Radio Identity Verification-based IoT Security Using RF-DNA Fingerprints and SVM

Donald Reising, *Senior Member, IEEE,* Joseph Cancelleri, T. Daniel Loveless, *Senior Member, IEEE,*
Farah Kandah, *Senior Member, IEEE,* and Anthony Skjellum *Senior Member, IEEE*

***Abstract*—It is estimated that the number of Internet of Things (IoT) devices will reach 75 billion in the next five years. Most of those currently and soon-to-be deployed devices lack sufficient security to protect themselves and their networks from attacks by malicious IoT devices masquerading as authorized devices in order to circumvent digital authentication approaches. This work presents a Physical (PHY) layer IoT authentication approach capable of addressing this critical security need through the use of feature-reduced, Radio Frequency-Distinct Native Attributes (RF-DNA) fingerprints and Support Vector Machines (SVM). This work successfully demonstrates (i) authorized Identity (ID) verification across three trials of six randomly chosen radios at signal-to-noise ratios greater than or equal to 6 dB and (ii) rejection of all rogue radio ID spoofing attacks at signal-to-noise ratios greater than or equal to 3 dB using RF-DNA fingerprints whose features are selected using the Relief-F algorithm.**

***Index Terms*—IoT Security, RF Fingerprinting, Support Vector Machines, Feature Selection, Radio ID Authentication**

I. Introduction

THE Internet of Things (IoT) is a collection of semi-autonomous, internet-connected devices, each comprising inexpensive computing, networking, sensing, and actuation capabilities for sensing and acting within the physical world [1]. The number of deployed IoT devices continues to explode annually and is estimated to reach roughly 75 billion by 2025 [2]–[4]. Alarmingly, 70% of all IoT devices do not employ encryption. Common reasons include (i) limited on-board computational capability, (ii) prohibitive cost for the manufacturer to implement, and (iii) scalability issues associated with implementation and management [5]–[7]. The resulting lower security makes such devices—and the associated infrastructure—susceptible to attack by other devices that are incorrectly authenticated through their use of compromised digital credentials (e.g., priorly transmitted in clear text). Thus, there is a critical need for an IoT-security approach capable of defeating attacks in which illegitimate devices digitally masquerade as authorized IoT devices to circumvent digital authentication approaches. The need is exacerbated because bad actors exploit this weakness to conduct attacks against IoT infrastructure, not just devices [8]–[15].

Recently, the physical (PHY) layer approach known as Specific Emitter Identification (SEI) has been put forward as a solution capable of addressing this critical IoT need [16], [17]. One specific SEI implementation, known as Radio Frequency (RF) fingerprinting, facilitates radio discrimination by exploiting the unintentional "coloration" that is inherently imparted upon a radio's waveform during its generation and transmission [18]–[56]. This radio-specific coloration comes from the distinct characteristics of each radio, as well as interactions associated with the devices and components that make up a radio's RF front-end (e.g., mixers, amplifiers, filters, etc.). Security approaches based upon RF fingerprints are difficult to bypass because they exploit the inherent, unique, and difficult to imitate features (e.g., amplifier non-linearity, carrier frequency offset, etc.) present within a given radio's transmitted waveforms [57], [58].

The majority of RF fingerprinting work has focused on radio *classification* (a.k.a. *identification*) [18]–[45], [53], [56]. In classification, an *unknown* radio's identity is determined through the comparison of its RF fingerprint(s) with each of the stored reference models that represent the *authorized/known* radios—representing a one-to-many comparison. The radio identity associated with the reference model that results in the "best" match is said to be the originator of the RF fingerprint(s). The flaw in classification is that class assignment—in this case the radio assigned as the RF fingerprint originator—is made no matter how poor this "best" match might be. This flaw can result in network access being granted to *rogue* radios. As defined in [50], a rogue radio is one that intentionally falsifies its digital credentials (e.g., compromised passwords or encryption keys, spoofed MAC addresses or equivalent digital identities) to match those of an authorized radio to bypass digital security mechanisms.

The potential for a rogue radio being classified as an authorized radio has led to the proposal of a one-to-one comparison known as radio identity (ID) *verification* (a.k.a. *authentication*) [16], [31], [46]–[50], [52]–[55], as opposed to classification. In radio ID verification, the RF fingerprint(s) of the unknown radio are compared *only* to the stored reference model associated with the presented digital ID [50]. Thus, the unknown radio's ID is either verified as that of an authorized radio or rejected as a rogue. In the presence of rogue radios,

D. Reising and T. Loveless are with the Department of Electrical Engineering, University of Tennessee at Chattanooga, Chattanooga, TN, 37403 USA. Email: {donald-reising, gsy536, daniel-loveless}@utc.edu.

J. Cancelleri was with the Electrical Engineering Department, University of Tennessee at Chattanooga, at the time of this work. He is now with NASA MSFC, Huntsville, AL 35808. Email: joseph.c.cancelleri@nasa.gov.

F. Kandah is with the Department of Computer Science and Engineering, University of Tennessee at Chattanooga, Chattanooga, TN, 37403 USA. Email: farah-kandah@utc.edu.

A. Skjellum is the Director of the SimCenter, University of Tennessee at Chattanooga, Chattanooga, TN, 37403 USA. Email: tony-skjellum@utc.edu.

Manuscript received THE DATE; revised SOME DATE.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.3045305, IEEE Internet of Things Journal

TABLE I
IDENTITY VERIFICATION OUTCOMES (ADOPTED FROM [50])

	System Declaration	
Actual ID	Authorized	Rogue
Authorized	True Verification (TVR)	False Reject (FRR)
Rogue	False Verification (FVR)	True Reject (TRR)

radio ID verification results in four possible outcomes, which were introduced in [50] and are presented in Table I.

In this work, we present a radio-ID-verification-based IoT security approach using RF-Distinct Native Attributes (RF-DNA) fingerprints and Support Vector Machines (SVM). Our work differs from prior RF fingerprinting-based ID verification approaches in that feature selection is assessed using eight different techniques and driven by the authorized radio whose ID is to be verified. Given the one-to-one nature of radio ID verification, the RF-DNA fingerprints can differ in composition and number of features from one authorized radio to another. The key in this case is that, prior to feature selection, the RF-DNA fingerprints of every radio (i.e., authorized and rogue) are generated to be composed of the same set of features. Then, "best" SVM model selection is performed using a novel approach that does not require any knowledge of the rogue radios' RF-DNA fingerprints.

The remainder of this paper is structured as follows. First, a description of system configuration is presented in Section II and the adopted threat model is presented in Section III. The motivation and contributions of this work to the state of the art in RF fingerprint-based ID verification is presented in Section IV. Section V provides a summary of prior RF fingerprint-based ID verification publications. Section VI outlines each stage within the presented ID verification process: signal collection, detection, and post-processing (Sect. VI-A); RF-DNA fingerprint generation (Sect. VI-B); feature selection methods (Sect. VI-C), SVM (Sect. VI-D); selection of the "best" SVM model (Sect. VI-E); and the ID verification approach (Sect. VI-F). The Methodology is followed by the ID verification and rogue rejection performance results and analysis in Section VII, which includes assessment of the developed approach using the eight feature selection approaches (Sect. VII-A) and under degrading channel noise conditions (Sect. VII-B). The conclusion is presented in Section VIII with a summary of future research presented in Section IX.

II. SYSTEM CONFIGURATION

This section provides an explanation of the wireless communication networks and protocols that our ID verification and rogue radio rejection approach is capable of integrating into and supporting. The wireless networks will be described first followed by the protocols.

Wireless communication networks can be categorized as (i) managed or (ii) ad hoc [59]. In a managed wireless network, there is an Access Point (AP) (a.k.a., base station) that provides wireless connections to all of the devices within its coverage area and all communications flow through it. Examples of AP-based wireless networks are IEEE 802.11 Wireless-Fidelity (Wi-Fi), cellular, and IEEE 802.16 World-wide Interoperability for Microwave Access (WiMAX) [60]–[62]. The number of devices supported by a given AP is dependent upon a wide range of factors such as density of the accessing devices, throughput desired by each device, and channel conditions, to name a few [59]. For AP-based wireless networks, our approach can be integrated within the AP itself, because the AP is typically less constrained in terms of size, power, and computational requirements. In Wireless Ad hoc NETorks (WANETs), there is no centralized AP. Instead, each wireless device serves as a node within a self-organized network in which communication links are created between pairs of nodes and routing tables are developed based upon the links [59]. Some examples of WANETs include IEEE 802.15.4 ZigBee, Wi-Fi, and Bluetooth [63], [64]. Because WANETs lack a centralized AP, our approach can be deployed using an "air monitor" to conduct ID verification and rogue rejection for all of the WANET's devices. If the WANET is geographically too large to be covered by a single air monitor, then multiple air monitors can be deployed to ensure that all of the WANET's devices are supported. In this work, the AP-based WiMAX wireless standard is used because of the availability of a waveform data set that consists of a sufficient number of radios (eighteen) to facilitate assessment of authorized radio-ID verification performance when rogue radios are spoofing the digital IDs of the authorized radios.

In terms of wireless protocols, our approach is constrained to protocols from which RF-DNA fingerprints can be extracted. RF-DNA fingerprints can be extracted from either the (i) turn-on transient portion of the waveform or (ii) portions of the waveform associated with a fixed, know sequence of symbols/bits (e.g., the 802.11a Wi-Fi preamble). Prior RF-DNA fingerprinting work has demonstrated success using fingerprints extracted from either of these waveform regions [26], [30], [43], [45], [48], [50], [51], [65]. In this work, the RF-DNA fingerprints are extracted from the turn-on transient portion of the WiMAX mobile subscribers' waveforms. However, our approach can be utilized in IoT systems that rely upon other wireless protocols so long as the RF-DNA fingerprinting constraint, stated above, is satisfied.

III. THREAT MODEL

The threat model adopted in this work is informed by the prior RF-DNA fingerprinting work in [48], [50], [51] as well as the threat models presented in [66], [67]. In this work, the adversary leverages commercially available IoT and compute devices to conduct their attack upon an IoT infrastructure, which is consistent with prior RF-DNA fingerprint-based ID verification research [48], [50], [51]. It is assumed that the adversary has either the knowledge of or access to simple software applications that enable them to modify the settings of their associated IoT and compute devices necessary to conduct their attack [66]. The adversary is not an authorized user of the targeted IoT infrastructure, so they do not inherently have access to its wireless network(s) or the individual IoT and support devices that form the infrastructure. Lastly, it is assumed that the IoT infrastructure communication links and hardware are not initially compromised.

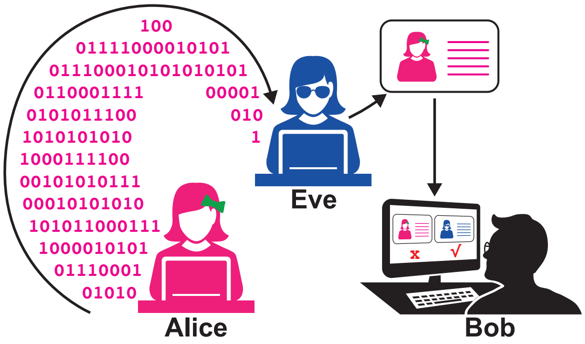


Fig. 1. Threat Model: Lacking encryption, the *rogue* device Eve is able to trick Bob, another authorized IoT device or IoT infrastructure monitor, into thinking that Eve is the authorized IoT device Alice by presenting Alice's digital ID credentials.

Figure 1 provides an illustration of the particular IoT attack of interest within this work, which is the unauthorized network access attack. The adversary, "Eve," is able to gain access to the IoT infrastructure by exploiting the lack of encryption or easily circumventing an incorrectly implemented encryption process. Once encryption is bypassed, Eve is then authenticated by "Bob," an authorized IoT device or IoT infrastructure monitoring device, by presenting the compromised digital credentials (e.g., MAC address, International Mobile Subscriber Identity (IMSI), password, etc.) of another authorized IoT device, "Alice." Once authenticated by Bob, Eve is granted access to the IoT infrastructure and is able to conduct nefarious activities, which may include observation, spoofing, injecting, removal, and alteration of data in real time, as well as spoofing the digital ID of other authorized IoT devices [67].

