ENHANCING NETWORK SECURITY USING 'LEARNING-FROM-SIGNALS' AND FRACTIONAL FOURIER TRANSFORM BASED RF-DNA FINGERPRINTS

Mark A. Buckner (Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, USA, bucknerma@ornl.gov); Miljko Bobrek (ORNL); Ethan Farquhar (ORNL); Paul Harmer (Air Force Institute of Technology); Michael Temple (AFIT).

ABSTRACT

Wireless Access Points (WAP) remain one of the top 10 network security threats. This research is part of an effort to develop a physical (PHY) layer aware Radio Frequency (RF) air monitoring system with multi-factor authentication to provide a first-line of defense for network security--stopping attackers before they can gain access to critical infrastructure networks through vulnerable WAPs. This paper presents early results on the identification of OFDM-based 802.11a WiFi devices using RF Distinct Native Attribute (RF-DNA) fingerprints produced by the Fractional Fourier Transform (FRFT). These fingerprints are input to a "Learning from Signals" (LFS) classifier which uses hybrid Differential Evolution/Conjugate Gradient (DECG) optimization to determine the optimal features for a low-rank model to be used for future predictions. Results are presented for devices under the most challenging conditions of intra-manufacturer classification, i.e., same-manufacturer, same-model, differing only in serial number. The results of Fractional Fourier Domain (FRFD) RF-DNA fingerprints demonstrate significant improvement over results based on Time Domain (TD), Spectral Domain (SD) and even Wavelet Domain (WD) fingerprints.

1. INTRODUCTION

With the rapid expansion and pervasiveness of wireless communication systems the threat of cyber attacks on critical infrastructure by way of Wireless Access Points (WAP) becomes increasingly likely. Using cloud computing for brute force attacks such as cracking passwords and cryptographic keys “an attacker can now achieve in minutes or hours what would have taken years.”[1] The only thing standing between a malevolent “hacker” and the nation’s critical infrastructure may be a WAP–recognized as one of the top 10 network security threats [2].

WAP vulnerability is traditionally addressed through bit-level security mechanisms in layer 2 or above in the Open Systems Interconnection (OSI) model. For example the majority of intrusion detection systems operate at Layer 3, the Network (NET) layer, or higher [3]. While providing a measure of security, these methods ignore information inherent to a device’s Radio Frequency (RF) emissions. Thus, potential security benefits could be realized from a PHY-layer aware multi-factor authentication approach to wireless network security based on RF Distinct Native Attributes (RF-DNA).

Multi-factor authentication (MFA) is a proven, reliable approach to network and computer security and is advised by the U.S. Federal Financial Institutions Examination Council for high-risk situations [4]. MFA uses three common categories of factors: (1) something you know, e.g., PIN, password, answer to a challenge question, (2) something you have, e.g., magnetic card, token, smartcard, contact memory button, and (3) something you are, e.g., biometric factors such as fingerprint, voiceprint, or iris scan. Our ultimate goal is to develop a PHY-layer aware multi-factor authentication solution where the device's "biometric factor" is derived from its RF-DNA.

Initial work has focused on augmenting bit-level protection mechanisms via RF air monitoring devices located at network access points [5]–[9]. Given the envisioned computational power required for air monitoring, typical WAP locations seem ideal given that the necessary resources (physical space, prime power, etc.) are generally available. These previous works demonstrated the potential for using RF-DNA fingerprints for identifying specific wireless devices [5]–[10] based on Time Domain (TD) [6], Spectral Domain (SD) [8] and Wavelet Domain (WD) [5] features. The system described in [6] and [7] was for GSM signals though it is believed a similar approach is directly applicable for similarly configured WiMAX, LTE and WiFi systems.

The Wavelet transform is a joint Time-Frequency (T-F) transform which exploits the localization of T-F phenomena inherent in a devices Electromagnetic (EM) signal structure [11]. The Fractional Fourier Transform (FRFT) an alternative T-F technique is investigated in this paper and demonstrates similar benefits as wavelets when applied to experimentally collected OFDM-based 802.11a WiFi signals under intra-manufacturer conditions (same manufacturer,

same model, different serial numbers). Relative to inter-manufacturer conditions (inter-operable devices from different manufacturers), intra-manufacturer classification poses the greatest classification challenge [5]–[8].

