

Gabor-Based RF-DNA Fingerprinting for Classifying 802.16e WiMAX Mobile Subscribers

Donald R. Reising, Michael A. Temple and Mark E. Oxley
US Air Force Institute of Technology
Wright-Patterson AFB, OH 45433 USA
Email: michael.temple@afit.edu

Abstract—Previous work has demonstrated the viability of using RF-DNA fingerprinting to provide serial number discrimination of IEEE 802.11a WiFi devices as a means to augment conventional bit-level security. This was done using RF-DNA extracted from signal regions containing standard pre-defined responses (preamble, midamble, etc.). Using these responses, proof-of-concept demonstrations with RF-DNA fingerprinting have shown some effectiveness for providing serial number discrimination. The discrimination challenge increases considerably when pre-defined signal responses are not present. This challenge is addressed here using experimentally collected IEEE 802.16e WiMAX signals from Alvarion BreezeMAX Mobile Subscriber (MS) devices. Relative to previous Time Domain (TD) and Spectral Domain (SD) fingerprint features, joint time-frequency Gabor (GT) and Gabor-Wigner (GWT) Transform features are considered here as a means to extract greater device discriminating information. For comparison, RF-DNA is extracted from TD, SD, GT, and GWT responses and MDA/ML feature extraction and classification performed. Preliminary assessment shows that Gabor-based RF-DNA fingerprinting is much more effective than either TD or SD methods. GT RF-DNA fingerprinting achieves individual WiMAX MS device classification of 98.5% or better for $SNR \geq -3$ dB.

I. INTRODUCTION

Work continues on exploiting Physical (PHY) layer attributes of the Open System Interconnection (OSI) model to augment bit-level security. The goal is to reduce or eliminate unauthorized network access while assuring access for authorized users [1]–[7]. The authors here are pursuing a better understanding of inherent PHY layer benefits provided through Radio Frequency “Distinct Native Attribute” (RF-DNA) Fingerprinting. Specifically, work in [4]–[7] has successfully used RF-DNA from selected portions of modulated signal responses to achieve serial number discrimination.

Exploitable RF-DNA attributes are 1) “native” from the time of manufacture and vary according to hardware implementation, component type, manufacturing processes, etc., and 2) sufficiently “distinct” to enable reliable cross-device discrimination. Ideally, RF-DNA is only a function of unintended “coloration” in modulated signal responses and when extracted, it can be processed to provide reliable device discrimination. Such processing generally involves feature selection, model generation, and device classification. To enable qualitative comparative assessment of improvements gained by introducing Gabor RF-DNA features, work here is based on Multiple Discriminant Analysis (MDA) feature selection with Maximum Likelihood (ML) classification [4]–[7].

The motivation for considering Worldwide Interoperability for Microwave Access (WiMAX) signals is provided by 1) the continued proliferation of IEEE 802.16e last mile communications, to include Long Term Evolution (LTE), and 2) potential adoption of an IEEE 802.16e compliant solution for next generation airport communication services as being pursued by the FAA, Eurocontrol and International Civilian Aviation Organization (ICAO) [8], [9]. WiMAX architectures are based on Wireless Access Points (WAP) that are among the top 10 IT threats [10] and unauthorized access to public safety services is a major concern [9]. The goal here is to develop RF-DNA techniques that are generally adaptable to the class of Orthogonal Frequency Division Multiplexed (OFDM) signals versus being limited to a given system implementation.

The methodology here is consistent with [4]–[7], [11] which extracted RF-DNA from near-transient (e.g., 802.11a preamble) and non-transient (e.g., GSM midamble) signal regions for RF-DNA fingerprinting. These regions contain “pre-defined” standard responses that are commonly used for device synchronization, channel estimation, network timing, etc. Ideally, these standard responses would be *identical* for all devices and would not include the unintentional coloration that produces RF-DNA uniqueness. The work reported here progresses toward signal regions that *do not* contain pre-defined responses.

The need to consider signal regions void of pre-defined standard responses was driven by empirical assessment using an Alvarion BreezeMAX Extreme 5000 system. As implemented, the Downlink (DL) Base Transceiver Station (BTS) signal includes a distinct preamble response while the Uplink (UL) Mobile Subscriber (MS) signals do not. Thus, the challenge with classifying BreezeMAX BTS devices is consistent with results reported in [12]. However, the challenge is greatly increased when considering the MS signals which do not contain a preamble or midamble response (consistent with the 802.16e standard [13], [14]). Common options for increasing classification performance include 1) finding a feature space that provides greater discrimination using a given classifier, 2) finding a more powerful classification engine for a given feature space, or 3) some combination thereof. As a first step, the authors here are considering an alternate feature space involving joint Time-Frequency (T-F) signal responses.

Benefits for using joint T-F features with RF-DNA fingerprinting were demonstrated in [4], [5] using a Dual-Tree Com-

plex Wavelet Transform (DT-CWT). In these works, statistical RF-DNA was extracted from complex DT-CWT responses of OFDM-based 802.11a preambles. The T-F resolution trade-off of the DT-CWT (increasing time resolution decreases frequency resolution and visa-versa) is potentially limiting. Given this T-F trade-off is not present with the Gabor (GT) and Gabor-Wigner (GWT) Transforms, this work investigates their use as an alternate feature space for RF-DNA fingerprint generation. While both the GT and GWT transforms provide T-F localization, the GWT combines the advantages of the GT (lack of cross-terms) with that of the Wigner-Ville Distribution (higher clarity/resolution) [15].