IV. Motivation and Contributions

Prior publications present results generated using (i) a single feature selection approach, (ii) a set of RF fingerprint features that remain fixed in both number and composition across all authorized and rogue radios, (iii) machine learning models that are developed to maximize classification and *not* ID verification performance, and (iv) threshold-driven performance. The work presented herein provides the following contributions to the area of SEI-based IoT security:

1) Feature selection is performed with ID verification in mind: the number and particular RF-DNA fingerprint features retained are allowed to differ from one authorized radio to another. The use of the same set of features, for every authorized radio, overlooks the specific features that make a given authorized radio unique, which impedes ID verification and rogue rejection performance as SNR degrades.
2) Support Vector Machine (SVM) model development is performed for the sole purpose of performing ID verification and rogue rejection for a given authorized radio. The SVM is trained using a two class approach where class 1 represents the authorized radio whose ID needs to be verified and class 2 represents all other radios, both rogue and authorized. During SVM training, class 2 is developed using the RF-DNA fingerprints of all remaining authorized radios (i.e., those authorized radios whose ID is *not* being verified to serve as a representative sample of possible rogue radios.)
3) ID verification and rogue radio rejection performance is assessed using eight feature selection approaches.
4) A novel approach is presented for selecting the SVM model that is "best" suited to simultaneously maximizing authorized radio ID verification and rogue radio rejection performance without any knowledge nor use of the rogue radios' RF-DNA fingerprints.
5) ID verification and rogue radio rejection performance is presented that does *not* require the setting of a user/administrator defined threshold. Threshold-based approaches require a trade-off between the rate at which the authorized radios' IDs are verified and rogue radios are rejected. So, increasing the ID verification rate requires sacrificing rogue rejection performance and vice versa. This dependency between the verification and rejection rates leads to degraded performance at lower SNR values.
6) Comparative assessment is facilitated by adopting the TVR≥90% and FVR≤10% benchmarks used in [16], [48], [50], [51], [55]. The goal is for the developed RF fingerprint-based ID verification approach to satisfy both of these benchmarks at the lowest SNR possible.

These contributions result in an average TVR=97.8% at SNR=6 dB while rejecting all rogue radio attacks at FVR≤10% for SNR≥3 dB, which is unseen in published literature.

V. Related Work

This section highlights the contributions and differences from previous RF fingerprint-based ID verification work. In [48], RF-DNA fingerprint-based radio ID verification was performed using nine IEEE 802.15.4 ZigBee radios (seven authorized and two rogue), Fisher-based feature selection, and a probabilistic-based verification approach. Using an FVR (Rogue & False Verification) value of ≤10%, 11 out of 14 rogue attacks (i.e., each rogue radio spoofs the ID of each authorized radio) were detected at a signal-to-noise ratio (SNR) of 10 dB. The goal is to achieve FVR≤10% for all 14 rogue radio attacks; a potential reason for the lower rate of rogue rejection may be that the models used for radio authentication were developed for the purpose of classification and *not* for verification.

A rogue radio rejection process based upon the k-Nearest Neighbor (KNN) classifier is presented in [49]. The presented approach achieved an accuracy from a low of 30% up to 94% at SNR=15 dB, a remarkably wide range. Overall, KNN suffers from (i) high outlier sensitivity, (ii) a lack of kernel functions that aid in handling nonlinear data, (iii) requiring hyperparameters that are precisely fine tuned to achieve optimal results, and (iv) being poorly suited to unpredictable cases.

In [50], RF-DNA fingerprints were used to verify the identity of WiMAX radios in the presence of rogue radio attacks. Near-transient signals were collected from a total of 18 WiMAX radios of the same manufacturer and model. The

18 WiMAX radios were divided into three trials of six each. For a given trial, the remaining 12 radios served as the rogues for that trial, which resulted in a total of 72 rogue radio attacks per trial. For the three trials, the highest number of rejected rogue radio attacks was 67 of 72 at a TRR (True Reject) rate of ≥90% and SNR=21 dB. In an effort to reject all rogue radio attacks, a fourth trial was selected. This fourth trial consisted of eight radios and successfully rejected all rogue radio attacks at SNR=21 dB. As in [48], the models and RF-DNA fingerprint feature selection was performed to maximize *classification* performance.

The work in [51] showed the results of radio ID verification of ZigBee radios using RF-DNA fingerprints and verification approaches using test metrics from three classifiers: Random Forest (RndF), Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML), and Generalized Relevance Learning Vector Quantization-Improved (GRLVQI). The RndF and MDA/ML-based approaches use posterior probability, while the GRLVQI-based verification approach uses the angle-distance metric from [50]. The authors in [51] performed feature selection using (i) the RndF classifier's built-in feature importance ranking, (ii) the Kolmogorov-Smirnov test, and (iii) the Dimensional Reduction Analysis (DRA) first presented in [50]. Radio ID verification and rogue rejection was conducted using a total of 13 ZigBee radios of which four were designated as authorized radios and the remaining nine assigned to serve as rogue radios, thus representing a total of 36 rogue attacks (i.e., each rogue radio spoofed the digital ID of each authorized radio). For a TRR≥90%, 31 of 36 (~86%) rogue radio spoofing attacks were rejected using DRA-selected features and RndF-based radio ID verification at an SNR=12 dB. As with the RF-DNA fingerprint-based work in [48], [50], the work in [51] used selected features and authorized radio models originally developed for the purpose of performing "one-to-many" classification, which may have contributed to the poorer rogue radio rejection performance.

In [16], rogue attacks on IoT and commercial home automation systems were detected through the use of Slope-Based Frequency Shift Keyed (SB-FSK) fingerprints and a MDA/ML-based ID verification process. The attacks were carried out by like-model Insteon Switch (IS) devices as well as YARD Stick One Software Defined Radios (SDRs). At SNR=15 dB, a total of 25 IS and 36 YARD Stick One SDR rogue attacks were successfully rejected for TRR=95% (FVR=5%) and TRR=100% (FVR=0%), respectively. As in [48], [50], [51], the work in [16] relied on features and machine learning models that are optimized for classification rather than for ID-verification performance.

SVM-based ID verification—using RF fingerprints drawn from the preambles of the Random Access Channel (RACH) waveforms—of five 3GPP UMTS mobile radios is presented in [46]. For ID verification, SVM is employed using both a single and ensemble-based approach. For ensemble-based ID verification, three configurations are used: tiered, weighted tiered, and double weighted tiered. All of the ensemble-based approaches are implemented using a two-class SVM in which each class represents a single radio. This approach requires the development of an SVM model for all possible paired combinations. Given radios A, B, and C, SVM models are developed for pairs (A and B), (B and C), and (A and C). For the case when a radio presents the digital credentials of A, then its corresponding RF fingerprints are compared with two SVM models: (A and B) and (A and C). Verification of the radio's ID is dependent upon which ensemble approach is selected, but all three consider the class decision returned by each SVM model.

In [53], ID verification is presented using Convolutional Neural Networks (CNN) and RF fingerprints learned from the waveforms of seven IEEE 802.15.4-compliant Zigbee radios. Similar to the work in [55] as well as this work, the work in [53] presents ID verification using a two-class model in which one class represented the authorized radio (a.k.a. case A), whose ID was to be verified, and the other represented all remaining known radios (i.e., the not-A case). Therefore, a total of seven CNNs were trained to perform ID verification. The use of CNN is more computationally and temporally complex than the use of SVM. An average TVR of 92.7% was achieved at SNR=10 dB. Individual ID verification results were not presented nor rogue radio rejection assessed.

The work in [55] presents IoT device authentication implemented via radio ID verification, as described in Sect. I of this work, using RF-DNA fingerprints extracted from the near-transient responses of 18 IEEE 802.16e WiMAX radios, the DRA feature selection approach from [50], and an SVM classifier. Six WiMAX radios were designated as authorized radios and the remaining 12 used as rogue radios. An SVM model was developed for each of the six authorized radios using the RF-DNA fingerprints for all authorized WiMAX radios, where class one represented the radio whose digital ID needed verification and class two represented the remaining five authorized WiMAX radios. The presented approach performed well in verifying the ID of five out of the six authorized radios while rejecting the rogue radios at a rate of 91% or better at SNR≥9 dB. However, for the sixth authorized radio, roughly 88% of the rogue radios' transmissions were verified (that is, FVR=88%) as having originated from this sixth radio at SNR=9 dB. The FVR did not improve with increased SNR, which suggests that the issue lies either with the DRA feature selection approach and/or the SVM classifier. In [55], the DRA features were not chosen for the purpose of verifying the ID of a given authorized radio but for optimizing one-to-many classification performance.

A Mobile IoT (MIoT) device ID verification approach using RF fingerprints and Support Vector Data Description (SVDD) is presented in [68]. The approach uses Principal Component Analysis (PCA) followed by Neighborhood Component Analysis (NCA) to generate the RF fingerprint features from the instantaneous amplitude envelope of the power-on transient signals collected from ten Motorola A12 radios. The presented approach achieved TVR∈[86, 96]% across five authorized radio trials at SNR=15 dB. Each trial was comprised of eight authorized radios to facilitate rogue radio rejection assessment using that trial's two remaining radios. The results achieved FVR∈[6, 9]% for the rogue radios across the five trials at SNR=15 dB. In [68], (i) the RF fingerprints were extracted from the signal's instantaneous amplitude which is easily

TABLE II
NOTATIONS

N_D	Number of radios used in this work	N_B	Number of collected signals per radio	N_O	Order of the Butterworth filter
G_{mk}	Complex Gabor Transform Coefficients	M	Total number of time shifts	N_Δ	Step size between Gabor calculations
K_G	Total number of frequency shifts	N_P	Total patches in the time-frequency plane	N_T	Size of a patch in time
N_F	Size of a patch in frequency	P_{tf}	A single patch in the time-frequency plane	σ	Standard deviation
σ^2	Variance	γ	Skewness	κ	Kurtosis
N_f	Number of RF-DNA fingerprint features	λ	DRA feature relevance vector	$\mathbf{f}$	A single RF-DNA fingerprint
$\mathbf{F}$	A set of RF-DNA fingerprints	$\mathbf{w}$	A projection matrix	c_i	The i^{th} SVM class
$N_{t.i}$	Training fingerprints of class i	N_τ	Total number of training fingerprints	$\bar{\mathbf{F}}$	A set of normalized RF-DNA fingerprints
e	Eigenvectors	λ_e	Eigenvalues	N_r	Number of retained fingerprint features
w_r	Weight assigned to feature r	$\mathcal{B}_r$	Bhattacharyya coefficient of feature r	$N_{\mathcal{B}}$	Number of histogram bins
$\mathcal{F}$	Set of RF-DNA fingerprints with class labels	Υ	A kernel function	ρ	Vector of Probability of Error values
α	Average Correlation Coefficient values	w_ρ	Probability of Error weight	w_α	Average Correlation Coefficient weight
$\mathbf{t}$	Statistic produced by the t-test	N_K	Number of Relief-F nearest neighbors	$\tilde{\mathbf{f}}$	Randomly chosen RF-DNA fingerprint
$\mathbf{f}_H$	Relief-F nearest hit fingerprint	$\mathbf{f}_M$	Relief-F nearest miss fingerprint	β	An SVM support vector
N_z	Number of noise realizations				

corrupted by noise, (ii) only a single feature selection approach was considered, (iii) the RF fingerprints of every radio were comprised of the same number of features, and (iv) TVR≥90% required SNR≥20 dB.

VI. Our Methodology

Our proposed ID verification approach is carried out through the use of six consecutive phases: (i) signal collection, detection, and post-processing; (ii) RF-DNA fingerprint generation; (iii) feature selection; (iv) SVM model development; (v) SVM model selection for ID verification under rogue radio attacks; and, (vi) the ID verification approach.

A. Signal Collection, Detection, and Post-Processing

This section provides a brief explanation of the process used to (i) collect the signals from each of the 18 WiMAX radios, (ii) separate individual transmissions from the overall collection record, and (iii) prepare the detected transmissions for RF-DNA fingerprint generation.

RF-DNA fingerprints are drawn from the near-transient response present at the start of each range-only transmission generated by a WiMAX Mobile Subscriber (MS) radio within the up-link sub-frame. A representative illustration of this near-transient response is shown in Fig. 2. We use the WiMAX near-transient response because we have on hand the data set in [50], [55], which enables comparative analysis.