A new hybrid Differential Evolution/Conjugate Gradient (DECG) variant of the Learning-from-Signals (LFS) "classification engine" described in [9] is only briefly introduced. A detailed description will be provided in a future publication. Classification accuracy of the DECG-LFS using Fractional Fourier Domain (FRFD) RF-DNA fingerprints is compared to a Fisher-based Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classifier using TD, SD, and WD fingerprints.

RF-DNA and LFS are also being used as part of a cognitive engine to rapidly classify waveforms for a Cognitive Radio and identification of unique electrical devices on commercial power lines.

The remaining sections of the paper are: Section 2 Technical Background; Section 3 Methodology; Section 4 Results; and Section 5 Summary and Conclusions.

2. TECHNICAL BACKGROUND

The following subsections provide a summary of the key technical concepts behind the results presented in Section4. This includes a description of RF-DNA Fingerprinting in Section 2.1, Fractional Fourier Transform in Section 2.2 and the hybrid DECG-LFS algorithm in Section 2.3.

2.1. RF-DNA Fingerprinting

RF-DNA fingerprinting is a technique for identifying devices based on unique characteristics in their PHY-layer (EM/RF) emissions. RF-DNA fingerprints are exploitable because they are: (1) *distinct*, enabling make, model and even serial number level identification device; and (2) *native* to the device from the time of manufacture, due to component tolerances and variability in manufacturing processes. The RF-DNA fingerprinting process is depicted in Figure 1.

Prior research has shown that specific serial-numbered devices possess unique RF-DNA characteristics attributable to subtle differences in manufacturing (component tolerances, part type, part lot number, assembly processes, etc.). This fact has been confirmed for multiple communication waveforms, including: 802.11 WiFi signals [5], [9], [12]–[15], GSM cell phone signals [7], [10], 802.16 WiMAX signals [8], 802.15 Bluetooth signals [16], and RFID signals [17], [18] using multiple RF fingerprinting techniques.

Even though the techniques used to produce the RF-DNA fingerprints varied, they generally followed these steps: (1) Signal Collection and Post-Collection Processing, (2) Fingerprint Generation, and (3) Signal/Device Classification.

2.1.1. Signal Collection and Post-Collection Processing

The single collection and post-collection processing used in [6] has been adopted for this work. All signals were collected with an RF Signal Intercept and Collection System (RFSICS) based on Agilent's E3238 system [19]. The OFDM-based 802.11a WiFi devices were isolated from the RFSICS to minimize the introduction of unrepeatable environmental and interference effects by placing (1) some devices in an RF anechoic chamber, (2) some in separate rooms—a typical office environment, (3) some RF absorbing material in strategic locations, and/or (4) combinations of 1-3. The post-filtered collected SNR for the collected signals is on the order of $SNR_C \in [30, 40]$ dB. This enables direct scaling (G_N in Figure. 1) and addition of like-filtered Additive White Gaussian Noise (AWGN) to generate analysis signals at the desired SNR_A. These signals are used for RF-DNA fingerprinting and device classification.

2.1.2. Fingerprint/Feature Generation

The RF-DNA fingerprints for TD [6], SD [8], and WD [5] were generated as described in previous work and used here for comparison.

2.1.3 Signal/Device Classification

Previously classification was performed using a Fisher-based MDA/ML process [5], [7], [10]. The MDA/ML classifier is an extension of Fisher's Linear Discriminant that is used when more than two input devices are to be classified. MDA uses a projection matrix (W) to reduce the input dimensionality. The MDA/ML process is that of finding W such that projected inter-class separation is maximized and intra-class spread is minimized [20]. Given N_D devices (input classes), the MDA/ML process projects the input features into an $N_D - 1$ decision space.

Device classification is performed using a ML classifier derived from Bayesian Decision Theory, with the multidimensional input data classified as belonging to one of N_D possible classes. A Bayesian-based decision uses known prior probabilities, probability densities, and relevant costs associated with making a decision. The decision process relies on an accurate representation of the class distribution and its parameters in order to define the likelihood. A sample is assigned the label of the class with the maximum likelihood response. For ML classification, the prior probabilities are assumed to be equal and the costs uniform.

We now describe how RF-DNA fingerprints are generated using the joint T-F Fractional Fourier Transform.