The remainder of this paper is arranged as follows: Sect. II provides an overview of the Alvarion BreezeMAX system used for demonstration; Sect. III provides the Demonstration Methodology, to include a description of Signal Collection and Detection, RF-DNA Fingerprinting, and MDA/ML Processing. Device Classification Results are presented in Sect. IV followed by a Conclusion in Sect. V.

II. WIMAX DEMONSTRATION SYSTEM

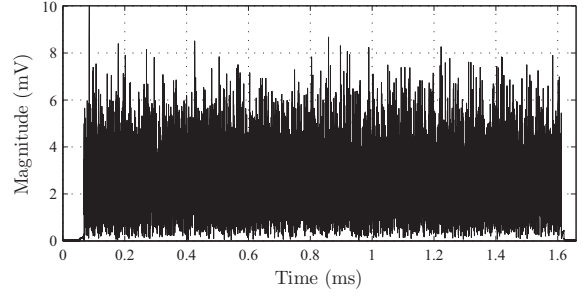
Alvarion BreezeMax Extreme 5000 equipment was used for demonstration [16]. The system uses 60/40 Time Division Duplexing (TDD) with the first 60% of each $T_F = 5 \text{ mSec}$ TDD frame allotted for BTS DL transmission and the remaining 40% allotted for MS UL transmission. An RF channel bandwidth of $W_{ch} = 5 \text{ MHz}$ centered at $f_c = 5475 \text{ MHz}$ was used for demonstration. Figure 1 shows experimentally observed UL sub-frame responses (preceding DL sub-frame responses not shown), designated herein as *Data Only*, *Range-Plus-Data*, and *Range Only* responses—designations that were neither confirmed with Alvarion nor readily apparent in documentation. All subsequent discussion and results in Sect. IV are based on MS *Ranging Only* operation.

Unlike previous GSM and 802.11 signals that have been considered [4]–[7], [11], the BreezeMAX Extreme MS signals lack a distinct region where identical modulation occurs across all devices. However, as most observable in Fig. 1(c) and expanded upon in Fig. 2, all responses contain a constant bias that spans the UL sub-frame. This was observed for all devices tested and believed to be incorporated by design to stabilize electronic component response and mitigate adverse peak-to-average power ratio effects that commonly occur with OFDM. The “near-transient” MS response in Fig. 2 (≈ 2.0 to $16.0 \mu\text{Sec}$) has thus far yielded the most useful RF-DNA and is used exclusively for all results presented in this paper.

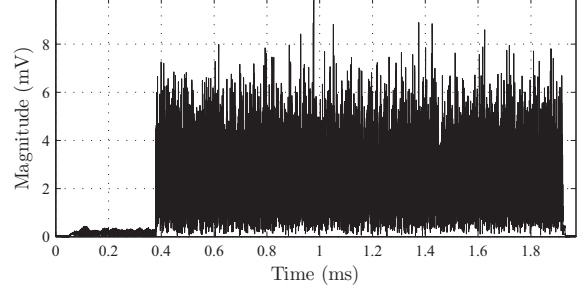
III. DEMONSTRATION METHODOLOGY

A. Signal Collection & Detection

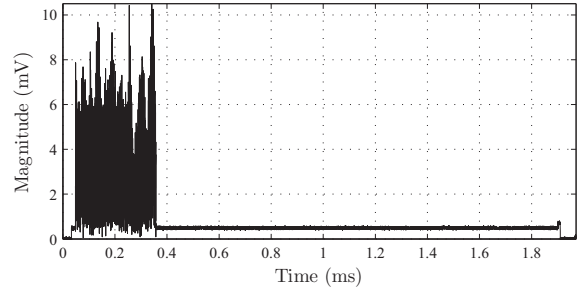
The signal collection and post-collection process in [6] was adopted for this work. All signal collections were made using the Agilent E3238S-based RF Signal Intercept and Collection System (RFSICS) that is tunable across $f_{RF} \in [0.02, 6.0] \text{ GHz}$ with a $W_{RF} = 36.0 \text{ MHz}$ RF filter [17]. The selected frequency band is down-converted to a $f_{IF} = 70 \text{ MHz}$ intermediate frequency (IF) and digitized by a $b =$



(a) MS *Data Only* Sub-Frame Response.



(b) MS *Range-Plus-Data* Sub-Frame Response.



(c) MS *Range Only* Sub-Frame Response.

Fig. 1. Magnitude plots for three distinct UL sub-frame responses observed during experimental collection of BreezeMAX 802.16e WiMAX Mobile Subscriber (MS) signals—designated herein as “modes” to facilitate discussion.

12 bit analog-to-digital converter operating at $f_s = 95 \text{ mega-samples-per-second (Msps)}$. The IF signal is down-converted, digitally filtered using a $W_{BB} = 9.28 \text{ MHz}$ filter, sub-sampled (Nyquist satisfied), and stored as complex In-phase (I) and Quadrature (Q) data. The WiMAX MS devices and

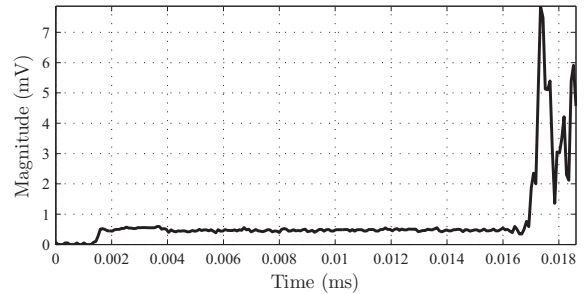


Fig. 2. “Near-transient” region of *Range Only* magnitude response in Fig. 1(c) showing pre-OFDM bias.