The near-transient responses of N_D=18 Alvarion BreezeMAX Extreme 5000 802.16e WiMAX MS radios are collected using an Agilent spectrum analyzer. The spectrum analyzer has an RF bandwidth of 36 MHz, operates over the range of frequencies from 20 MHz to 6 GHz, has a maximum sampling rate of 95 mega-sample/s, and has a 12-bit analog-to-digital converter [69]. Amplitude-based variance trajectory detection was used to select a total of N_B=1,000 near-transient responses for each of the WiMAX MS radios [26]. All detected near-transient responses are filtered using an N_O=6th order Butterworth filter and the In-phase and Quadrature (IQ) samples stored for RF-DNA fingerprint generation.

B. RF-DNA Fingerprint Generation

In this section, the process used for generating an RF-DNA fingerprint from a given collected signal is explained. RF-DNA fingerprints are generated from the WiMAX near-transient response's time-frequency (TF) representation, which is calculated using the Discrete Gabor Transform (DGT) [70]. The DGT is chosen because of its computational complexity being proportional to the sampling rate, its robustness to degrading SNR when the calculation is *oversampled*, and its demonstrated success in prior RF-DNA fingerprinting work [50], [55], which facilitates comparative assessment. For all

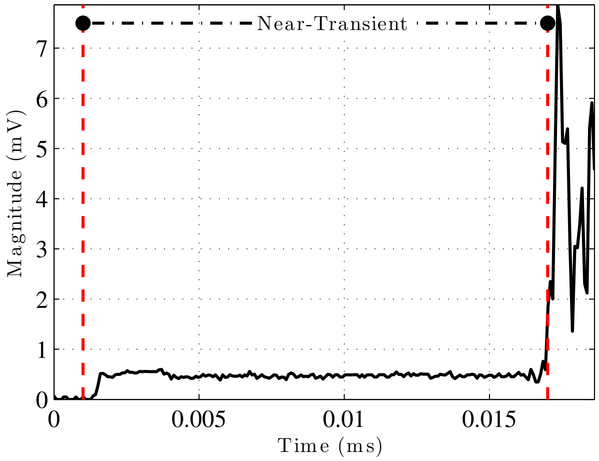


Fig. 2. Representative "near-transient" response from a WiMAX MS radio's range-only transmission within the up-link sub-frame (adopted from [50])

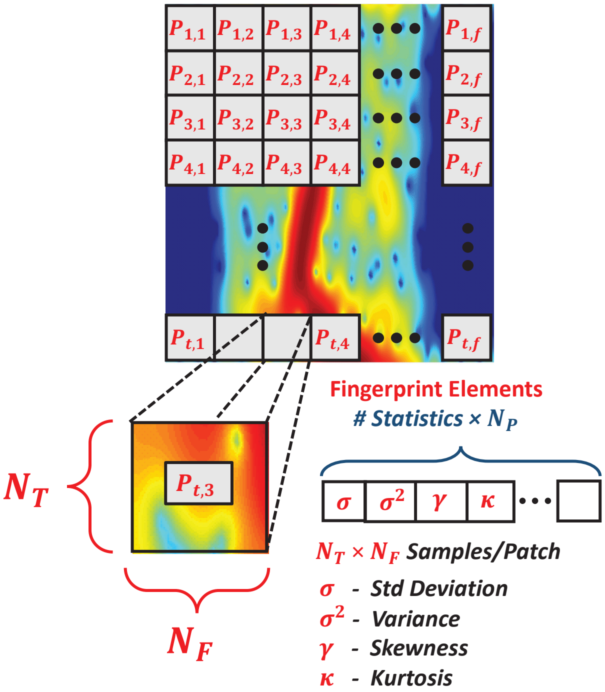

$P_{1,1}$ $P_{1,2}$ $P_{1,3}$ $P_{1,4}$ $P_{1,f}$
$P_{2,1}$ $P_{2,2}$ $P_{2,3}$ $P_{2,4}$ $P_{2,f}$
$P_{3,1}$ $P_{3,2}$ $P_{3,3}$ $P_{3,4}$ $P_{3,f}$
$P_{4,1}$ $P_{4,2}$ $P_{4,3}$ $P_{4,4}$ $P_{4,f}$
$P_{t,1}$ $P_{t,4}$ $P_{t,f}$
$P_{t,3}$
N_T
N_F
Fingerprint Elements
# Statistics × N_P
σ σ² γ κ
N_T × N_F Samples/Patch
σ - Std Deviation
σ² - Variance
γ - Skewness
κ - Kurtosis

Fig. 3. Illustration of Gabor-based RF-DNA fingerprint generation using $N_T{\times}N_F$ two-dimensional patches extracted from the centered, normalized, magnitude-squared Gabor coefficients.

results presented in Sect. VII, the DGT is calculated by

$$G_{mk} = \sum_{n=1}^{MN_\Delta} s(n+lMN_\Delta)v^*(n-mN_\Delta)exp^{-j2\pi kn/K_G}, \quad (1)$$

where G_{mk} are Gabor coefficients, $s(n)$ is the near-transient response, $v(n)$ is a Gaussian analysis window, $m{=}1,2,\ldots,M$ for M total shifts along the time dimension, and $k{=}0,1,\ldots,K_G-1$. Selection of M, N_Δ, and K_G must result in the modulus of (MN_Δ) and K_G returning zero. For consistency with [50], [55], the DGT is calculated with $M{=}150$, $K_G{=}150$, and $N_\Delta{=}1$, which results in *oversampling* (since $K_G{>}N_\Delta$).

The RF-DNA fingerprints are extracted from the normalized, magnitude-squared Gabor coefficients. The normalization ensures that all values within the resulting TF representation range between zero and one. Figure 3 shows the RF-DNA fingerprint generation process. The normalized TF representation is subdivided into $N_P{=}50$ patches. Each patch comprises $N_T{=}15$ by $N_F{=}10$ entries and is annotated as P_{tf}, where t and f denotes a particular patch's position within the TF response. Following selection of a particular patch, it is reshaped into a $N_T{\times}N_F{=}150$ length vector and the features standard deviation (σ), variance (σ^2), skewness (γ), and kurtosis (κ) are calculated. This process is repeated for all patches, and subsequent features are appended to those calculated from previous patches. Additionally, these features are calculated for the entire normalized TF representation and added as the final four features of the RF-DNA fingerprint. Thus, each RF-DNA fingerprint comprises $N_f{=}204$ total features.

C. Feature Selection Approaches

This work investigates eight feature selection techniques: DRA, Linear Discriminant Analysis (LDA), PCA, NCA, Probability Of Error plus Average Correlation Coefficient (POEACC), Bhattacharyya Coefficient (BC), t-test, and Relief-F [31], [71]–[77]. The features that comprise an RF-DNA fingerprint are the variance, standard deviation, skewness, and kurtosis calculated from the normalized, magnitude-squared Gabor response as described in Section VI-B. Feature selection is performed for each authorized radio with the goal of maximizing the TVR while simultaneously minimizing the FVR. This goal is met by allowing both the number of retained features N_r and precisely which features are selected to vary from one authorized radio's set of RF-DNA fingerprints to another. The number of retained features, N_r, is chosen to be the fewest that results in TVR≥90% and FVR≤10%. The remainder of this section explains the feature-selection process for each of the eight selected approaches.

1) Dimensional Reduction Analysis (DRA): DRA is a feature selection approach first introduced in [31] and leveraged in [50], [55] to reduce the dimensionality of the RF-DNA fingerprints prior to radio ID verification. DRA selects the most relevant features based upon the values contained in the feature relevance vector, λ, which is generated as part of the GRLQVI classifier's training phase. At a given SNR, the relevance vector is

$$\lambda(\text{SNR}) = \left[\lambda_1, \lambda_2, \ldots, \lambda_{N_f}\right], \quad (2)$$

where $\lambda_j{\in}[0,1]$ indicates how much feature j influences the classification decision. If $\lambda_j{>}\lambda_k$, then feature j is more influential on the classification decision than is feature k. For the presented results, feature selection is performed on a per-SNR basis using the feature relevance vector corresponding to the GRLVQI classification model learned at that SNR.

2) Linear Discriminant Analysis (LDA): LDA is a linear operation that projects the N_f−dimensional RF-DNA fingerprints onto a line that results in the greatest separation of the two classes of interest. In this work, the two classes are the set of RF-DNA fingerprints corresponding to (i) the authorized radio (c_1) whose ID is to be verified and (ii) all other authorized radios (c_2) that serve as representatives of all other WiMAX radios including rogues. The RF-DNA fingerprints are projected onto the line by

$$\mathbf{F}_w = \mathbf{w}^T\mathbf{F}, \quad (3)$$

$$\mathbf{F} = \left[\mathbf{f}_1^{c_1}, \mathbf{f}_2^{c_1}, \ldots, \mathbf{f}_{N_{t,1}}^{c_1}, \ldots, \mathbf{f}_1^{c_2}, \mathbf{f}_2^{c_2}, \ldots, \mathbf{f}_{N_{t,2}}^{c_2}\right]^T_{N_\tau \times N_f}, \quad (4)$$

where $\mathbf{f}$ is an N_f−dimensional RF-DNA fingerprint belonging to class c_1 or c_2, $N_{t,i}$ is the total number of RF-DNA fingerprints in the training set of class i, $N_\tau{=}(N_{t,1}+N_{t,2})$, and the superscript T denotes transposition. The projection $\mathbf{w}$ is

$$\mathbf{w} = \mathbf{S}_w^{-1}(\mu_1 - \mu_2), \quad (5)$$

where

$$\mu_i = \frac{1}{N_{t,i}} \sum_{\mathbf{f}\in\mathbf{F}^i} \mathbf{f}, \;\; i=[1,2], \quad (6)$$

$$\mathbf{S}_w = \sum_{\mathbf{f}\in\mathbf{F}^1} (\mathbf{f}-\mu_1)(\mathbf{f}-\mu_1)^T + \sum_{\mathbf{f}\in\mathbf{F}^2} (\mathbf{f}-\mu_2)(\mathbf{f}-\mu_2)^T, \quad (7)$$

and $\mathbf{S}_w$ is the within-class scatter matrix [71].

3) Principal Component Analysis (PCA): PCA is an alternate feature space transformation that reduces dimensionality for the purpose of finding those components most useful for representing the data [71]. The PCA transformation is a series of projections that are mutually uncorrelated and ordered, from largest to smallest, in variance; thus, the principal axis is aligned along the direction associated with the largest variance [78]. The principal components are the eigenvectors of the covariance matrix as calculated by

$$\Sigma_{\bar{\mathbf{F}}} = \frac{1}{N_\tau}\bar{\mathbf{F}} \cdot \bar{\mathbf{F}}^T, \tag{8}$$

where $\bar{\mathbf{F}}$ is a matrix of shape $N_\tau \times N_f$ defined as

$$\bar{\mathbf{F}} = \mathbf{F} - \left[\mu_1^{c_1}, \mu_2^{c_1}, \ldots, \mu_{N_{t,1}}^{c_1}, \ldots, \mu_1^{c_2}, \ldots, \mu_{N_{t,2}}^{c_2}\right]^T_{N_\tau \times N_f}, \tag{9}$$

where μ_j is the mean of the j^{th} RF-DNA fingerprint and i=$[1, 2]$ [78].

We reveal the PCA model by computing the singular-value decomposition (SVD) of $\bar{\mathbf{F}}$:

$$\bar{\mathbf{F}} = \bar{U}S\bar{V}^T \tag{10}$$

where S is the diagonal matrix of shape $N_\tau \times N_f$ of the singular values σ_i of $\bar{\mathbf{F}}$ in decreasing order and the square, orthonormal matrices $\bar{U}$ $(N_\tau \times N_\tau)$ and $\bar{V}$ $(N_f \times N_f)$ together and canonically span the four fundamental subspaces of the linear operator $\bar{\mathbf{F}}$. Then,

$$\bar{\mathbf{F}} \cdot \bar{\mathbf{F}}^T = \bar{U}(SS^T)\bar{U}^T = \bar{U}S_{N_\tau \times N_\tau}\bar{U}^T \tag{11}$$

where

$$S_{N_\tau \times N_\tau} = \operatorname{diag}(\sigma_1^2, \ldots, \sigma_{N_\tau}^2) \tag{12}$$

and, $\Sigma_{\bar{\mathbf{F}}}$ becomes:

$$\Sigma_{\bar{\mathbf{F}}} = \frac{1}{N_\tau}\bar{U}S_{N_\tau \times N_\tau}\bar{U}^T, \tag{13}$$

whose eigenvalues and eigenvectors evidently are $(\sigma_i^2/N_\tau, u_i)_{i=1,\ldots,N_\tau}$, where u_i is the i^{th} column of $\bar{U}$.

