz, spectral feature length is found to be 3 by using (7) and (8). Note that, as explained in Section III-B, spectral features of length 3 consist of the DC component ($k = 0$), the first positive ($k = 1$), and the first negative ($k = N - 1$) frequency components.

B. CLASSIFICATION PERFORMANCE AT HIGH SNR

In this test, transients at the collected SNR were applied to the classifier in both the training and testing stages. SNR of the captured transients is measured to be around 25 dB. One hundred trials, in each of which training and test sets were selected randomly, were performed to obtain more accurate performance estimates through Monte Carlo cross-validation. Confusion matrices of transmitter classification results achieved by using the spectral and PCA features at the collected SNR were obtained for each classification test, and the average values over trials are given in Table 3 and Table 4. The rows of the matrix represent the actual classes while the columns represent the predicted classes. The diagonal elements of the matrix are the correct classification rates whereas all off-diagonal elements are misclassified rates.

TABLE 3. Classification results using spectral features at high SNR.

Actual class	Predicted class							
	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7	Tx8
Tx1	95.3	3.1	1.5	0	0	0	0	0.1
Tx2	0.5	98.4	0.1	0	0	0.6	0	0.4
Tx3	4.3	0.4	95.3	0	0	0	0	0
Tx4	0	0	0	99.4	0.6	0	0	0
Tx5	0	0	0	3.9	96.1	0	0	0
Tx6	0	0.8	0	0	0	98.7	0	0.5
Tx7	0	0	0	0	0	0	100	0
Tx8	0	0	0	0	0	0	0	100

TABLE 4. Classification results using PCA features at high SNR.

Actual class	Predicted class							
	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7	Tx8
Tx1	94.6	3.9	1.5	0	0	0	0	0
Tx2	0	100	0	0	0	0	0	0
Tx3	3.0	0.8	96.2	0	0	0	0	0
Tx4	0	0	0	100	0	0	0	0
Tx5	0	0	0	11.0	89.0	0	0	0
Tx6	0	0.9	0	0	0	97.7	0	1.4
Tx7	0	0	0	0	0	0	100	0
Tx8	0	0	0	0	0	0	0	100

The class separability measure J defined by (15) for all combinations of two classes were also obtained from the classification test sets. The average J values are given in Table 5 and Table 6 for the spectral and PCA features, respectively. It is observed from Table 3 and Table 4, that the most confusing three pairs of transmitters are Tx1-Tx2, Tx1-Tx3, and Tx4-Tx5 for both spectral and PCA features. The corresponding J values for these class pairs in Table 5 and Table 6 are small, which implies that these pairs have large within-class variance and/or small between-class distance.

The average of the diagonal elements of the confusion matrices in Table 3 and Table 4 gives the average classification performance. The average classification error rates for Spectral(3), Amplitude(1024), and PCA(5) features were obtained as 2.09%, 2.61%, and 2.80%, respectively. The values in parentheses next to the feature names represent the dimension of the feature vector. When the number of principal components was set to 3 to construct PCA(3) features which are given in Fig. 7 for the purpose of visual

TABLE 5. *J* values for spectral features at high SNR.

	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7
Tx2	3.11						
Tx3	2.10	7.46					
Tx4	162.56	143.55	177.56				
Tx5	80.48	75.71	88.63	3.78			
Tx6	6.11	3.90	11.11	11.14	9.28		
Tx7	34.34	40.79	55.47	84.15	91.65	32.77	
Tx8	48.93	59.33	79.38	155.46	95.34	12.40	70.21

TABLE 6. *J* values for PCA features at high SNR.

	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7
Tx2	3.72						
Tx3	3.86	4.99					
Tx4	661.64	513.20	490.56				
Tx5	298.85	270.34	225.48	3.40			
Tx6	15.44	13.37	18.53	89.63	46.11		
Tx7	267.95	228.65	147.13	172.53	166.54	35.43	
Tx8	69.80	63.12	63.33	250.73	68.86	5.59	376.01

comparison, the average classification error rate was found to be 2.95%. The classification error histograms for the three different features at the collected SNR are given in Fig. 8. These results show that all the features have a similar classification performance at the collected SNR.