RFSICS were co-located in a typical office environment during collection. Collections were made using $N_{MS} = 6$ MS devices operating in *Ranging Only* mode with subsequent burst detection performed using the process in [4], i.e., the start of near-transient responses was located using amplitude-based variance trajectory (VT) at the collected SNR .

B. Time Domain (TD) RF-DNA Fingerprinting

For Time Domain (TD) fingerprinting, RF-DNA is generated from sequences representing the signal's instantaneous amplitude, phase, and frequency responses. Results in Sect. IV are based on TD fingerprints (\mathbf{F}_{TD}) generated from $N_s = 150$ near-transient samples of signal $s(n) = I(n) + jQ(n)$. For consistency with [6], [7], \mathbf{F}_{TD} is generated from the centered (subscript c) and normalized (over bar) amplitude $\{\bar{a}_c(n)\}$, phase $\{\bar{\phi}_c(n)\}$ and frequency $\{\bar{f}_c(n)\}$ sequences. Each TD sequence is centered and normalized through subtraction of the mean, calculated across N_s samples, and then divided by the maximum value of the centered sequence.

The \mathbf{F}_{TD} fingerprint is generated by dividing each of the TD sequences into $N_R = 5$ equal length, sequential subregions using the process in [12]. Features are generated by calculating statistics, standard deviation (σ), variance (σ^2), skewness (γ) and kurtosis (κ), over each of the N_R subregions as well as the $N_R + 1$ subregion. Where the $N_R + 1$ subregion consists of the full length of a TD sequence. The calculated statistics, for each of the selected subregions, are arranged as follows:

$$F_{R_i} = [\sigma_{R_i}, \sigma_{R_i}^2, \gamma_{R_i}, \kappa_{R_i}]_{1 \times 4}, \quad (1)$$

where $i = 1, 2, \dots, N_R + 1$. The composite fingerprint for a given TD sequence is formed by concatenating F_{R_i} from (1) for all regions and is given by [12],

$$\mathbf{F}^\delta = \left[\mathbf{F}_{R_1} : \mathbf{F}_{R_2} : \mathbf{F}_{R_3} \cdots \mathbf{F}_{R_{N_R+1}} \right]_{1 \times 4(N_R+1)}, \quad (2)$$

where the superscript δ denotes a specific TD sequence, i.e., $\{\bar{a}_c(n)\}$, $\{\bar{\phi}_c(n)\}$ and $\{\bar{f}_c(n)\}$. When multiple TD sequences are used for RF-DNA fingerprinting (typical case), the \mathbf{F}^δ from (2) are concatenated to form the final TD fingerprint:

$$\mathbf{F}_{TD} = \left[\mathbf{F}^a : \mathbf{F}^\phi : \mathbf{F}^f \right]_{1 \times 4(N_R+1) \times 3}. \quad (3)$$

For TD classification results in Sect. IV, $N_R = 5$ TD subregions are used and the resultant \mathbf{F}_{TD} contains a total of 72 elements (3 Features \times 4 Statistics \times 6 Subregions).

C. Spectral Domain (SD) RF-DNA Fingerprinting

For Spectral Domain (SD) fingerprinting, RF-DNA is generated per the process introduced in [12] to create SD RF-DNA Fingerprints (\mathbf{F}_{SD}). The SD fingerprints are generated from the power-normalized, Power Spectral Density (PSD) of the near-transient sample sequence $\{s(n)\}$. Given N_s near-transient samples, the desired PSD sequence $\{\bar{p}(k)\}$ is calculated via a Discrete Fourier Transform (DFT) as follows [18],

$$S(k) = \frac{1}{N_s} \sum_{n=1}^{N_s} s(n) e^{-j\Phi(N_s, n, k)}, \quad (4)$$

$$\Phi(N_s, n, k) = \left(\frac{2\pi}{N_s} \right) (n-1)(k-1). \quad (5)$$

The desired PSD sequence $\{\bar{p}(k)\}$ is obtained by dividing (4) by the signal's average power,

$$\bar{p}(k) = \frac{1}{P_s} |S(k)|^2, \quad (6)$$

where P_s is given by,

$$P_s = \frac{1}{N_s} \sum_{n=1}^{N_s} s(n)s(n)^*, \quad (7)$$

and $*$ denotes complex conjugate. The PSD is normalized to reduce potential biasing affects due to the collection process. For consistency with [3], [12], the DC term ($k=0$) and redundant ($N_s/2 + 1, N_s/2 + 2, \dots, N_s$) terms are removed prior to SD RF-DNA fingerprint generation. Consistent with the TD process in Sect. III-B, statistics are calculated over distinct PSD regions, i.e., over contiguous sub-sequences within $\{\bar{p}(k)\}$. Elements of the final \mathbf{F}_{SD} fingerprint are formed according to (1). For SD classification results in Sect. IV, $N_R=5$ SD subregions are used and the resultant \mathbf{F}_{SD} contains a total of 24 elements (4 Statistics \times 6 Subregions).