Prior to ID verification, the RF-DNA fingerprints are projected into the PCA-defined space by

$$\mathbf{F}_w = \bar{\mathbf{F}} \cdot \mathbf{P}_{N_r}, \tag{14}$$

where $\mathbf{P}_{N_r}$=$(u_1, u_2, \ldots, u_{N_r})$ is a sub-matrix composed of the first N_r columns of the $\bar{U}$ matrix.

4) Neighborhood Component Analysis (NCA): NCA is a nearest-neighbor-based feature selection approach that maximizes the “Leave-One-Out” classification accuracy [79]. Let the training set of RF-DNA fingerprints and the corresponding class label c_i be defined as

$$\mathcal{F}_{N_\tau \times (N_f+1)} = \left[f_{i,r}, c_i\right], \tag{15}$$

where i=$[1, 2]$ and r=$1, 2, \ldots, N_f$. In NCA, an RF-DNA fingerprint is randomly selected from $\mathcal{F}$ and is designated as the reference $\mathbf{f}_j$. The probability that a new RF-DNA fingerprint $\mathbf{f}_i$ is assigned the same class label as $\mathbf{f}_j$ is

$$p_{ij} = \frac{k\left(d_w(\mathbf{f}_i, \mathbf{f}_j)\right)}{\sum\limits_{j=1, j\neq i}^{N_\tau} k\left(d_w(\mathbf{f}_i, \mathbf{f}_j)\right)}, \tag{16}$$

where

$$d_w\left(\mathbf{f}_i, \mathbf{f}_j\right) = \sum_{r=1}^{N_f} w_r^2 \left|f_{ir} - f_{jr}\right|, \tag{17}$$

$$\Upsilon(z) = \exp\left(-\frac{z}{\psi}\right), \tag{18}$$

Υ is the kernel function, ψ=1 is the kernel width, and w_r is the weight assigned to the r^{th} feature. The goal is to find the value of each weight w_r such that the chosen subset of RF-DNA fingerprints produces the highest nearest-neighbor classification accuracy [79]. The weight vector $\mathbf{w}$ that achieves this goal is determined by

$$\hat{\mathbf{w}} = \arg\min_w \left\{\frac{1}{N_\tau}\sum_{i=1}^{N_\tau}\sum_{j=1, j\neq i}^{N_\tau} p_{ij} l\left(c_i, c_j\right) + \lambda_R \sum_{r=1}^{N_f} w_r^2\right\}, \tag{19}$$

where

$$l\left(c_i, c_j\right) = \begin{cases} 1 & \text{if } c_i \neq c_j \\ 0 & \text{otherwise} \end{cases} \tag{20}$$

is the loss function and λ_R is the regularization parameter, which results in most of the weights in $\hat{\mathbf{w}}$ being set to zero. The RF-DNA fingerprint features associated with the N_r largest weights are retained and the remainder discarded.

5) Probability Of Error & Average Correlation Coefficient (POEACC): POEACC is the weighted sum of the Probability Of Error (POE) and Average Correlation Coefficient (ACC) feature selection techniques. The r^{th} RF-DNA fingerprint feature is ranked as

$$w_r = w_\rho \bar{\rho} + w_\alpha \alpha, \tag{21}$$

where w_ρ and w_α are weights that sum to 1 [73]. The POE values are normalized according to

$$\bar{\rho}_r = \frac{\rho_r - \rho_{\min}}{\rho_{\max} - \rho_{\min}}. \tag{22}$$

where $r = 1, \ldots, N_f$. The ACC is given by

$$\alpha_{r,q} = \left|\frac{\Sigma_{r,q}}{\sigma_r \sigma_q}\right|, \tag{23}$$

where r and q are a pair of features, $\Sigma_{r,q}$ is the covariance of the training set of RF-DNA fingerprints, and σ_r and σ_q are the standard deviations of the of the r^{th} and q^{th} selected features, respectively [80]. As with POE, the ACC is normalized prior to selection of the r^{th} feature, which ensures that w_1 and w_2 remain true measures of importance in (21).

In POEACC, the first feature selected is that which results in the smallest normalized POE (i.e., the smallest classification error). The second feature chosen is that which results in the smallest correlation value between itself and the first selected feature. The third selected feature is that which results in the smallest average correlation coefficient between itself and the first two when compared with the average correlation coefficients for all remaining features. This feature selection continues until all N_f features have been assigned a w_r value. Selection of the r^{th} feature is based upon its average correlation value with respect to those previously chosen [73]. This work uses POEACC feature selection, so values of w_1=0 and w_1=1 are neglected as they represent feature selection based only on ACC or POE, respectively.

6) Bhattacharyya Coefficient (BC): The BC facilitates feature selection by providing a measure of the amount of overlap that exists between histograms. This measure provides an indication of the relative closeness of the histograms. The BC for a given RF-DNA fingerprint feature f_r is given by

$$\mathcal{B}_r = \sum_{b=1}^{N_{\mathcal{B}}} \sqrt{P_{c_1}(b) P_{c_2}(b)}, \tag{24}$$

where $N_{\mathcal{B}}$ is the number of "bins/buckets" comprising the histograms, $P_{c_1}(b)$ is the probability of b for histogram c_1, and $P_{c_2}(b)$ is the probability of b for the histogram c_2 [71], [74]. The histogram $P_{c_1}(b)$ is constructed from the r^{th} feature of the authorized radio whose ID is to be verified, and $P_{c_2}(b)$ is constructed from the r^{th} feature associated with the RF-DNA fingerprints of the remaining authorized radios. If $\mathcal{B}_r$=0, then there is no overlap between the histograms associated with feature f_r. If $\mathcal{B}_r$=1, then the histograms overlap completely for feature f_r. For the work presented here, each RF-DNA fingerprint is comprised of N_f=204 features and a BC is calculated for each. The RF-DNA fingerprint features corresponding to the smallest BC values are kept, as they indicate the least amount of overlap between histograms, and the remainder are discarded.

7) t-Test: In this work, the Welch's t-test is calculated for each of the N_f RF-DNA fingerprint features. In the Welch's t-test, the null hypothesis is tested when the two populations have equal means but unequal variances or sample sizes [81]. As with the Student's t-test, the Welch's t-test assumes the two populations are distributed normally. This assumption makes the Welch's t-test well-suited to this work, because the number of RF-DNA fingerprints comprising the data set differs between c_1 and c_2 (there are unequal sample sizes) and because channel noise is normally distributed [75], [82]. For the Welch's t-test, the test statistic is

$$\mathbf{t} = (\mu_1 - \mu_2)\left(\frac{\sigma_1^2}{N_{t,1}} + \frac{\sigma_2^2}{N_{t,2}}\right)^{-1/2}, \tag{25}$$

where μ_i is given by (6) and σ_i is the standard deviation of the i^{th} RF-DNA fingerprint training set. For the estimated variance, the degrees of freedom v are approximated using the Welch-Satterthwaite equation given by

$$v \approx \left(\frac{\sigma_1^2}{N_{t,1}} + \frac{\sigma_2^2}{N_{t,2}}\right)^2 \left(\frac{\sigma_1^4}{v_1 N_{t,1}^2} + \frac{\sigma_2^4}{v_2 N_{t,2}^2}\right)^{-1} \tag{26}$$

where v_i=$N_{t,i} - 1$ for i=[1, 2] [76]. RF-DNA fingerprint features for which the null hypothesis is *rejected* are retained, while the rest are discarded. The retained features are ordered from the smallest to largest probability of observing a t value equal to or larger than that associated with the current value.

8) Relief-F: Relief-F extends the Relief algorithm to account for missing values, noisy data, and more than two classes [77]. It is for the first two reasons that Relief-F feature selection is used here. Relief-F uses an iterative approach to determine the quality of each RF-DNA fingerprint feature using within-feature dimension distances between the selected RF-DNA fingerprint and its N_K nearest in-class (a.k.a. *nearest hit*) and N_K out-of-class (a.k.a. *nearest miss*) neighbors [83], [84]. The weight assigned to the r^{th} feature is iteratively updated by

$$w_r = w_r' - \sum_{k=1}^{N_K} \frac{\Delta_r\left(\tilde{\mathbf{f}}, \mathbf{f}_H^k\right)}{N_\tau N_K} + \sum_{c_j \neq c_i} \sum_{k=1}^{N_K} \frac{p_{c_j}}{1 - p_{c_i}} \frac{\Delta_r\left(\tilde{\mathbf{f}}, \mathbf{f}_M^k\right)}{N_\tau N_K}, \tag{27}$$

where w_r' is the previous weight value of the r^{th} feature, $\tilde{\mathbf{f}}$ is the RF-DNA fingerprint randomly selected from the set of N_τ training fingerprints, $\mathbf{f}_H^k$ is one of the N_K nearest hits to $\tilde{\mathbf{f}}$, $\mathbf{f}_M^k$ is one of the N_K nearest misses to $\tilde{\mathbf{f}}$, p_{c_i} is the prior probability of the class to which $\tilde{\mathbf{f}}$ belongs, p_{c_j} is the prior probability of the class to which $\mathbf{f}_M^k$ belongs, and

$$\Delta_r\left(\tilde{\mathbf{f}}, \mathbf{f}_\delta^k\right) = \frac{\left|\tilde{\mathbf{f}}(r) - \mathbf{f}_\delta^k(r)\right|}{\max\left\{\tilde{\mathbf{f}}(r), \mathbf{f}_\delta^k(r)\right\} - \min\left\{\tilde{\mathbf{f}}(r), \mathbf{f}_\delta^k(r)\right\}}, \tag{28}$$

where δ=$[H, M]$ selects nearest hits and misses [85], [86]. The retained features are ordered from the largest assigned weight value w_r to the smallest.

D. Support Vector Machines (SVM)

This section briefly explains the SVM machine learning algorithm. The choice of SVM is motivated by (i) its successful use in prior, published SEI works [46], [55], and (ii) our "best" model selection approach that uses the SVM margin value and is described in Section VI-E.

In SVM, the goal is to determine the separating hyperplane with the largest margin. The larger the margin, the greater the generality of the classifier [71]. The optimal hyperplane is defined by the support vectors, which are the RF-DNA fingerprints most difficult to classify within the training set. Separation of both classes' RF-DNA fingerprints is facilitated through their non-linear mapping onto a much higher dimensional space. When sufficiently high, this mapping always facilitates separation of the two classes by a hyperplane [71].