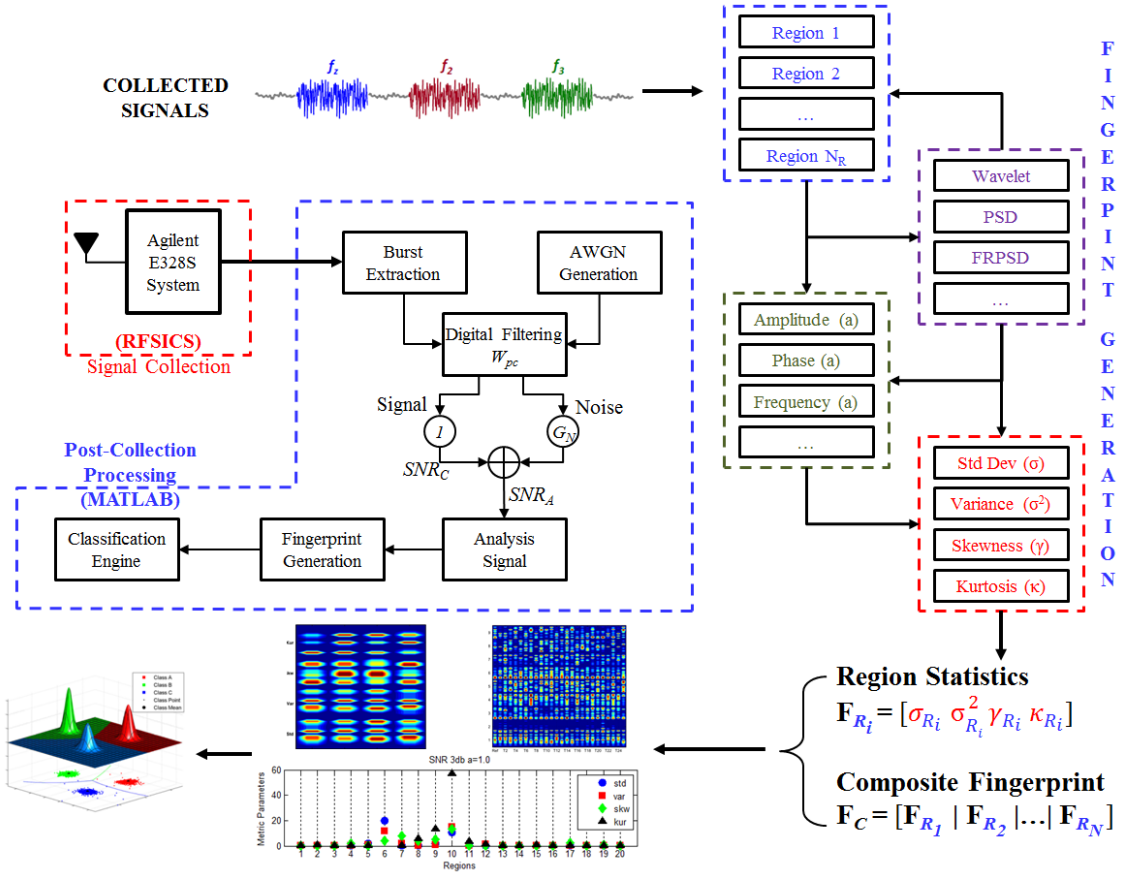

Figure 1. RF-DNA Fingerprint/Feature Generation Process.

2.2. Fractional Fourier Transform

The Fractional Fourier Transform (FRFT) is a generalization of the conventional Fourier Transform (FT) defined as

$$F^{a}(u) = \int_{-\infty}^{+\infty} f(t)K(\alpha,u,t)dt \qquad (1)$$

where $a = 2\alpha/\pi$ is the order of the transform, and $K(\alpha,u,t)$ is the generalized transform kernel defined by

$$\sqrt{\frac{1-j\cot\alpha}{2\pi}}\exp\left[j\left(\frac{u^2+t^2}{2}\cot\alpha - ut\csc\alpha\right)\right], \quad \alpha \neq 0,\pi,2\pi$$
$$\delta(t-u), \quad \alpha = 0,2\pi$$
$$\delta(t+u), \quad \alpha = \pi \qquad (2)$$

The transform order (a) determines the rotation angle (α) of the time-frequency plane. It takes values of a = [0 4] with corresponding rotation angles of α = [0 to 2π]. Table 1 shows the kernels for several typical values for a.

For a rotation angle of $\alpha = 0$, FRFT gives the time-only representation of the signal and for the angle of $\alpha = \pi/2$ the frequency-only representation. For angles between [0 $\pi/2$] , the FRFT contains both time and frequency features which gives it a unique capability of looking at the time and frequency transitions simultaneously (similar to wavelets).