D. Gabor-Based RF-DNA Fingerprinting

Previous work in [4]–[7], [12] used RF-DNA extracted independently from either time or frequency domain responses. In related applications improvement has been realized by exploiting momentary and/or time localized signal energy as a function of frequency [19]. This can be done using Time-Frequency (T-F) localization whereby signal behavior is captured and can be displayed across a T-F plane. The Discrete Gabor Transform (DGT) provides one method for T-F localization and is given by [19],

$$G_{mk} = \sum_{n=1}^{MN_\Delta} s(n) W^*(n - mN_\Delta) \exp^{-j2\pi kn/K_G}, \quad (8)$$

where G_{mk} are the Gabor coefficients, $s(n) = s(n + lMN_\Delta)$ is the periodic input signal, $W(n) = W(n + lMN_\Delta)$ is the periodic analysis window, N_Δ is the number of samples shifted, $m = 1, 2, \dots, M$ for M total shifts, and $k = 0, 1, \dots, K_G - 1$ for $K_G \geq N_\Delta$ and $\text{mod}(MN_\Delta, K_G) = 0$ satisfied. Transformation with $K_G = N_\Delta$ represents *critical sampling* and $K_G > N_\Delta$ represents *oversampling* [19], [20], with some amount of oversampling desirable when processing noisy data [21], [22]. For convenience, the *oversampling factor* is defined here as $N_{OS} \equiv K_G/N_\Delta$. Given that the near-transient responses of *Range Only* bursts being considered here are noisy, oversampled GT processing is appropriate and enables reliable analysis with varying SNR.

In [15], the GT is combined with the Wigner-Ville Distribution (WVD) to form the Gabor-Wigner Transform (GWT). The GWT takes advantage of the GT's lack of cross-terms and faster computation as well as the higher clarity of the WVD. In this work the GWT is implemented as [15],

$$GWT_{mk} = G_{mk}^{2.6} WVD_{mk}^{0.6}. \quad (9)$$

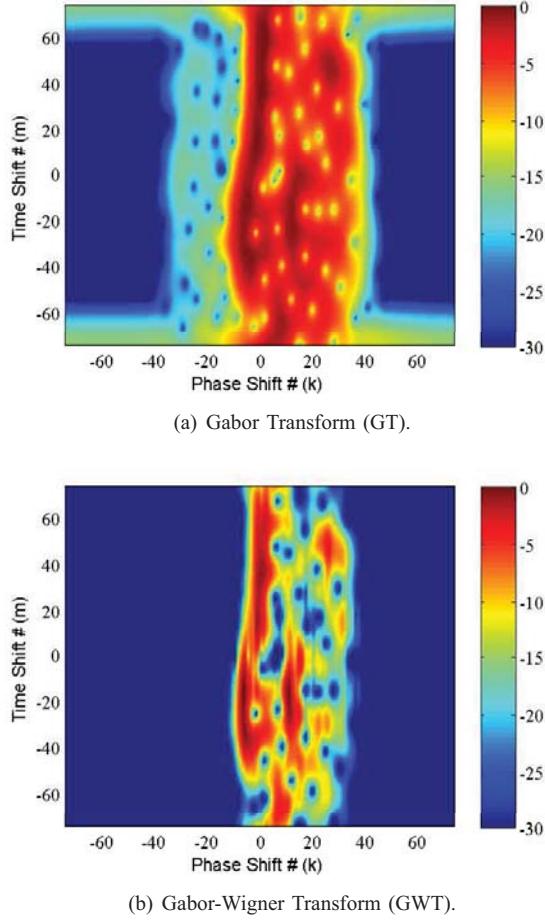


Fig. 3. Representative Gabor-based T-F magnitude responses for a 802.16e WiMAX MS device. Responses based on near-transient responses of bursts collected during *Range Only Mode* at $SNR = 0$ dB.

The WVD in (9) is actually implemented using the Discrete Pseudo Wigner Distribution (DPWD) here [23] and calculated as follows:

$$WVD_{mk} = \sum_{n=-(K_G/2-1)}^{K_G/2-1} a(n) \exp^{-j2\pi kn/K_G}, \quad (10)$$

$$a(n) = w(n)w^*(n)s(m+n)s^*(m-n), \quad (11)$$

where $w(n)$ is a specific window function. Consistent with [23], a Hamming window function was implemented.

The complex $I-Q$ components of Gabor coefficients G_{mk} and GWT_{mk} , generated respectively in (8) and (9), can be used to compute corresponding T-F magnitude and phase responses. Figure 3 shows representative magnitude responses, at $SNR = 0$ dB, for the GT and GWT used for generation of RF-DNA fingerprints and the results presented in Sect. IV. The T-F localization benefits of the GT and GWT transforms were considered for characterizing and identifying types of power supply disturbances [23], [24].

For results in Sect. IV, the GT and GWT were implemented using the Gaussian analysis window in (8) per [19]. RF-DNA

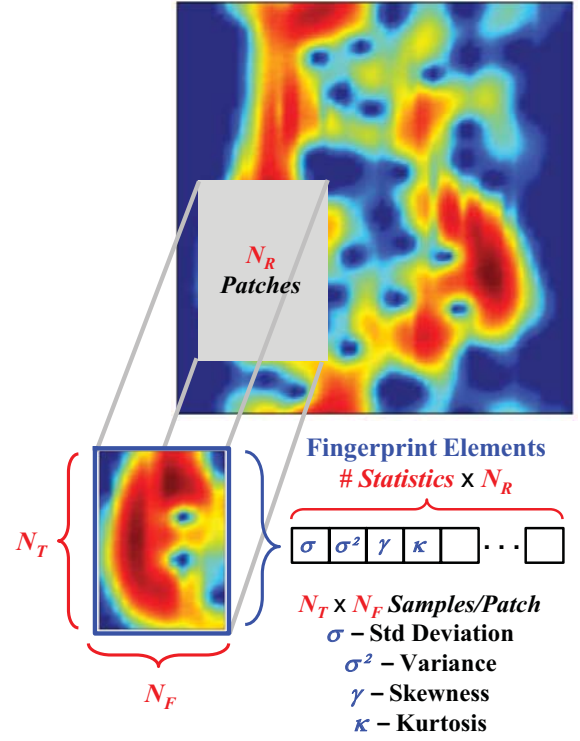


Fig. 4. Gabor-based RF-DNA fingerprint generation using $N_T \times N_F$ 2-D patches taken from the centered and normalized magnitude-squared GT and GWT coefficients