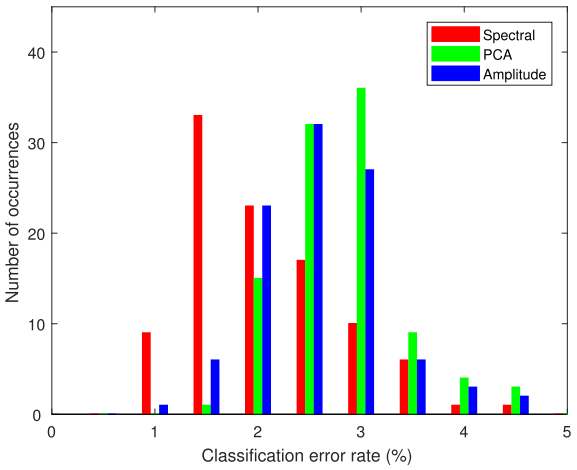

FIGURE 8. Classification error histograms for Spectral(3), Amplitude(1024), and PCA(5) features at the collected SNR.

C. EFFECT OF ADDITIVE NOISE ON CLASSIFICATION PERFORMANCE

Classification performances of three different fingerprints were tested for low SNR conditions. Low SNR transient signals were classified by using the PNN classifier trained with high SNR transient signals collected in a controlled environment. To simulate low SNR conditions, SNR levels of test transients were reduced by adding recorded channel noise to collected transients. Channel noise samples were recorded by using the data acquisition system during no transmission. Recorded noise samples were scaled and added to the collected test signals to change SNR level in the range of 0 dB to 20 dB with 1 dB steps.

For a given SNR level, a training set at the collected SNR was selected randomly and classification tests were performed. For a fixed training set, fifty different recorded noise signals were added to the test signals prior to feature generation. Three different fingerprints were extracted from the same test signals corrupted by the same recorded noise samples for fair comparison. This process was repeated fifty times where training set was selected randomly in each trial. Classification error rates at each SNR level were calculated by averaging over trials.

Confusion matrices and *J* values for the spectral and PCA features were calculated through classification simulations at 10 dB SNR. The average values are given in Tables 7-10. From these tables, it is observed that average of the diagonal elements of the confusion matrices and all the *J* values decrease for both features when compared to the values in Tables 3-6, which were obtained at the collected SNR. This can be explained by the fact that the distance between the classes for each pair becomes smaller and the variance of

TABLE 7. Classification results using spectral features at 10 dB SNR.

Actual class	Predicted class							
	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7	Tx8
Tx1	94.6	3.1	2.3	0	0	0	0	0
Tx2	0.5	98.7	0.1	0	0	0.4	0	0.3
Tx3	4.7	0.3	95.0	0	0	0	0	0
Tx4	0	0	0	88.0	12.0	0	0	0
Tx5	0	0	0	7.4	92.6	0	0	0
Tx6	0	1.0	0	0	0	98.4	0	0.6
Tx7	0	0	0	0	0	0	100	0
Tx8	0	0	0	0	0	0	0	100

TABLE 8. Classification results using PCA features at 10 dB SNR.

Actual class	Predicted class							
	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7	Tx8
Tx1	92.7	1.6	5.7	0	0	0	0	0
Tx2	1.6	98.4	0	0	0	0	0	0
Tx3	2.0	0.6	97.4	0	0	0	0	0
Tx4	0	0	0	100	0	0	0	0
Tx5	0	0	0	33.2	66.8	0	0	0
Tx6	0	1.2	0	0	0	97.9	0	0.9
Tx7	0	0	0	0	0	0	100	0
Tx8	0	0	0	0	0	0	0	100

TABLE 9. *J* values for spectral features at 10 dB SNR.

	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7
Tx2	3.09						
Tx3	1.99	7.01					
Tx4	72.61	70.41	87.01				
Tx5	49.22	47.04	58.78	1.86			
Tx6	5.69	3.70	9.40	8.02	5.85		
Tx7	23.68	30.82	28.53	32.76	34.13	23.73	
Tx8	31.36	28.00	41.19	57.52	37.15	5.25	26.10

TABLE 10. *J* values for PCA features at 10 dB SNR.