Table 1. Fractional Fourier kernels for select transform order (a) and rotation angles (α).

a	$\alpha = a\pi/2$	Kernel	Description
0, 4	0, 2π	$\delta(t-u)$	Identity
1	$\pi/2$	exp(-*jut*)	FT
2	π	$\delta(t+u)$	Reflection
3	$3\pi/2$	exp(*jut*)	Inverse FT

Several algorithms for approximate calculation of the FRFT have been published recently including Direct Form DFRFT, Improved Sampling DFRFT [21], Eigenvector Decomposition DFRFT [22], and Linear Combination DFRFT [23].

2.2.1. Signal Collection and Post-Collection Processing

Each 802.11a OFDM packet has a preamble structure with two distinct regimes or training sequences, including one short and one long. The results in this paper use only the short segment which contains ten short 0.8 μsec OFDM symbols and uses only 12 of the available 52 subcarriers. The preamble for each burst is autocorrelated and then the

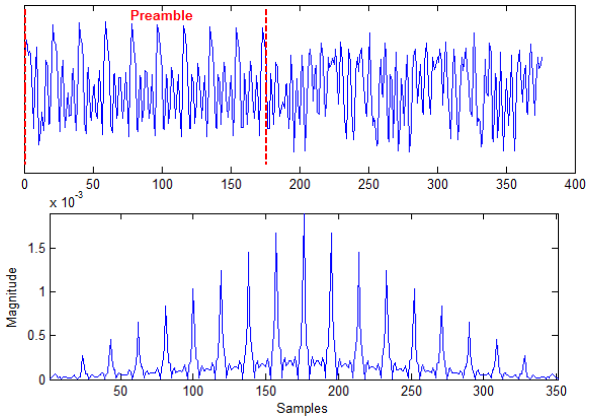

Figure 2. Time domain and preamble autocorrelation of a captured 802.11a signal.

normalized Fractional Fourier Power Spectral Density (FRPSD) is calculated for specified values of α. Figure 2 shows the time-domain capture of the preamble (top) and the autocorrelation of the short preamble segment (bottom).

2.2.2. FRFD Fingerprint Generation

FRFD fingerprints are generated by dividing the FRPSD into 20 regions ($N_R = 20$) and calculating four, $N_{SM} = 4$, statistical measures for each: standard deviation (σ), variance (σ^2), skewness (γ), and kurtosis (κ). Figure 3 shows the normalized FRPSD of the autocorrelated preambles for α = [π/8, π/4, 3π/8, π/2] and the 20 regions for four different values of α. The statistics form the *fingerprint* of FRPSD's *i*th *region*

$$\mathrm{F}_{\mathrm{R}_i} = \left[\sigma_{R_i}\ \sigma_{R_i}^2\ \gamma_{R_i}\ \kappa_{R_i}\right]_{1\times N_{SM}} \tag{4}$$

where $i = 1,2,\ldots,N_R$. The fingerprints from each region are concatenated to form the *FRFD composite statistical fingerprint aiven*

$$\mathbf{F}_c = \left[\mathrm{F}_{R_1} \vdots \mathrm{F}_{R_2} \vdots \cdots \vdots \mathrm{F}_{R_N}\right]_{1\times N_F} \tag{5}$$

where N_F is the total number of fingerprint features (dimension), which for FRFD is 80,

$$N_F = N_R \times N_{SM} \tag{6}$$

2.3. DECG-LFS

LFS is an adaption of "Learning From Data" (LFD) techniques where the input training data is derived from samples of a sensor response [9], [24], [28]. A DE-only version LFS is described in [9]. DE is a population-based, direct search, evolutionary strategy. While DE is similar to other population based search algorithms, like Genetic Algorithms (GA), it differs in both its self-referential