For the non-separable case, the SVM is defined as

$$\min_{\beta, \beta_0} \frac{1}{2}||\beta||^2 + C \sum_{i=1}^{N_\tau} \xi_i, \quad \xi_i \geq 0, \tag{29}$$

$$\xi_i \geq 1 - y_i\left(\mathbf{f}_i^T \beta + \beta_0\right), \ \forall i, \tag{30}$$

where $\left(\mathbf{f}_i^T \beta + \beta_0\right)$ defines the hyperplane, $y_i \in [-1, 1]$, β is a unit vector such that half the margin is $(1/||\beta||)$, ξ_i is a "slack" variable that accounts for RF-DNA fingerprints that fall on the wrong side of the margin, and C is a "cost" parameter used to tune the function and is set to 1 for all results presented in Section VII. The primal Lagrange function is given as

$$\begin{aligned} L_P = {} & \frac{1}{2}||\beta||^2 + C \sum_{i=1}^{N_\tau} \xi_i - \sum_{i=1}^{N_\tau} \mu_i \xi_i \\ & - C \sum_{i=1}^{N_\tau} \alpha_i \left[y_i(\mathbf{f}_i^T \beta + \beta_0) - (1 - \xi_i)\right], \end{aligned} \tag{31}$$

which is minimized with respect to β, β_0, and α_i. The derivatives of (31) are set to zero to obtain

$$\beta = \sum_{i=1}^{N_\tau} \alpha_i y_i \mathbf{f}_i, \tag{32}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.3045305, IEEE Internet of Things Journal

where $\sum_{i=1}^{N_\tau} \alpha_i y_i=0$ and $\alpha_i=C-\mu_i$. Substituting (32) into (31) results in the Lagrangian dual objective function

$$L_D = \sum_{i=1}^{N_\tau} \alpha_i - \frac{1}{2} \sum_{i=1}^{N_\tau} \sum_{j=1}^{N_\tau} \alpha_i \alpha_j y_i y_j \Upsilon\left(\mathbf{f}, \mathbf{f}'\right), \tag{33}$$

where $\Upsilon\left(\mathbf{f}, \mathbf{f}'\right)$ maps the RF-DNA fingerprints into the higher dimensional space. In this work, the Radial Basis Function (RBF) is used for this non-linear mapping, which is given by

$$\Upsilon\left(\mathbf{f}, \mathbf{f}'\right) = \exp\left(-\zeta ||\mathbf{f} - \mathbf{f}'||^2\right), \tag{34}$$

where ζ is a positive constant and $\mathbf{f}$ and $\mathbf{f}'$ are two RF-DNA fingerprints [78]. The solutions to (31) and (33) are found by minimizing β, β_0, and α_i and are given by

$$\hat{\beta} = \sum_{i=1}^{N_\tau} \hat{\alpha}_i y_i \mathbf{f}_i, \tag{35}$$

where the support vectors $\hat{\beta}$ are the RF-DNA fingerprints for which $\hat{\alpha}_i \neq 0$. Support vectors on the edge of the margin have values of $0 \leq \hat{\alpha}_i \leq C$ and $\xi_i=0$. All remaining support vectors have $\hat{\alpha}_i=C$ and $\xi_i>0$. Based upon these constraints and the Karush-Kuhn-Tucker conditions in [78], the SVM decision is

$$\hat{S}\left(\mathbf{f}\right) = \text{sign}\left[\mathbf{f}\hat{\beta} + \hat{\beta}_0\right], \tag{36}$$

where "sign[$\bullet$]" assigns a -1 or 1 to an RF-DNA fingerprint based on its location with respect to the margin.

As in [53], [55], radio ID verification is implemented using a two-class classifier. One class represents the authorized radio whose ID is to be verified, while the second serves to represent all other radios including rogues. During SVM training, this second class is represented using the RF-DNA fingerprints of the remaining authorized radios.

E. SVM Model Selection

This section provides an explanation of the process developed to select the SVM model "best" suited to maximize ID verification and rogue radio rejection performance. One challenge in ID verification is the selection of a model that is well suited not only to verification of the authorized radio's ID, but also to rejection of rogue radios masquerading as the authorized radio without having access to the rogue radios' RF-DNA fingerprints during model development. The selection of the "best" SVM model—the one that achieves the highest simultaneous ID verification and rogue rejection performance—is predicated on achieving TVR≥90% for the authorized radio, whose ID is to be verified, and FVR≤10% for the remaining known radios that serve as representative rogues. Thus, if either of these two benchmarks is not satisfied for the selected SVM model, then that SVM model is removed from consideration. If there is no SVM model that satisfies this TVR requirement for a given authorized radio at a particular SNR across all N_r retained feature sets, then the SVM model that achieves the highest TVR value for that authorized radio is selected. For SVM models that satisfy the TVR≥90% requirement, the margin is calculated for all of the RF-DNA fingerprints of the authorized radio being verified and the remaining authorized radios, designated herein in as "others," across all noise realizations at the selected SNR and N_r features. The margin is calculated by

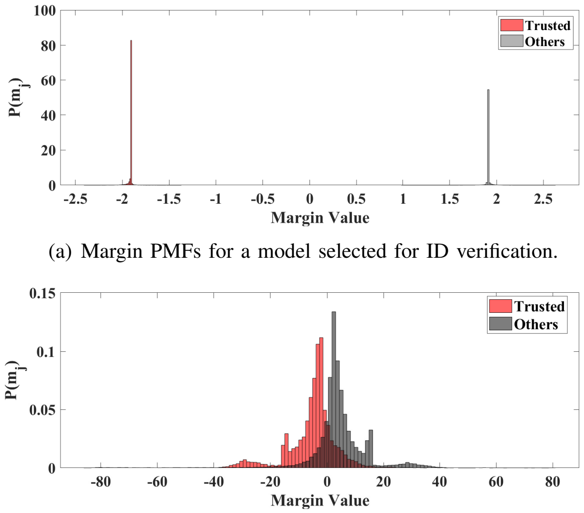
$$m = 2yf\left(\mathbf{f}_{1\times N_r}\right), \tag{37}$$

$$f\left(\mathbf{f}_{1\times N_r}\right) = \sum_{j=1}^{N_\tau} \hat{\alpha}_j y_j G\left(\hat{\beta}_j, \mathbf{f}_{1\times N_r}\right) + \hat{\beta}_0, \tag{38}$$

where $\left(\hat{\alpha}_1, \ldots, \hat{\alpha}_{N_T}, \hat{\beta}_0\right)$ are the estimated SVM parameters, $y_j \in [-1, 1]$, and $G\left(\hat{\beta}_j, \mathbf{f}_{1\times N_r}\right)$ is the dot product between the selected RF-DNA fingerprint and the support vectors [87]. Following calculation of all of the margin values, the Probability Mass Function (PMF) is generated for the positive and negative classes (authorized radios and others, respectively). The mean and variance of each PMF is calculated along with the BC value using (24). At a given SNR, the SVM model resulting in the largest distance between the PMFs' mean values as well as the smallest BC and variance values is selected as the "best" model for ID verification and rogue rejection using the prescribed set of N_r features. Figure 4 provides a representative illustration of the two margin PMFs for two different SVM models. In this case, the SVM models are generated for the same authorized radio at the same SNR, using RF-DNA fingerprints comprised of differing sets of retained features in both those selected and number. The SVM model that resulted in the PMFs shown in Fig. 4(a) would be selected for ID verification and rogue radio rejection, while the SVM model associated with Fig. 4(b) would not.

F. ID Verification Approach

As stated in Sect. VI-A, our work uses a total of N_D=18 WiMAX MS radios of the same manufacturer and model, which represents the most challenging ID verification and rogue rejection case. This is the most challenging case because the radios are manufactured using the same process and parts/components (e.g., the transceiver chipset). ID verification with rogue radio rejection assessment is facilitated by dividing



(a) Margin PMFs for a model selected for ID verification.

(b) Margin PMFs for a model *not* selected for ID verification.

Fig. 4. Representative PMFs of the margin values using two different SVM models generated for the same authorized radio and SNR (i.e., a different set of retained RF-DNA fingerprint features is used).

TABLE III
WiMAX Authorized Device Trials [50].

	Trial #		
	1	2	3
Digital ID #	MS63A7	MS637D	MSC2FF
	MS63A9	MS9993	MSDAC5
	MS66E7	MSDAB9	MSDDC7
	MS6373	MSDAC9	MSDF5B
	MS6387	MSDADB	MSDF7D
	MSD905	MSDDBF	MSDF65

the 18 radios into two sets: a set of six authorized radios and a set of 12 rogue radios. Selection of the six authorized radios was done randomly while ensuring that each radio is designated as an authorized radio once and a rogue twice. The result is three separate trials of six authorized and 12 rogue radios. The composition of each trial's authorized radios is given in Table III and is consistent with that of [50] to enable comparative assessment. For example, to verify the ID of MS63A7, in Trial #1, class one of the SVM is trained using MS63A7's RF-DNA fingerprints while class two training is done using the RF-DNA fingerprints of the remaining authorized radios: MS63A9, MS66E7, MS6373, MS6387, and MSD905. For Trial #1, the remaining 12 radios (i.e., Trial #2 and #3's authorized radios) serve as rogues attempting to gain network access by spoofing the digital ID of MS63A7. This process is repeated for each authorized radio of a given trial and across all three trials. It is important to note that the RF-DNA fingerprints associated with the rogue radios are never used for training the SVM nor selection of the "best" SVM model. They simply serve as a means by which to assess the "best" SVM model's effectiveness in detecting the rogue radios.

VII. Results

In this section, the developed an ID verification and rogue radio rejection process, which uses feature-reduced RF-DNA fingerprints and a two-class SVM, is evaluated for its effectiveness in mitigating the threat as described in Sect. III. All ID verification and rogue radio rejection results are generated using SVM models that are developed following the approach described in Sect. VI-F. For a given SNR value, an authorized radio's SVM model is developed using Monte Carlo simulation that is enabled through the use of N_z=10 independent, like-filtered Additive White Gaussian Noise (AWGN) realizations being added to every radio's near-transient responses prior to RF-DNA fingerprint generation. The SVM classifier is trained using k=5-fold cross validation and N_b=900 total N_r-dimensional RF-DNA fingerprints for each of the authorized radios; thus, class one and two are represented using 900 and 5,400 RF-DNA fingerprints, respectively. Each feature selection approach, with the exception of LDA, designates the $N_r \in [1, 200]$ top-ranked RF-DNA fingerprint features as described in Sect. VI-C1 through Sect. VI-C8. For each authorized radio, a total of $k \times N_z$=50 SVM models are generated at each value of N_r. The model that results in the smallest classification error across all Monte Carlo trials and k-fold steps is used to represent the selected authorized radio at the particular value of N_r. The authorized radio's "best" SVM model, across all values of N_r, is chosen using the procedure presented in Sect. VI-E.

A. Evaluation of the Feature Selection Approaches

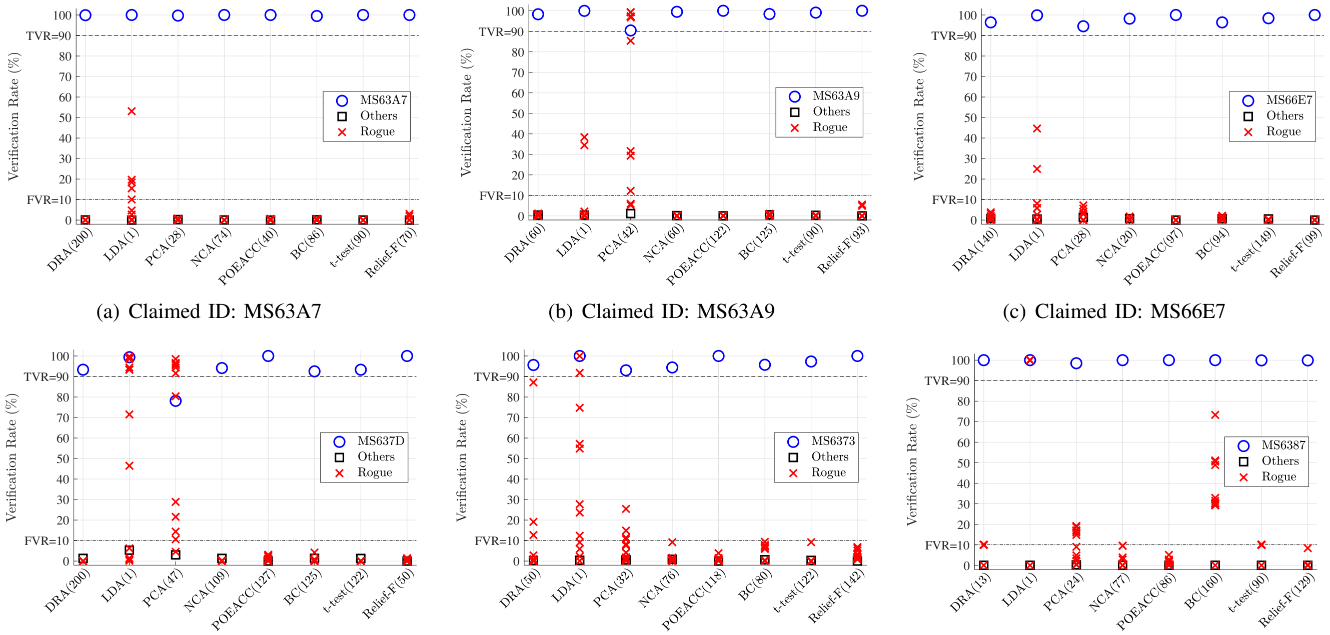
The purpose of this section is to determine the feature selection method(s) most effective in choosing the set and number of retained RF-DNA fingerprint features based on ID verification and rogue rejection performance. For the authorized radio whose ID is to be verified, the "best" ID verification performance is defined as achieving TVR$\geq$90%, while the "best" rogue rejection performance is achieving FVR$\leq$10% for all rogue radios and the remaining authorized radios (i.e., those whose IDs are *not* being verified by the selected SVM model). The feature selection method(s) that simultaneously achieve both of these conditions, for all authorized radios, is used for SNR-based analysis.