	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7
Tx2	2.15						
Tx3	1.75	4.00					
Tx4	56.42	110.31	40.16				
Tx5	51.01	87.48	36.61	1.63			
Tx6	7.05	7.10	9.92	36.98	28.75		
Tx7	44.17	43.63	26.91	38.27	39.54	9.93	
Tx8	15.77	21.27	17.03	54.55	31.87	2.17	55.93

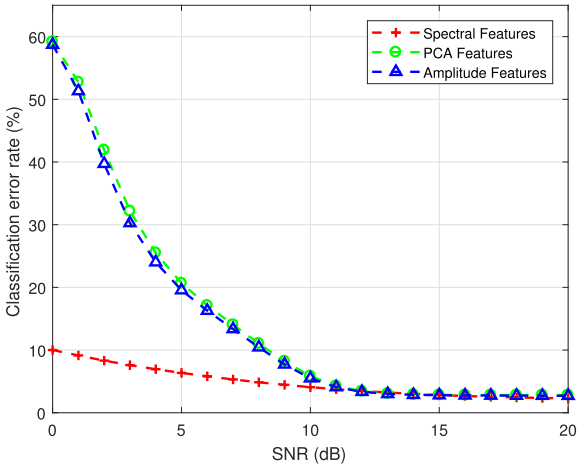

FIGURE 9. Average classification error rates for Spectral(3), Amplitude(1024), and PCA(5) features at different SNR levels.

the samples within each class becomes larger with increasing noise level. The most confusing three pairs of the transmitters for both spectral and PCA features are the same as those at the collected SNR: Tx1-Tx2, Tx1-Tx3, and Tx4-Tx5.

The average classification error rates for SNR levels of 0-20 dB are plotted in Fig. 9. This figure shows that the average classification performance of the spectral features is significantly better than the amplitude and PCA features, as the SNR decreases below 10 dB. Incorrect classification rate exceeds 10% at SNR values below 9 dB for amplitude and PCA features, whereas the error rates for the spectral features are below 10% at the SNR levels between 0 and 20 dB. At 20 dB SNR, all the features have a similar classification error rate of about 2.5%. As the SNR level decreases to 0 dB, the amplitude and PCA features lose their ability to discriminate the classes of interest whereas the spectral features have a classification accuracy of 90%. The classification error histograms for spectral and PCA features at 0 dB SNR are given in Fig. 10. Error histogram of amplitude features is not presented in this figure, since it has similar form to that obtained for PCA features. The average classification errors were found to be 10%, 59%, and 59% for spectral, amplitude, and PCA features, respectively.

Robustness of the proposed spectral features to additive noise can be explained by considering the effect of additive noise on strong spectral components used as features. The energy ratio of three spectral components to total signal energy was calculated as about 90% at the collected SNR for 800 transient signals. Therefore the effect of noise on three strong components, in terms of separability, is small

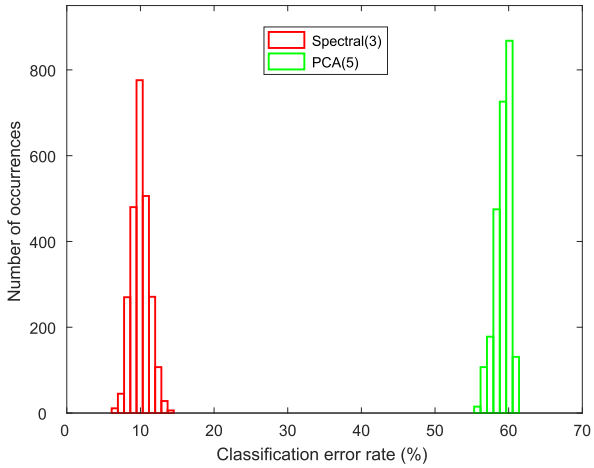

FIGURE 10. Average classification error histograms for Spectral(3) and PCA(5) features at 0 dB SNR.

even when the SNR of transient signal is low (see Fig. 6 (b)). Since the objective herein is to assess the robustness of the features with respect to additive noise, start and end points of the transients were set to the estimated values at the collected SNR for all the three methods as the SNR was changed.