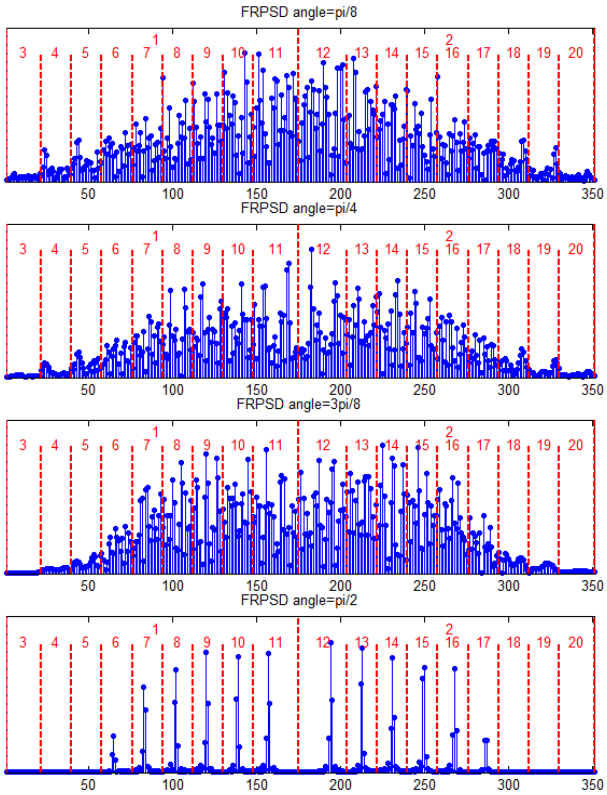

Figure 3. FRFD Fingerprint Regions: Normalized FRPSD magnitude response of the preamble for α = [π/8, π/4, 3π/8, π/2] as indicated.

mutation scheme and its selection process [9], [28], [29]. The version of LFS described in this section, which combines DE with Conjugate-Gradient/Line-Search (CGLS) [26], [27] was first introduced in [24] as a *Method of Detecting Local Minima in Multidimensional data (ModelM)*. While providing a detailed description of the DECG internals is beyond the scope of this paper, it will be described in a future publication.

DECG-LFS constructs a model of an unknown input-output relationship from a set of labeled training data and uses it to predict or classify previously unseen data [25]. DECG-LFS can be viewed as a method of low rank model estimation or feature selection. It does this by using a modified version of multivariate kernel regression or localized kernel regression (LKR) described by the equation:

$$\hat{y}(\mathbf{x};\mathbf{H}) = \hat{m}(\mathbf{x};\mathbf{H}) = \frac{\sum_{i=1}^{n} K(d_{\mathbf{H}}^2(\mathbf{x}_i,\mathbf{q}))y_i}{\sum_{i=1}^{n} K(d_{\mathbf{H}}^2(\mathbf{x}_i,\mathbf{q}))} \tag{7}$$

where $\mathbf{x}$ is the *m*-dimensional input vector and $d_{\mathbf{H}}^2(\mathbf{x}_i,\mathbf{q}) = (\mathbf{x}_i - \mathbf{q})^T\mathbf{H}(\mathbf{x}_1 - \mathbf{q})$ is the squared Euclidian distance parameterized $\mathbf{H}$, a positive semi-definite, symmetric square matrix and the inverse of the bandwidth matrix: $\mathbf{H} \equiv \sum^{-1} = \mathrm{diag}(h_1^2, h_2^2, \ldots, h_v^2)$. While the squared

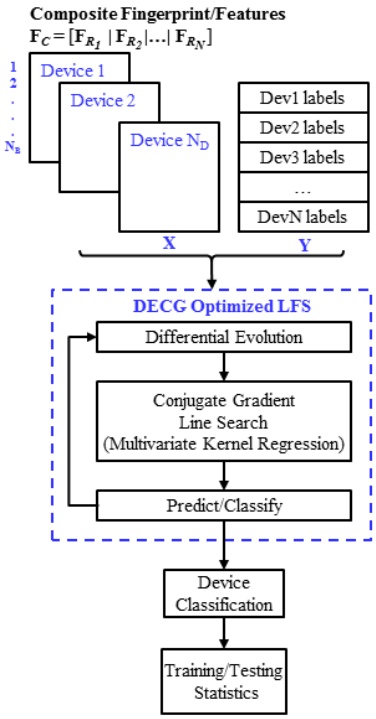

Figure 4. DECG-LFS Process.

Euclidian distance is used here, the general methodology could use any meaningful distance measure**.** Consistent with [25], [26] we refer to h_D as a *smoothing* parameter and h_D^2 as a *metric* parameter.