fingerprints are generated from the *normalized* (i.e., subtraction of the minimum value followed by division by the maximum value) magnitude-squared Gabor ($|G_{mk}|^2$) and Gabor-Wigner ($|GWT_{mk}|^2$) coefficients. As illustrated in Fig. 4, the resultant T-F surface is subsequently divided into $N_T \times N_F$ 2-D subregions (patches), vectorized to a length of N_{TF} , and statistics (standard deviation (σ), variance (σ^2), skewness (γ), and kurtosis (κ)) calculated. The $N_T \times N_F$ dimensions were chosen to ensure a minimum of $N_{TF} = 15$ coefficients were used for statistical calculation.

The total number of fingerprint regions is dependent on the total number of Gabor or Gabor-Wigner coefficients generated via (8) or (9), respectively. To facilitate comparative analysis, the parameters $M = 150$, $K_G = 150$ and $N_\Delta = 1$ were selected for generation of both the GT and GWT. Therefore, an *oversampling* of $N_{OS} = 150$ was used in the calculation of the GT and GWT. The resulting 150×150 T-F plane is divided into $N_R = 50$ patches where $N_T = 10$ ($m = -75, -74, \dots, 75$) and $N_F = 5$ ($k = -21, -20, \dots, 28$). Similar to TD and SD RF-DNA fingerprint generation, statistics calculated over the entire 150×150 T-F plane are included representing the N_{R+1} subregion. For GT and GWT classification results in Sect. IV, the resultant Gabor-based RF-DNA fingerprints are comprised of a total of 204 elements (4 Statistics \times 51 Subregions).

E. MDA/ML Processing

As in previous work [5]–[7], [12], [25], this work uses Multiple Discriminant Analysis (MDA) for feature selection

and Maximum Likelihood (ML) estimation for device classification, i.e., MDA/ML processing.

1) *MDA Feature Selection*: Multiple Discriminant Analysis (MDA) is used to reduce feature dimensionality while improving class separability. MDA extends Fisher's Linear Discriminant Analysis (LDA) from a two-class case to the C -class case, where C is the number of classes/devices. MDA is a linear operation that projects the samples (i.e., the RF-DNA fingerprints) to a $(C - 1)$ -dimensional subspace without reducing the power of class separability [26]. The MDA projection maximizes inter-class distances while minimizing intra-class spread. All results presented herein are projected into a $(C - 1) = 5$ -dimensional subspace.

In MDA, the between class (inter-class, \mathbb{S}_b) and within class (intra-class, \mathbb{S}_w) scatter matrices are computed as [26],

$$\mathbb{S}_b = \sum_{i=1}^C P_i \Sigma_i, \quad (12)$$

$$\mathbb{S}_w = \sum_{i=1}^C P_i (\mu_i - \mu_0)(\mu_i - \mu_0)^T, \quad (13)$$

where Σ_i is the covariance matrix of class c_i and P_i is the prior probability of class c_i . The prior probabilities are assumed to be equal and the costs uniform for the results presented herein. Individual RF-DNA fingerprints are projected into the lower $(C - 1)$ -dimensional subspace using,

$$\mathbf{F}_i^{\mathbb{W}} = \mathbb{W}^T \mathbf{F}_i, \quad (14)$$

where \mathbb{W} is the projection matrix formed from the $(C - 1)$ eigenvectors of $\mathbb{S}_w^{-1} \mathbb{S}_b$. This formation of \mathbb{W} results in the optimal ratio between the inter-class distances and intra-class variances [26]. Given N_p fingerprints per device (class), the projected training matrix $\mathbb{F}^{\mathbb{W}}$ is formed as follows,

$$\mathbb{F}^{\mathbb{W}} = [\mathbf{F}_1^{\mathbb{W}}, \mathbf{F}_2^{\mathbb{W}}, \dots, \mathbf{F}_{N_p}^{\mathbb{W}}]^T. \quad (15)$$

A multivariate normal distribution is then fitted to the MDA-projected data and the estimated mean vector $\hat{\mu}_i^{\mathbb{W}}$ and covariance matrix $\hat{\Sigma}_i^{\mathbb{W}}$ are calculated for each class. A pooled estimate of covariance matrices is used to implement a *linear* Bayesian classifier [26]. A reference template is created for each device by fitting a distribution, using the pooled covariance estimate and the selected class' mean vector, to the device's projected training data (noted by the superscript \mathbb{W}).

2) *ML Device Classification*: In RF-DNA fingerprinting, a device's identity is estimated by comparing an *unknown* input fingerprint with C trained models that have been generated for all class members. A classification decision is made by computing a similarity measure between the unknown fingerprint and each of the C known reference templates and assigning it to the class that yields the best match. As in [25], a Bayesian posterior probability is used for the similarity measure under the assumptions of uniform costs and equal priors. This approach optimally minimizes the classification error probability [26].