The effectiveness of each feature selection method is assessed using the authorized radios of Trial #1 at an SNR of 21 dB. Selection of this trial and SNR is motivated by the published results in [50], which presents ID verification and rogue radio rejection performance using the same set of N_f-dimensional RF-DNA fingerprints, noise realizations, as well as authorized and rogue radios.

Our results are presented in Fig. 5: the ID verification for each of the six authorized radios comprising Trial #1 at an SNR equal to 21 dB. For authorized radio MS63A7, shown in Fig. 5(a), TVR=100% is achieved using RF-DNA fingerprint features selected using all eight feature selection approaches. The other five authorized radios—MS63A9, MS66E7, MS6373, MS6387, and MSD905—are successfully rejected at FVR$<$10% using the features selected by all eight methods. The digital ID spoofing attacks by the rogue radios (i.e., those comprising Trials #2 and #3) are successfully rejected at FVR$<$10% using DCA, PCA, NCA, POEACC, BC, t-test, and Relief-F selected features. LDA-selected RF-DNA features fail to satisfy the FVR$\leq$10% requirement for five of the 12 total digital ID spoofing attacks, the worst case being a rogue radio that achieves a successful attack rate of $\sim$53% when spoofing the digital ID of MS63A7.

ID verification and rogue radio rejection results for each of the eight feature selection approaches are presented in Fig. 5(b) for the authorized radio MS63A9. The ID of MS63A9 is successfully verified at TVR$\geq$90% using the features designated by all eight selection methods. The other five authorized radios are all successfully rejected at FVR$\leq$2% regardless of the feature selection method used. For rogue radio rejection, RF-DNA fingerprints comprised of LDA- and PCA-selected features fail to achieve the required FVR$\leq$10% benchmark for all 12 rogue radio attacks. For PCA-selected features, two rogues are granted network access at rates of over 96% and as high as 99%. In this case, the two rogue radios are virtually indistinguishable from the authorized radio, MS63A9, when presenting its digital ID.

The ID verification and rogue rejection results for MS66E7 are presented in Fig. 5(c). The ID of MS66E7 is successfully



(a) Claimed ID: MS63A7

(b) Claimed ID: MS63A9

(c) Claimed ID: MS66E7

(d) Claimed ID: MS6373

(e) Claimed ID: MS6387

(f) Claimed ID: MSD905

Fig. 5. ID verification (○) and rogue rejection (×) performance for the six authorized radios of Trial #1 using all eight feature selection methods at SNR=21 dB. The number of retained features is in parentheses along the x-axis, "Others (□)" indicates the five authorized radios whose IDs are not being verified, and each red cross (×) represents a rogue radio.

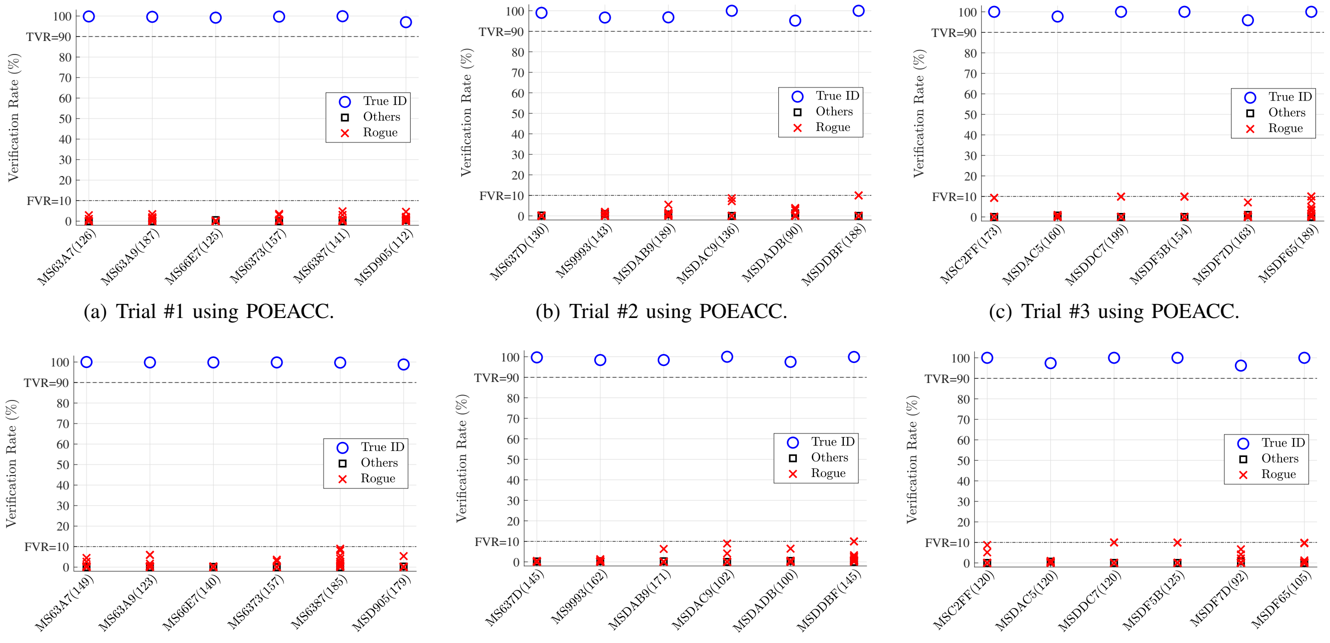
verified using RF-DNA fingerprint features selected by each of the eight methods described in Sect. VI-C. The feature-reduced RF-DNA fingerprints of the other authorized radios are successfully rejected at FVR≤3% for all eight feature selection methods. The rejection performance of the other authorized radios is important to prevent any one of them from being incorrectly verified as the authorized radio whose ID is being verified. Two of the rogue radios are falsely verified as MS66E7 at rates of 25% and 45% when the retained RF-DNA fingerprint features are chosen using LDA.

The ID verification and rogue rejection performance for authorized radio MS6373 is shown in Fig. 5(d). The ID of MS6373 is successfully verified at TVR≥90% using RF-DNA fingerprints whose features are selected using the DRA, LDA, NCA, POEACC, BC, *t*-test, and Relief-F methods. When using PCA-selected RF-DNA fingerprint features, the ID of MS6373 is verified 78% of the time. The remaining authorized radios are all successfully rejected at FVR≤7% when using any one of the eight methods to reduce RF-DNA fingerprint dimensionality. For MS6373, all 12 rogue radio attacks are successfully rejected when using DRA, NCA, POEACC, BC, *t*-test or Relief-F reduced RF-DNA fingerprints. When using LDA and PCA reduced RF-DNA fingerprints, a total of five and six rogue radios are incorrectly verified as radio MS6373 at FVR≥90%, respectively. LDA assumes that the discriminating information is contained in the class means; thus, the poorer rogue rejection performance is attributed to violation of this assumption [71]. In PCA-based feature selection, it is assumed that the principal components are (i) linear combinations of the original features comprising the RF-DNA fingerprint(s), (ii) orthogonal, and (iii) associated with the axes of highest variance [71]. If one or more of these assumptions does not hold, then PCA will fail to select a set of RF-DNA fingerprint features that facilitates separation of one or more rogue radios from the authorized radio whose ID is being verified by the developed SVM model.

MS6387 ID verification and rogue rejection performance is presented in Fig. 5(e). The ID of MS6387 is successfully verified at TVR≥90% using all eight retained RF-DNA fingerprint feature sets. FVR≤2% is achieved for the other authorized radios. However, rogue rejection using DRA-, LDA-, and PCA-selected RF-DNA fingerprint features fails to achieve the required FVR≤10% benchmark for three, eight, and four of the 12 rogue attacks, respectively. For LDA, two of the rogue radios' IDs are verified as that of MS6387 at FVR=[92, 100]%.

Figure 5(f) shows that the ID of MSD905 is verified at TVR≥98%, while the other authorized radios are correctly rejected at FVR≤1%. For rogue radios spoofing the ID of MSD905, the required FVR≤10% is achieved using the top-ranked RF-DNA fingerprint features selected using five of the eight methods (DRA, NCA, POEACC, *t*-test, and Relief-F). The worst-case rogue rejection performance is FVR=100%, which results when using LDA-selected RF-DNA fingerprint features.

Considering the ID verification results shown in Fig. 5 across the six authorized radios of Trial #1, the required TVR≥90% and FVR≤10% benchmarks are achieved using N_r-dimensional RF-DNA fingerprints whose top features are ranked using NCA, POEACC, *t*-test, and Relief-F. The remaining four feature selection methods (DRA, LDA, PCA, and BC) fail to satisfy one or both of the requisite benchmarks for at least one of the six authorized radio ID verification scenarios. The worst case occurs when using LDA-reduced RF-DNA fingerprints, which fails to achieve the rogue rejec-



(a) Trial #1 using POEACC.

(b) Trial #2 using POEACC.

(c) Trial #3 using POEACC.

(d) Trial #1 using Relief-F.

(e) Trial #2 using Relief-F.

(f) Trial #3 using Relief-F.

Fig. 6. ID verification (○) and rogue rejection (×) performance for the six authorized radios of *all* three trials using the POEACC and Relief-F feature selection methods at SNR=9 dB. The x-axis labels indicate the *claimed* digital ID with the number of retained features in parentheses, and "Others (□)" indicates the five authorized radios whose IDs are not being verified and each red cross (×) represents a rogue radio.

tion FVR≤10% requirement for all six authorized radio ID verification scenarios. LDA's poor performance is attributed to the projection itself, because it assumes that the two classes are linearly separable. If the two classes are *not* linearly separable, then LDA cannot discriminate between them [88]. In this work, the LDA projection matrix **w** is calculated using only the authorized radios' RF-DNA fingerprints; thus, providing no way of ensuring that the rogue radio's projected RF-DNA fingerprints are linearly separable from those of the authorized radios.

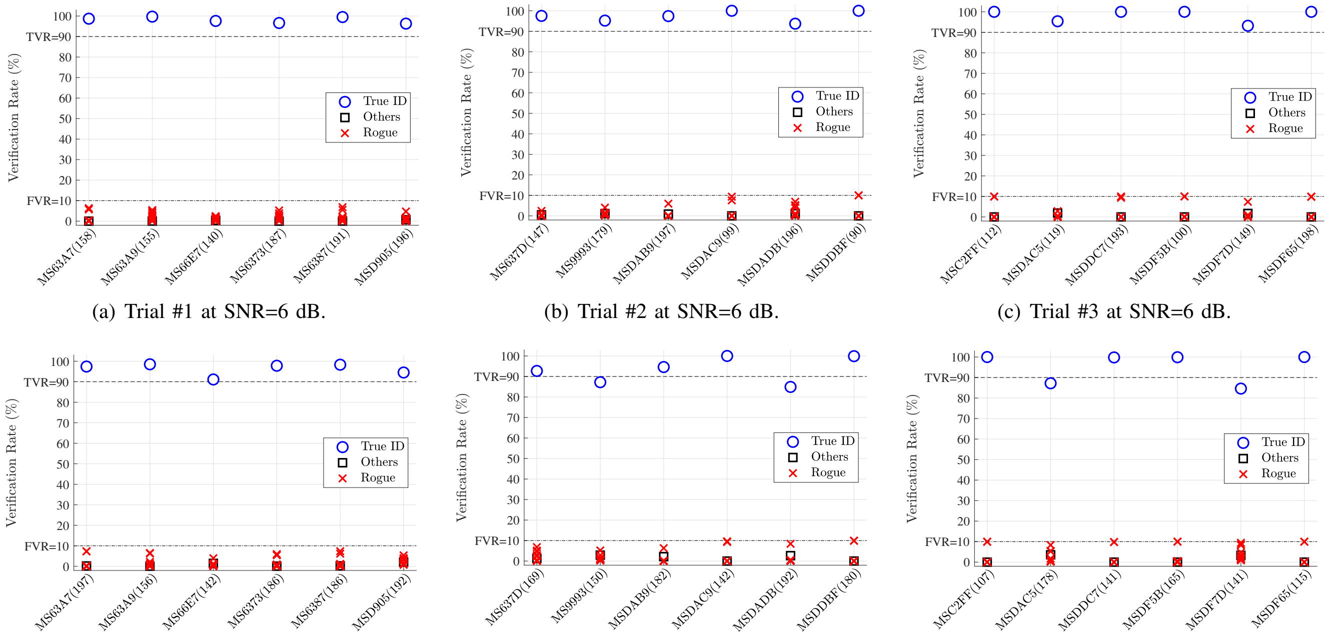
In comparison to the results in [50], the DRA results shown in Fig. 5 prove superior in that the IDs of all six Trial #1 authorized radios are verified at TVR≥90%. A total of three and four rogue radio attacks fail to be rejected at the FVR≤10% benchmark in Fig. 5 and [50], respectively. The worst-case DRA-based rogue rejection performance in Fig. 5 is 87% versus ~50% in [50].