VIII. CONCLUSIONS

In this work, RF fingerprints of WiFi transmitters were extracted from energy spectrums of transient signals for device classification. Experimental test results showed that the proposed spectral fingerprints could be used to classify the WiFi devices with a high classification accuracy. It was also verified by simulations that the spectral fingerprints were robust to additive noise. Based on the transient duration estimations, the number of spectral coefficients constituting the RF fingerprints was found to be 3 for IEEE 802.11b devices.

In order to use the proposed technique for the classification of other type of wireless IoT devices, one needs to determine the number of the spectral features to be used. Once the number of the spectral features is fixed, entire spectrum of the analyzed signal does not need to be calculated. This provides an advantage in terms of computational complexity over the other spectral transform-based methods which use entire spectrum. Besides, dimension reduction is not required in our proposed technique since the transient characteristics can be represented with a small number of spectral components. These advantages are particularly attractive for low-cost IoT applications. In the device classification system using the proposed RF fingerprints, the investigation of the impact of using low-cost receivers and the performance analysis for classification of different IoT devices are subjects for future work.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[3] 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 Things J.*, to be published. doi: 10.1109/JIOT.2018.2838071.

[4] C. M. Talbot, M. A. Temple, T. J. Carbino, and J. A. Betances, "Detecting rogue attacks on commercial wireless Insteon home automation systems," *Comput. Secur.*, vol. 74, pp. 296–307, May 2018.

[5] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of Things," in *Proc. IEEE 17th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2016, pp. 1–3.

[6] 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.

[7] J. Toonstra and W. Kinsner, "Transient analysis and genetic algorithms for classification," in *Proc. IEEE Conf. Commun., Power, Comput. (WESCANEX)*, vol. 2, May 1995, pp. 432–437.

[8] O. Ureten and N. Serinken, "Detection of radio transmitter turn-on transients," *Electron. Lett.*, vol. 35, no. 23, pp. 1996–1997, Nov. 1999.

[9] N. Serinken and O. Ureten, "Generalised dimension characterisation of radio transmitter turn-on transients," *Electron. Lett.*, vol. 36, no. 12, pp. 1064–1066, Jun. 2000.

[10] K. J. Ellis and L. Serinken, "Characteristics of radio transmitter fingerprints," *J. Radio Sci.*, vol. 36, no. 4, pp. 585–597, Jul./Aug. 2001.

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

[12] 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 Global Telecommun. Conf. (GLOBECOM)*, Nov./Dec. 2008, pp. 1–5.

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

[14] 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.

[15] P. Padilla, J. L. Padilla, and J. F. Valenzuela-Valdés, "Radiofrequency identification of wireless devices based on RF fingerprinting," *Electron. Lett.*, vol. 49, no. 22, pp. 1409–1410, Oct. 2013.

[16] 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.

[17] S. Ta cio lu, M. Köse, and Z. Telatar, "Effect of sampling rate on transient based RF fingerprinting," in *Proc. 10th Int. Conf. Elect. Electron. Eng. (ELECO)*, 2017, pp. 1156–1160.

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

[19] I. O. Kennedy, P. Scanlon, and M. M. Buddhikot, "Passive steady state RF fingerprinting: A cognitive technique for scalable deployment of co-channel femto cell underlays," in *Proc. 3rd IEEE Symp. New Frontiers Dyn. Spectr. Access Netw.*, Oct. 2008, pp. 1–12.

[20] M. D. Williams, S. A. Munns, M. A. Temple, and M. J. Mendenhall, "RF-DNA fingerprinting for airport WiMAX communications security," in *Proc. 4th Int. Conf. Netw. Syst. Secur. (NSS)*, 2010, pp. 32–39.

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

[22] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 160–167, Feb. 2018.