In the case of C devices, an *unknown* device's RF-DNA fingerprint $\hat{\mathbf{F}}$ is assigned to class c_i according to,

$$P(c_i|\hat{\mathbf{F}}) > P(c_j|\hat{\mathbf{F}}) \quad \forall j \neq i, \quad (16)$$

where $i \in \{1, 2, \dots, C\}$ and $P(c_i|\hat{\mathbf{F}})$ is the conditional posterior probability that $\hat{\mathbf{F}}$ belongs to class c_i . Applying Bayes' Rule, the conditional probability is computed as [27],

$$P(c_i|\hat{\mathbf{F}}) = \frac{P(\hat{\mathbf{F}}|c_i)P(c_i)}{P(\hat{\mathbf{F}})}. \quad (17)$$

Assuming equal prior probabilities for all classes, i.e., $P(c_i) = 1/C$, $P(c_i)$ can be neglected when evaluating (17). Also, since the conditional probability is being calculated for a given fingerprint $\hat{\mathbf{F}}$, the denominator remains constant across all c_i and can be neglected as well. This reduces the decision criteria in (17) to maximizing the likelihood for $P(\hat{\mathbf{F}}|c_i)$ for all c_i . A multi-variate Gaussian distribution is fitted to each class' training set to form the reference templates. These reference templates are used to estimate the likelihood values of the given fingerprint $\hat{\mathbf{F}}$ [26].

$$P(\hat{\mathbf{F}}|c_i) = \frac{1}{(2\pi)^{(C-1)/2} |\hat{\Sigma}|^{1/2}} \cdot \exp(\mathcal{F}_e), \quad (18)$$

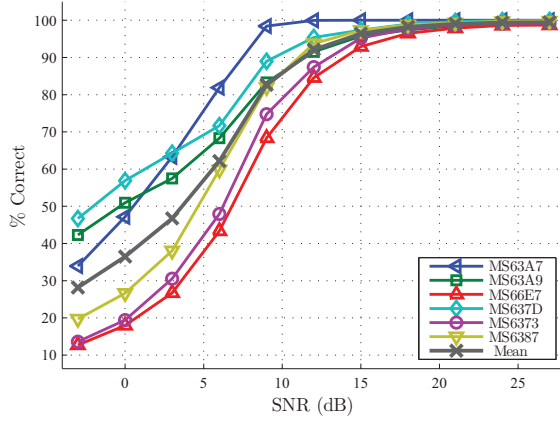
where,

$$\mathcal{F}_e = -\frac{1}{2}(\hat{\mathbf{F}} - \hat{\mu}_i)^T \hat{\Sigma}^{-1}(\hat{\mathbf{F}} - \hat{\mu}_i). \quad (19)$$

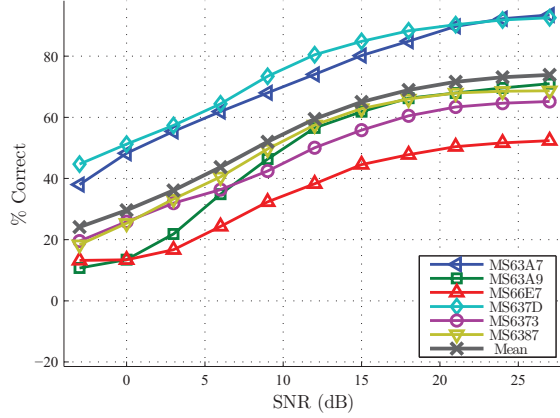
Average percent correct device classification is calculated as the percentage of the time the classifier correctly assigns an unknown RF-DNA fingerprint to its true class over all trials. To ensure statistical significance and improve reliability of results, *K-fold cross-validation* with $K=5$ was implemented during the feature selection and subsequent ML classification. While selection of K can be data dependent, a value of $K=5$ is consistent with common practice and literature which suggests values of $K=5$ and $K=10$ are appropriate [28].

IV. DEVICE CLASSIFICATION RESULTS

MDA/ML classification results for $N_{MS} = 6$ MS devices and each RF-DNA fingerprinting technique are shown in Fig. 5 (TD and SD fingerprinting) and Fig. 6 (Gabor-based fingerprinting) for $SNR \in [-3, 27]$ dB. Accounting for the total number of collected near-transient responses, 1000 per device, and 10 Monte Carlo noise realizations per SNR, the ML classification results in these figures are based on 10000 classification decisions. The number of classification decisions provide sufficient statistical significance to enable Confidence Interval (CI) assessment using CI=95%. For all plotted data in this section, the vertical extent of each data marker exceeds the extent of CI=95% intervals. Error bars have been omitted to enhance visual clarity. As shown in Fig. 5(a), TD RF-DNA fingerprinting achieves individual device classification performance of 90% or better for all devices at $SNR \geq 15$ dB. However, Fig. 5(b) shows that this same 90% or better accuracy is only achieved for two devices using SD RF-DNA fingerprinting at $SNR \geq 21$ dB. In an effort to achieve



(a) Time Domain (TD) RF-DNA.

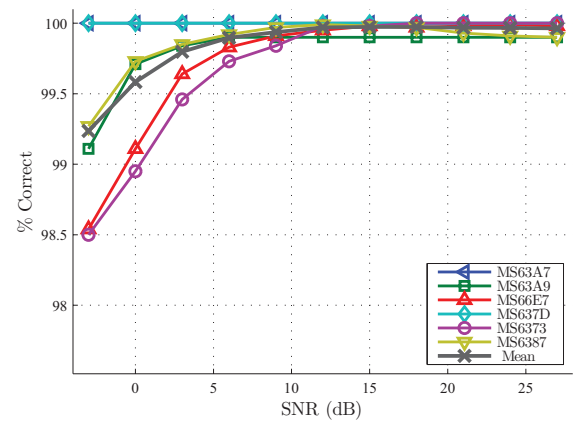


(b) Spectral Domain (SD) RF-DNA.