B. Evaluation of ID verification Under Degrading SNR

Based on the results in Fig. 5, ID verification and rogue rejection performance is assessed using N_r-dimensional RF-DNA fingerprints whose top-ranked features are selected using the NCA, POEACC, *t*-test, and Relief-F feature selection methods under degrading SNR for all three trials in Table III. The set of all N_f-dimensional RF-DNA fingerprints contains SNR∈[-3, 27] dB in 3 dB steps; thus, the degrading SNR assessment is conducted in 3 dB steps starting with 18 dB. Initially, only the authorized radios of Trial #1 are used and additional trials are assessed as long as the required TVR and FVR benchmarks are satisfied for the previous trial(s). At the selected SNR, a feature selection method is removed from consideration if either TVR≥90% is not met for any of the authorized radios being verified or FVR≤10% is not satisfied for the other authorized and rogue radios for any one of the three trials. For SNR∈[12, 18] dB, all four of the chosen feature selection approaches met the TVR and FVR benchmarks for each trial's set of authorized and rogue radios.

However, at SNR=9 dB, only POEACC- and Relief-F-selected N_r RF-DNA fingerprint features achieve the TVR≥90% and FVR≤10% benchmarks for all three authorized radio trials, as shown in Fig. 6. The x-axis indicates the *claimed* digital ID with the number of retained features in parentheses. The SNR=9 dB results are presented for two reasons: (i) many digital communication standards require a received signal SNR≥10 dB for reliable demodulation performance (e.g., IEEE 802.11 Wi-Fi [60]), and (ii) the results presented in [55] are at SNR=9 dB, which permits comparative assessment. The work in [55] only assessed ID verification and rogue rejection performance for Trial #1 authorized radios. In [55], four of the six authorized radios have their ID verified at TVR≥90%. Rogue radio attacks are successfully rejected at FVR≤10% when spoofing five of the six authorized radios' digital IDs. When spoofing the ID of MSD905, the 12 rogue radios are rejected at FVR=88%, which means that the SVM struggles to differentiate a rogue radio from MSD905 when using the DRA-selected RF-DNA fingerprint features in [55].

Based upon the TVR and FVR performance results presented in Fig. 6, ID verification and rogue rejection performance continues to be assessed for SNR=[3, 6] dB. However, for these SNR values, the POEACC-selected N_r-dimensional RF-DNA fingerprints no longer satisfied the selected the TVR≥90% and FVR≤10% benchmarks. Thus, ID verification and rogue radio rejection results are only presented for N_r-dimensional RF-DNA fingerprints whose features are selected



(a) Trial #1 at SNR=6 dB.

(b) Trial #2 at SNR=6 dB.

(c) Trial #3 at SNR=6 dB.

(d) Trial #1 at SNR=3 dB.

(e) Trial #2 at SNR=3 dB.

(f) Trial #3 at SNR=3 dB.

Fig. 7. ID verification (○) and rogue rejection (×) performance for the six authorized radios of *all* three trials using Relief-F feature selection at SNR=[3, 6] dB. The x-axis labels indicate the *claimed* digital ID with the number of retained features in parentheses and "Others (□)" indicates the five authorized radios whose IDs are not being verified and each red cross (×) represents a rogue radio.

using the Relief-F technique, as shown in Fig. 7.

Results for an SNR of 6 dB are presented in Fig. 7(a), Fig. 7(b), and Fig. 7(c) for Trial #1, Trial #2, and Trial #3, respectively. For the SNR=6 dB case, the Relief-F selected N_r RF-DNA fingerprint features achieve the required TVR≥90% and FVR≤10% benchmarks for all authorized and rogue radios across all three of the trials in Table III. The lowest TVR is for MSDF7D of Trial #3 (Fig. 7(c)) with a rate of 93.2%. All other authorized radios have their IDs verified at TVR>93.2%. For each trial, a total of 72 total rogue radio spoofing attacks occur, which are all successfully defeated at a FVR≤10%.

The SNR=3 dB results are shown for Trial #1 in Fig. 7(d), Trial #2 in Fig. 7(e), and Trial #3 in Fig. 7(f). For Trial #1, the IDs of all six authorized radios are correctly verified at TVR≥90%. The lowest true verification performance occurred for radio MS66E7 at TVR=91%. All rogue radios, representing 12 spoofing attacks per authorized radio for a total of 72, are successfully rejected at FVR≤10% at SNR=3 dB. Trial #1's worst rejection performance is at FVR=7.4%, which occurs when a rogue radio spoofs the ID of the authorized radio MS6387. In terms of Trial #2 presented in Fig. 7(e), the IDs of four of the six authorized radios are verified at TVR≥90%. The two remaining radios, MS9993 and MSDADB, are verified at rates of 87.2% and 84.9%, respectively. Despite these two authorized radios not being verified at or above the selected TVR benchmark, all rogue radios are still successfully rejected within the FVR≤10% benchmark. Worst-case rogue rejection performance is FVR=9.93% when the ID of authorized radio MSDDBF is spoofed by one of the 12 rogue radios. For Trial #3 in Fig. 7(f), the TVR≥90% benchmark is achieved when verifying the ID of four out of the six authorized radios. Authorized radios MSDAC5 and MSDF7D are verified at TVR=87.2% and TVR=84.6%, respectively. Similar to Trial #2, all of the rogue radio attacks on Trial #3 authorized radios are successfully rejected within the desired FVR≤10% benchmark. Worst-case rogue rejection performance is FVR=10% when the IDs of authorized radios MSC2FF, MSDDC7, MSDF5B, and MSDF65 are spoofed by a rogue radio. When considering the results for Trial #2 and Trial #3, with respect to the threat model presented in Sect. III, the ability to successfully reject all the rogue radio attacks at the selected FVR benchmark is of greater import than verifying the IDs of all authorized radios at the selected TVR benchmark. The success of the Relief-F-selected RF-DNA fingerprint features is attributed to the algorithm's use of the N_K nearest in-class and out-of-class neighbors when determining the feature weights, which makes it more robust under degrading SNR conditions.

VIII. Conclusion

This work presents a PHY layer IoT security approach capable of defeating digital ID spoofing attacks through the use of feature-reduced RF-DNA fingerprints and an SVM classifier. A total of eight feature-selection approaches are assessed to determine the RF-DNA fingerprint features that facilitate authorized radio ID verification at TVR≥90% while simultaneously rejecting all rogue radio digital ID spoofing attacks at FVR≤10% at the lowest SNR possible. Unlike prior work that employs RF fingerprints formed using a fixed number and/or composition of features for all authorized radios, this work allows the number and composition of selected RF fingerprint features to be driven by individual authorized radio ID verification performance. Selection is driven by the distribution of the margin values generated from the SVM model and the authorized radios' N_r-dimensional RF-DNA fingerprints—that is, without knowledge of rogue radios' RF-DNA fingerprints. This work successfully demonstrates 100% correct (i) ID verification (that is, TVR≥90% across three trials of six randomly selected authorized radios at SNR≥6dB) and (ii) rejection (that is, FVR≤10% of 72 rogue radio ID spoofing attacks per authorized radio SNR≥3dB using N_r-dimensional RF-DNA fingerprints whose features are selected using the Relief-F algorithm). Such performance is absent in previous RF fingerprint-based ID verification publications.

IX. Future Research

Future work will focus on the following three activities: 1) ID verification and rogue radio rejection for networks made up of differing numbers of authorized radios and of radios that are heterogeneous in manufacturer and/or model; 2) Integration of the presented approach within a hardware platform to facilitate determination of needed resources and capabilities as well as testing and analysis of the presented approach in an operational IoT setting; and 3) Assessing the scalability of the approach under increasing numbers of authorized radios, rogue radios, or both.

References

[1] Chief Information Officer, U.S. Department of Defense, "DoD Policy Recommendations for The Internet of Things (IoT)," https://www.hsdl.org/?view&did=799676, Dec. 2016.

[2] Gartner Research, "Gartner Says 6.4 Billion Connected"Things" Will Be in Use in 2016, Up 30 Percent From 2015," Nov. 2015.

[3] Juniper Research, "'Internet of Things' Connected Devices to Triple by 2021, Reaching Over 46 Billion Units," Dec. 2016.

[4] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, 2019.

[5] Rawlinson, K., "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," Jul. 2014.

[6] Ray, I., D. Kar, J. Peterson, and S. Goeringer, "Device Identity and Trust in IoT-sphere Forsaking Cryptography," in *International Conference on Collaboration and Internet Computing (CIC)*, 2019.

[7] Neshenko, N., E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[8] Larsen, S., "A smart fish tank left a casino vulnerable to hackers," Website: https://money.cnn.com/2017/07/19/technology/fish-tank-hack-darktrace/index.html, Jul 2017.

[9] Wright, J., and J. Cache,, *Hacking Wireless Exposed: Wireless Security Secrets & Solutions*, 3rd ed. McGraw-Hill, 2015.

[10] Stanislav, M., and T. Beardsley, "Hacking IoT: A Case Study on Baby Monitoring Exposures and Vulnerabilities," *Rapid7*, 2015.

[11] Wright, J., "KillerBee: Practical ZigBee Exploitation Framework or 'Wireless Hacking and the Kinetic World'." [Online]. Available: https://www.inguardians.com/works/

[12] Simon, S., "'Internet Of Things' Hacking Attack Led To Widespread Outage Of Popular Websites," *NPR*, Oct 2016. [Online]. Available: https://www.wbur.org/npr/498954197/internet-outage-update-internet-of-things-hacking-attack-led-to-outage-of-popular.

[13] Shipley, P., "Insteon: False Security and Deceptive Documentation," *DEFCON 23*, 2014. [Online]. Available: https://www.youtube.com/watch?v=dy1LTQLmPtM

[14] ——, "Tools for Insteon RF," *GitHub*, 2015. [Online]. Available: https://github.com/evilpete/insteonrf

[15] Brook, C., "Mirai IoT Botnet Co-Authors Plead Guilty," *Digital Guardian*, 2017. [Online]. Available: https://digitalguardian.com/blog/mirai-iot-botnet-co-authors-plead-guilty/

[16] Talbot, C., M. Temple, T. Carbino, and J. Betances, "Detecting Rogue Attacks on Commercial Wireless Insteon Home Automation Systems," *Computers & Security*, vol. 74, 10 2017.

[17] Sa, K., D. Lang, C. Wang, and Y. Bai, "Specific Emitter Identification Techniques for the Internet of Things," *IEEE Access*, 2019.

[18] Toonstra J. and W. Kinsnew, "Transient Analysis and Genetic Algorithms for Classification," in *IEEE Conf on Communications, Power & Computing*, May 1995.

[19] Ureten O. and N. Serinken, "Detection of Radio Transmitter Turn-On Transients," *IEE Electronics Letters*, vol. 35, no. 23, Nov 1999.

[20] Dudczyk J., J. Matuszewski and M. Wnuk, "Applying the Radiated Emission to the Specific Emitter Identification," in *15th International Conference on Microwaves, Radar & Wireless Communications (IEEE Cat. No.04EX824)*, vol. 2, 2004, pp. 431–434 Vol.2.

[21] Jeffrey, P., G. Ben, G. Ramakrishna, S. Srinivasan and W. David, "802.11 User Fingerprinting," in *ACM Int'l Conf on Mobile Computing & Networking*, Jun 2013.

[22] Jana, S. and S. Kasera, "On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews," in *ACM Int'l Conf on Mobile Computing & Networking*, Sep 2008.