Many different kernel functions are supported in DECG-LFS but for this work we focus on the Gaussian kernel,

$$K(d_{\mathbf{H}}^2(\mathbf{x}_i, \mathbf{q}) = \exp^{-0.5 d_{\mathbf{H}}^2(\mathbf{x}_i, \mathbf{q})} \tag{8}$$

where $\mathbf{H} = \mathrm{diag}(h_1^2, h_2^2, \ldots, h_{NF}^2)$ and h_i^2 is the metric parameter for the i^{th} feature in $\mathbf{F}_C$.

2.3.3. Simple Device Classification

The DECG-LFS classification process shown in Figure 4 "learns" the optimal LKR model from a set of training data, $\mathcal{T} = (\mathbf{X}, \mathbf{Y})$, by minimizing a k-fold Cross-Validation Error (CVE), which is an estimator of generalization error. The input $\mathbf{X}$ is an $m \; x \; N_F$ matrix of RF-DNA fingerprints and the output $\mathbf{Y}$ is an $m \; x \; 1$ vector of integer corresponding to the class labels of the devices—if we have N_D devices we assign the first device as '1', the second as '2', …, and device N_D as 'D'. The output $\hat{\mathbf{y}}_i$ of the LKR model is a continuous real-valued number. Since what we are interested in is classification accuracy we simply round $\hat{\mathbf{y}}_i$ to produce an integer "label" corresponding to the class of the predicted device. This is then used to compute other statistics and values of interest such as % Correct Classification, and Confusion Matrix.

As demonstrated in [9], [24] and used here, DE-based LKR optimization effectively "learns" the best bandwidth parameter (metric parameter) to use for each dimension which can be used to improve LFS classifier performance.

3. METHODOLOGY

OFDM-based 802.11a WiFi signals were collected from four like-model Cisco Aironet wireless PCMCIA adapters using a pair of laptops configured as a point-to-point (P2P) network in an RF anechoic chamber. The start of the preamble in each collected burst was detected using a simple amplitude detection method with a threshold − 6 dB. The detected bursts were post-collection filtered using a 6th-order Butterworth filter having a − 3 dB bandwidth of W_{PC} = 7.7 MHz. This same filter was used for generating the like-filtered AWGN used for SNR scaling of 3, 6, 9, 12, and 15 dB. The full data set $\mathcal{F} = (\mathbf{X}, \mathbf{Y})$ contains 4000 bursts (1000 for each device). RF-DNA fingerprints for all burst at each of the SNR levels were generated for TD [6], SD [8], and WD [5] features, as described in previous work, and for FRFD as described in Section 2.2.1. Each set of RF-DNA fingerprints ($\mathbf{X}$) is normalized using mean centering and variance 1. The outputs ($\mathbf{Y}$) are not modified.

The full data set $\mathcal{F}$ was split into 2 groups, with one used for design (learning/training) $\mathcal{D}$ (1000 bursts, 250 per device) and the other used for testing $\mathcal{T}$ (3000 bursts, 750 per device). This first split we call the design/test split. The 'design' set $\mathcal{D}$ is used to develop a model that accurately predicts a new output $\hat{\mathbf{y}}$ when presented with an unseen fingerprint $\mathbf{x}$. To do this we need a model that generalizes well. The test set $\mathcal{T}$ is used evaluate how well. We use the k-fold CVE as an estimate of the generalization error.

Results for TD, SD, WD fingerprints were generated using MDA/ML. The version of MDA/ML used here only handles three devices so to estimate the 4-device classification results, four permutations (Perm123, Perm124, Perm134, Perm234) were trained and the models with the best CVE for each were averaged to approximate the total % Correct Classification over all devices.

Separate models were trained using DECG-LFS for FRFD fingerprints for all SNR levels and time-frequency order (angle) combinations of a=0.6 (α=0.9452), a=0.8 (α=1.2566) a=1 (α=1.5708) and a=1.2 (α=1.8850) – (20 models in all). CVE, design (training) Mean Squared Error (MSE_D) and test MSE (MSE_T) results were computed. CVE is obtained from k-fold CV results, which is an estimate of generalization error. The training MSE_D is obtained by applying the trained model and applying it to the complete training set $\mathcal{D}$. The testing MSE_T is obtained by applying the trained model to the unseen test set $\mathcal{T}$. All results