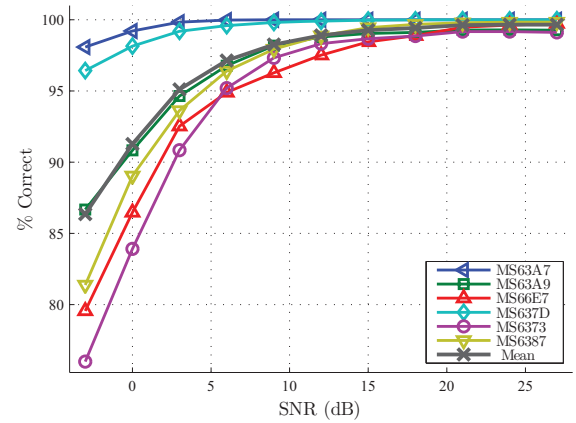
Fig. 5. TD and SD RF-DNA fingerprinting: MDA/ML classification performance for individual WiMAX MS devices with serial numbers as indicated.

increased device level discrimination of 802.16e WiMAX MS devices (i.e., serial number discrimination), the effectiveness of RF-DNA fingerprinting with Gabor coefficient magnitudes was investigated. Figure 6(a) shows that individual device classification performance with GT RF-DNA fingerprinting was 98.5% or better for all devices at $SNR \geq -3$ dB. For GWT RF-DNA fingerprints, Fig. 6(b) shows that individual device classification performance for all devices is better than 90% for $SNR \geq 3$ dB.

For direct comparison, average results across all devices in Fig. 5 and Fig. 6 are shown overlaid in Fig. 7. As indicated, GT and GWT RF-DNA fingerprinting is clearly superior to TD and SD. Furthermore, GT and GWT are statistically equivalent at $SNR \geq 10$ dB. For other SNR considered here, the benefit of enhanced T-F localization with the GWT is not evident. This effect may be attributable to GT RF-DNA processing artifacts that are not present in the GWT responses. For example, the $m \in [-75, 75]$ and $k \in [-21, 28]$ coefficients used for processing in both cases were arbitrarily chosen for demonstration. Per Fig. 3, the $k \in [-21, -18]$ region in the GWT response is minimal. Comparative analysis of GT and GWT processing continues, with a goal toward assessing robustness under varying operational conditions,



(a) Gabor Transform (GT) RF-DNA.



(b) Gabor-Wigner Transform (GWT) RF-DNA.

Fig. 6. Gabor-based RF-DNA fingerprinting: MDA/ML classification performance for individual WiMAX MS devices with MAC ID as indicated.

e.g., multipath, mobility, channel fading, etc..

V. CONCLUSION

Using previously developed RF-DNA fingerprinting concepts that successfully exploited “pre-defined” preamble re-

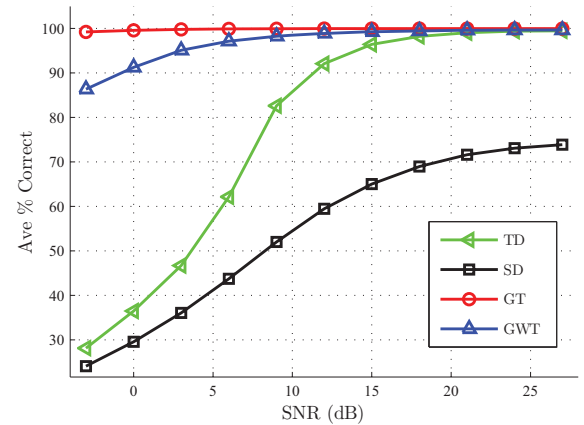


Fig. 7. Average MDA/ML classification performance for time, spectral, and Gabor-based RF-DNA fingerprint generation techniques.

sponses in OFDM-based 802.11a signals [4], [5], the authors here present results for an initial investigation that focuses on OFDM-based signals that *do not* contain pre-defined responses. This is done using both Time Domain (TD) and Spectral Domain (SD) signal features as used in previous work, as well as, a new set of features generated from Gabor Transform (GT) coefficients. The need for considering an alternate feature space was driven by the increased classification challenge presented by a lack of pre-defined signal responses. The selection of Gabor-based features was driven by previous work that assessed GT and GWT applicability for characterizing and identifying types of power supply disturbances [23], [24].

Relative to TD and SD fingerprinting, RF-DNA fingerprinting with GT fingerprints provided the best means for achieving reliable (better than 90% correct) discrimination of 802.16e MS devices for $SNR \in [-3, 27]$ dB. In terms of “gain” (reduction in required SNR to achieve a given percentage of correct classification), GT RF-DNA fingerprinting provided 18 dB, 24 dB and 3 dB of gain at 90% classification relative to TD, SD and GWT fingerprinting, respectively. As with previous RF-DNA fingerprinting using Wavelet-based T-F features [4], [5], preliminary results here suggest that T-F localization provided by the GT and GWT effectively highlights RF-DNA features for device classification.

ACKNOWLEDGMENT

This work sponsored by the Sensors Directorate, Air Force Research Laboratory, Wright-Patterson AFB, OH.