[23] Brik, V., S. Banerjee, M. Gruteserand S. Oh, "Wireless Device Identification with Radiometric Signatures," in *ACM Int'l Conf on Mobile Computing & Networking*, Sep 2008.

[24] Suski W. II, M. Temple, M. Mendenhall and R. Mills, "RF Fingerprinting Commercial Communication Devices to Enhance Electronic Security," *Int'l J. Electronic Security & Digital Forensics*, vol. 1, no. 3, Oct. 2008.

[25] Danev B. and S. Kapkun, "Transient-Based Identification of Wireless Sensor Nodes," in *ACM Int'l Conf on Info Processing in Sensor Networks*, Apr 2009.

[26] Klein R., M. Temple, M. Mendenfhall and D. Reising, "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance," in *IEEE Int'l Conf on Communications*, Jun 2009.

[27] Liu, M. and J. Doherty, "Nonlinearity Estimation for Specific Emitter Identification in Multipath Environment," in *IEEE Sarnoff Symp*, Mar 2009.

[28] ——, "Nonlinearity Estimation for Specific Emitter Identification in Multipath Channels," *IEEE Trans on Info Forensics & Security*, vol. 6, no. 3, Sep 2011.

[29] Kennedy, I. and A. Kuzminskiy, "RF Fingerprint Detection in a Wireless Multipath Channel," in *Int'l Symp on Wireless Comm Systems*, Sep 2010.

[30] Reising, D., M. Temple,and M. Mendenhall, "Improved wireless security for GMSK-based devices using RF fingerprinting," *Int. J. Electron. Secur. Digit. Forensic*, vol. 3, no. 1, Mar 2010.

[31] Reising, D., "Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing," Ph.D. dissertation, Air Force Institute of Technology, Dec. 2012.

[32] Williams M., S. Munns, M. Temple and M. Mendenhall, "RF-DNA Fingerprinting for Airport WiMax Communications Security," in *Int'l Conf on Net & Sys Security*, Sep 2010.

[33] Takahashi, D., Y. Xiaoa, Y. Zhang, P. Chatzimisios, and H. Chend, "IEEE 802.11 User Fingerprinting and its Applications for Intrusion Detection," *Computers & Math with Applications*, vol. 60, no. 2, Jul 2010.

[34] Tekbas, O., O. Ureten and N. Serinken, "Improvement of Transmitter Identification System for Low SNR Transients," *IEE Electronics Letters*, vol. 40, no. 3, Jul 2004.

[35] Ellis K. and N. Serinken, "Characteristics of Radio Transmitter Fingerprints," *Radio Science*, vol. 36, no. 4, 2001.

[36] Soliman, S. and S-Z. Hsue, "Signal Classification Using Statistical Moments," *IEEE Trans on Communications*, vol. 40, no. 5, 1992 1992.

[37] Defence R&D Canada - Ottawa, "Interferometric Intrapulse Radar Receiver for Specific Emitter Identification and Direction-Finding," *Fact Sheet REW 224*, Jun 2007.

[38] Azzouz E. and A. Nandi, *Automatic Modulation Recognition of Communication Signals*. Kluwer Academic Publishers, 1996.

[39] Wheeler C. and D. Reising, "Assessment of the impact of CFO on RF-DNA fingerprint classification performance," in *Int'l Conf on Computing, Networking & Communications*, Jan 2017.

[40] Jafari, H., O. Omotere, D. Adesina, H-H. Wu, and L. Qian, "IoT Devices Fingerprinting using Deep Learning," in *IEEE Military Comm Conf (MILCOM)*, Oct 2018.

[41] Pan, Y., S. Yang, H. Peng, T. Li and W. Wang, "Specific Emitter Identification Based on Deep Residual Networks," *IEEE Access*, vol. 7, 2019.

[42] Köse, M., S. Taşcioğlu and Z. Telatar, "RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum," *IEEE Access*, vol. 7, 2019.

[43] Fadul M., D. Reising, D. Loveless and A. Ofoli, "RF-DNA Fingerprint Classification of OFDM Signals Using a Rayleigh Fading Channel Model," in *IEEE Wireless Communications and Networking Conf (WCNC)*, April 2019.

[44] Tian, Q., Y. Lin, X. Guo, J. Wen, Y. Fang, J. Rodriguez, and S. Mumtaz, "New Security Mechanisms of High-Reliability IoT Communication Based on Radio Frequency Fingerprint," *IEEE IoT Journal*, 2019.

[45] Wilson, A., D. Reising, and T. Loveless, "Integration of Matched Filtering within the RF-DNA Fingerprinting Process," in *IEEE Global Telecommunications Conf (GLOBECOM)*, Jul 2019.

[46] Kroon, B., S. Bergin, I. Kennedy, and G. O'Mahony Zamora, "Steady State RF Fingerprinting for Identity Verification: One Class Classifier versus Customized Ensemble," in *A.I. & Cognitive Science*, 2010.

[47] Cobb W., E. Laspe, R. Baldwin, M. Temple and Y. Kim, "Intrinsic Physical Layer Authentication of ICs," *IEEE Trans on Information Forensics and Security*, vol. 2, no. 4, p. 7, Dec 2011.

[48] Dubendorfer C., B. Ramsey and M. Temple, "An RF-DNA Verification Process for ZigBee Networks," in *Proc of 2012 IEEE Military Comm Conf (MILCOM12)*, Oct 2012.

[49] Rehman, S., K. Sowerby, and C. Coghill, "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *Journal of Computer and System Sciences*, vol. 80, p. 591–601, 05 2014.

[50] Reising D., M. Temple and J. Jackson, "Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints," *IEEE Trans on Info Forensics & Security*, vol. 10, no. 6, Jun 2015.

[51] Patel, H., M. Temple, and R. Baldwin, "Improving ZigBee Device Network Authentication Using Ensemble Decision Tree Classifiers With Radio Frequency Distinct Native Attribute Fingerprinting," *IEEE Trans on Reliability*, vol. 64, no. 1, March 2015.

[52] Baldini, G., R. Giuliani,and G. Steri, "Physical Layer Authentication and Identification of Wireless Devices Using the Synchrosqueezing Transform," *Applied Sciences*, vol. 8, p. 2167, 11 2018.

[53] Merchant, K., S. Revay, G. Stantchev, and B. Nousain, "Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks," *IEEE J. of Selected Topics in Signal Processing*, vol. 12, no. 1, Feb 2018.

[54] Andrews, S., R. Gerdes, and M. Li, "Crowdsourced Measurements for Device Fingerprinting," in *ACM Conf on Security and Privacy in Wireless and Mobile Network (WiSec)*, May 2019.

[55] Kandah, F., J. Cancelleri, D. Reising, A. Altarawneh, and A. Skjellum, "A Hardware-Software Co-design Approach to Identity, Trust, and Resilience for IoT/CPS at Scale," in *International Conference on Internet of Things (iThings)*, July 2019.

[56] Peng, L., A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, "Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme," *IEEE Internet of Things Journal*, vol. 6, no. 1, Feb 2019.

[57] Wang, X., P. Hao, and L. Hanzo, "Physical-Layer Authentication for Wireless Security Enhancement: Current Challenges and Future Developments," *IEEE Communications Magazine*, vol. 54, Jun 2016.

[58] Xu, Q., R. Zheng, W. Saad, and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, 2016.

[59] Tse, D. and P. Viswanath, *Digital Communications*, 1st ed., F. of Wireless Communication, Ed. Cambridge University Press, 2005.

[60] *IEEE Std 802.11-2007, Local and Metropolitan Area Networks, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE, Jun 2007.

[61] *IEEE Std 802.16-2009, Local and Metropolitan Area Networks, Part 16: Air Interface for Broadband Wireless Access Systems*, IEEE, May 2009.

[62] *IEEE Std 802.16e-2005, Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access System*, IEEE, Feb 2006.

[63] *IEEE 802.15.4 Standard, Wireless MAC and PHY Specifications for Low-Rate WPANS*, IEEE, Jun 2006.

[64] *Bluetooth Core Specification Version 5.2*, Core Specification Working Group, Dec 2019.

[65] Williams, M., M. Temple, and D. Reising, "Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting," in *IEEE Global Telecommunications Conf (GLOBECOM)*, 2010.

[66] Xie, T., G. Tu, C. Li, and C. Peng, "How Can IoT Services Pose New Security Threats In Operational Cellular Networks?" *IEEE Transactions on Mobile Computing*, 2020.

[67] Clancy, T. C. and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," in *International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, 2008.

[68] Tian, Q., Y. Lin, X. Guo, J. Wang, O. AlFarraj, and A. Tolba, "An Identity Authentication Method of a MIoT Device Based on Radio Frequency Fingerprint Technology," *Sensors*, vol. 20, no. 4, Feb 2020.

[69] "Agilent E3238 Signal Intercept and Collection Solutions," 2004.

[70] Bastiaans, M. J., "Discrete Gabor Transform and Discrete Zak Transform," in *IEEE Int'l Conf on Signal & Image Proc Applications*, 1996.

[71] Duda R., P. Hart and D. Stork, *Pattern Classification*, 2nd ed. John Wiley & Sons, Inc., 2001.

[72] Yang, W., K. Wang, and W. Zuo, "Neighborhood Component Feature Selection for High-Dimensional Data," *Journal of Computers (JCP)*, vol. 7, 2012.

[73] Mucciardi, A. N. and E. E. Gose, "A Comparison of Seven Techniques for Choosing Subsets of Pattern Recognition Properties," *IEEE Trans on Computers*, vol. C-20, no. 9, pp. 1023–1031, 1971.

[74] Comaniciu, D., V. Ramesh, and P. Meer, "Real-Time Tracking of Non-Rigid Objects using Mean Shift," in *Proceedings IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, vol. 2, June 2000.

[75] Derrick, B. and P. White, "Why Welch's Test is Type I Error Robust," *The Quantitative Methods for Psychology (TQMP)*, vol. 12, no. 1, 2016.

[76] Allwood, M., "The Satterthwaite Formula for Degrees of Freedom in the Two-Sample t-Test," *AP Statistics*, 2008. [Online]. Available: http://apcentral.collegeboard.com/apc/public/repository/ap05_stats_allwood_fin4prod.pdf

[77] Kononenko, I., "Estimating Attributes: Analysis and Extensions of RELIEF," in *European Conference on Machine Learning: ECML-94*, 1994.

[78] Hastie T., R. Tibshirani and J. Friedman, *The Elements of Statistical Learning; Data Mining, Inference, and Prediction*. Springer-Verlag, New York, New York, USA, 2001.

[79] Yang, W., K. Wang, and W. Zuo, "Neighborhood Component Feature Selection for High-Dimensional Data," *J. of Computers*, vol. 7, 2012.

[80] González J. A., "Numerical Analysis for Relevant Features in Intrusion Detection (NARFid)," Master's thesis, Air Force Institute of Technology, 2950 Hobson Way, WPAFB, OH, March 2009.

[81] Welch, B., "The Generalization of 'Student's' Problem when Several Different Population Variances are Involved," *Biometrika*, vol. 34, no. 1/2, 1947. [Online]. Available: http://www.jstor.org/stable/2332510

[82] Ruxton, G., "The Unequal Variance t-test is an Underused Alternative to Student's t-test and the Mann–Whitney U test," *Behavioral Ecology*, vol. 17, no. 4, May 2006.

[83] Kira, K. and L. A. Rendell, "The Feature Selection Problem: Traditional Methods and a New Algorithm," in *Proceedings of the Tenth National Conference on Artificial Intelligence AAAI*, 1992.

[84] Kira, K. and L. Rendell, "A Practical Approach to Feature Selection," in *Proceedings of the Ninth International Workshop on Machine Learning*, 1992, p. 249–256.

[85] Durgabai, R. and Y. RaviBhushan, "Feature Selection using ReliefF Algorithm," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 10, pp. 8215–8218, 2014.

[86] Stief, A., J. Ottewill, and J. Baranowski, "Relief F-Based Feature Ranking and Feature Selection for Monitoring Induction Motors," in *International Conference on Methods Models in Automation Robotics (MMAR)*, Aug 2018.

[87] Christianini, N., and J. Shawe-Taylor, *An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods*. Cambridge, UK: Cambridge University Press, 2000.

[88] Tharwat, A., T. Gaber, A. Ibrahim, and A. Hassanien, "Linear discriminant analysis: A detailed tutorial," *A.I. Comms*, vol. 30, May 2017.