[23] T. J. Bihl, K. W. Bauer, and M. A. Temple, "Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1862–1874, Aug. 2016.

[24] J. Hall, M. Barbeau, and E. Kranakis, "Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting," in *Proc. 3rd IASTED Int. Conf. Commun. Comput. Netw.*, 2006, pp. 108–113.

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

[26] M. Köse and Z. Telatar, "An approach on identification of 802.11b devices by RF signature in wireless local area networks," in *Proc. IEEE 18th Signal Process. Commun. Appl. Conf. (SIU)*, Apr. 2010, pp. 800–803.

[27] M. Köse, S. Ta cio lu, and Z. Telatar, "Wireless device identification using descriptive statistics," *Commun. Fac. Sci. Univ. Ankara A2-A3*, vol. 57, no. 1, pp. 1–10, 2015.

[28] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, and Y. C. Kim, "Intrinsic physical-layer authentication of integrated circuits," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 14–24, Feb. 2012.

[29] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, no. 1, Nov. 2012, Art. no. 6.

[30] 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. (VTC-Fall)*, Sep. 2008, pp. 1–5.

[31] S. U. Rehman, K. Sowerby, and C. Coghill, "Analysis of receiver front end on the performance of RF fingerprinting," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 2494–2499.

[32] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," *IET Commun.*, vol. 8, no. 8, pp. 1274–1284, May 2014.

[33] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11, 2012.

[34] R. G. Lyons, *Understanding Digital Signal Processing*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.

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

[36] M. Köse, S. Ta cio lu, and Z. Telatar, "The effect of transient detection errors on RF fingerprint classification performance," in *Proc. 14th Int. Conf. Circuits, Syst., Electron., Control Signal Process. (CSECS)*, 2015, pp. 89–93.

[37] A. Brandt, *Noise and Vibration Analysis: Signal Analysis and Experimental Procedures*. Chichester, U.K.: Wiley, 2011.

[38] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed. New York, NY, USA: Wiley, 2001.

[39] S. Shalev-Shwartz and S. Ben-David, *Understanding Machine Learning: From Theory to Algorithms*. New York, NY, USA: Cambridge Univ. Press, 2014.

[40] M. Köse, S. Ta cio lu, and Z. Telatar, "Signal-to-noise ratio estimation of noisy transient signals," *Commun. Fac. Sci. Univ. Ankara A2-A3*, vol. 57, no. 1, pp. 11–19, 2015.

[41] S. Theodoridis and K. Koutroumbas, *Pattern Recognition*, 4th ed. San Diego, CA, USA: Elsevier, 2009.

MEMDUH KÖSE received the B.S. and M.S. degrees from the Department of Electrical and Electronics Engineering, Ankara University, in 1996 and 2000, respectively, where he is currently pursuing the Ph.D. degree and he was a Specialist with the Electronics Engineering Department, from 1999 to 2010. He has been a Researcher with the Computer Sciences Research and Application Center, Kır ehir Ahi Evran University, since 2010. His current research interest includes physical layer security of wireless networks.

SELÇUK TAŞCIOĞLU received the Ph.D. degree in electronics engineering from Ankara University, Ankara, Turkey, in 2011, where he was a Research Assistant with the Department of Electrical and Electronics Engineering, from 2002 to 2011, and he is currently an Assistant Professor. He was a Visiting Fellow with the Communications Research Centre Canada with a grant from the International Research Fellowship Programme of the Scientific and Technological Research Council of Turkey, from 2007 to 2008. His research interests include spectrum sensing and the identification of wireless devices.

ZİYA TELATAR received the B.S. degree in electronics and communication engineering from Yildiz University, in 1983, and the M.S. and Ph.D. degrees in electronics engineering from Ankara University, in 1992 and 1996, respectively, where he has been with the Department of Electrical and Electronics Engineering since 1996, as an Assistant Professor, Associate Professor, and he is currently Professor. His research interests include image processing, pattern recognition, with a focus on applications in biological and medical image analysis and communications with a focus spectrum sensing, and RF device signature detection.