“The views expressed in this article are those of the author(s) and do not reflect official policy of the United States Air Force, Department of Defense or the U.S. Government”

REFERENCES

- [1] Jana, S. and S.K. Kasera, “Wireless Device Identification with Radiometric Signatures,” in *Proc of the ACM 14th Int’l Conf on Mobile Computing and Networking (MOBICOM08)*, Sep 2008.
- [2] Tippenhauer, N.O., K.B. Rasmussen, C. Popper, and S. Capkun, “Attacks on Public WLAN-Based Positioning,” in *Proc of the ACM 7th Int’l Conf on Mobile Systems, Applications and Services (MOBISYS09)*, Jun 2009.
- [3] Danev B. and S. Kapkun, “Transient-Based Identification of Wireless Sensor Nodes,” in *Proc of the 8th ACM/IEEE Int’l Conf on Information Processing in Sensor Networks (IPSN09)*, Apr 2009.
- [4] Klein R.W., M.A. Temple, M.J. Mendenhall and D.R. Reising, “Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance,” in *Proc of IEEE Int’l Conf on Communications (ICC09)*, Jun 2009.
- [5] Klein, R.W., M.A. Temple and M.J. Mendenhall, “Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security,” *Jour of Communications and Networks*, Vol. 11, No. 6, Dec 2009.
- [6] Reising D.R., M.A. Temple and M.J. Mendenhall, “Improving Intra-Cellular Security Using Air Monitoring with RF Fingerprints,” in *Proc of 2010 IEEE Wireless Communications & Networking Conf (WCNC10)*, Apr 2010.
- [7] —, “Improved Wireless Security for GMSK-Based Devices Using RF Fingerprinting,” *Int. J. Electronic Security and Digital Forensics*, Vol. 3, No. 1, pp. 41-59, 2010.
- [8] *IEEE 802.16E System Profile Analysis for FCI’s Airport Surface Operation*, European Organisation for the Safety of Air Navigation, Edition 1.3, Released Issue, 30 Sep 2009.
- [9] Hall E., J. Budinger, R. Diamond and R. Apaza, “Aeronautical Mobile Communications System Development Status,” in *Proc of Int Communications, Navigation and Surveillance Conf (ICNS10)*, May 2010.
- [10] “Top 10 Network Security Threats, *Government Technology*,” Sep 2010. [Online]. Available: <http://www.govtech.com/security/Top-10-Network-Security-Threats>
- [11] Williams M.D., M.A. Temple and D.R. Reising, “Augmenting Bit-Level Network Security Using PHY Layer RF-DNA Fingerprinting,” in *Proc of 2010 IEEE Global Communications Conf (GLOBECOM10)*, Dec 2010.
- [12] Williams M.D., S.A. Munns, M.A. Temple and M.J. Mendenhall, “RF-DNA Fingerprinting for Airport WiMax Communications Security,” in *Proc of 4th Int’l Conf on Net and Sys Security (NSS10)*, Sep 2010.
- [13] *IEEE Std 802.16-2009, Local and Metropolitan Area Networks, Part 16: Air Interface for Broadband Wireless Access Systems*, Inst of Electrical and Electronics Engineers, New York, New York, USA, May 2009.
- [14] *IEEE Std 802.16e-2005, Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access System*, Inst of Electrical and Electronics Engineers, New York, New York, USA, Feb 2006.
- [15] Pei, S. and J. Ding, “Relations Between Gabor Transforms and Fractional Fourier Transforms and Their Applications for Signal Processing,” *IEEE Trans on Signal Processing*, Vol. 55, No. 10, Oct 2007.
- [16] *BreezeMAX Extreme 5000: WiMAX 16e Pioneer for the License-Exempt Market*, Alvarion, Edition 215373 Rev. A, 2009.
- [17] *Agilent E3238 Signal Intercept and Collection Solutions: Family Overview*, Agilent Technologies Inc., USA, Publication 5989-1274EN, Jul 2004.
- [18] Proakis J., *Digital Communications*, 4th ed., G. T. Hoffman and J. M. Morris, Eds. New York, NY: McGraw-Hill, 2001.
- [19] Bastiaans, M. J., “Discrete Gabor Transform and Discrete Zak Transform,” in *Proc of IEEE Int’l Conf on Signal and Image Processing Applications (ICSIPA96)*, 1996.
- [20] Gabor D., “Theory of Communication,” *J. Inst. Elect. Eng. (London)*, Vol. 93, No. III, pp. 429-457, 1946.
- [21] Wexler J. and S. Raz, “Discrete Gabor Expansions,” *Signal Processing*, Vol. 21, No. 3, pp. 207-220, 1990.
- [22] Zibulski M. and Y. Y. Zeevi, “Oversampling in the Gabor Scheme,” *IEEE Trans. Signal Processing*, Vol. 41, No. 8, pp. 2679-2687, 1993.
- [23] Cho, et al., “Time-Frequency Analysis of Power-Quality Disturbances via the Gabor-Wigner Transform,” *IEEE Trans on Power Delivery*, Vol. 25, No. 1, Jan 2010.
- [24] Szmajda, M., K. Gorecki and J. Mroczka, “Gabor Transform, SPWVD, Gabor-Wigner Transform and Wavelet Transform—Tools for Power Quality Monitorins,” *Metrology and Measurement Systems*, Vol. 42, No. 3, Dec 2010.
- [25] 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, pp. 793-808, Dec 2011.
- [26] Theodoridis S. and K. Koutoumbas, *Pattern Recognition*, 4th ed. Academic Press, 2009.
- [27] MacKay D.J.C., *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press, 2003.
- [28] 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.