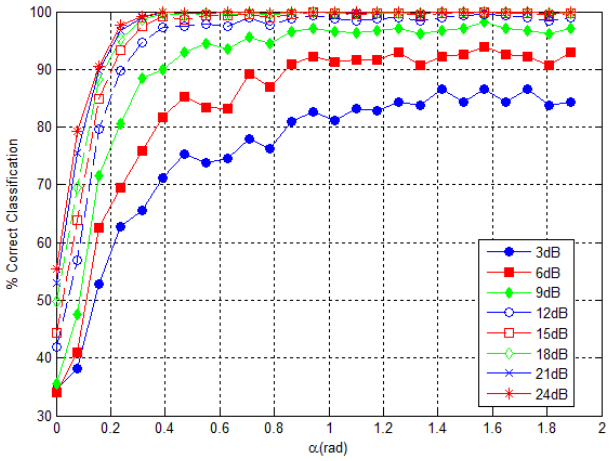

Figure 5. % Correct Classification versus rotation angle α at SNR levels of 3, 6, 9, 12, 15, 18, 21, and 24dB as indicated.

represent training a separate model for each combination of SNR and rotation α.

A version of DECG-LFS is under development that jointly optimizes the metric parameters and transform parameters τ, e.g., α for FRFD, or wavelet coefficients.

4. RESULTS

A preliminary assessment of the effectiveness of the FRPSD is made by calculating the Euclidian distance between the normalized FRPSD for each capture and the mean FRPSD of 1000 captures of each device. We use four devices of the same model, from the same manufacturer and have 1000 captures of each device. For the simple Euclidean comparison the signal samples are denoted by $Sin,\ i = [1\ 4],\ n = [1\ 1000]$ where *i* represents the index of the unit and *n* the index of the unit signal samples. The device means are calculated by

$$Ci = \frac{\sum_{n=0}^{n=N-1} Sin}{N}, N = 1000 \quad (9)$$

The in-device distances $Dii(n), i = [1\ 4], n = [1\ 1000]$ are calculated as the MSE between the signal samples for the device and the device's mean. The cross-device distances $Dij(n), i, j = [1\ 4], n = [1\ 1000]$ are calculated as the MSE between the signal samples and other device means. If $Dij(n) > Dii(n), i = [1\ 4], n = [1\ 1000]$ the device clusters are completely separable. Figure 5 shows the probability of the percent classification error for different values of the rotation angle α and different SNR ratios, when $Dij(n) > Dii(n)$ classification criterion is used. Next we describe how the Fractional Fourier Domain (FRFD) fingerprints are generated.

Next, classifier performance is assessed using average % Correct Classification on training data versus SNR, for

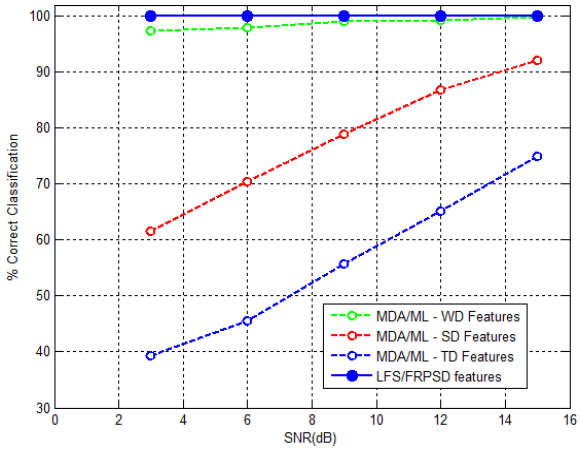

Figure 6. Training results: % Correct Classification versus SNR for MDA/ML with Spectral Doman features and LFS with FRPSD features.

TD, SD, and WD based fingerprints using MDA/ML. This is compared to the results of FRFD fingerprints optimized with DECG-LFS. Figure 6 compares the % Correct Classification results of the training CVE at all SNR levels for TD, SD, WD fingerprints (based on MDA/ML) and FRFD fingerprints (based on DECG-LFS).

Figure 7 shows the % Correct Classification for the FRFD fingerprints optimized with DECG-LFS on the test set $\mathcal{T}$ for all SNR levels and time-frequency order (angle) combinations of *a*=0.6 (α=0.9452), *a*=0.8 (α=1.2566) *a*=1 (α=1.5708) and *a*=1.2 (α=1.8850).

Figure 8 is a zoomed in view of the % Correct Classification for the FRFD fingerprints optimized with DECG-LFS on the test set $\mathcal{T}$ for all SNR levels and order (angle) combinations of *a*=0.8 (α=1.2566) *a*=1 (α =1.5708) and *a*=1.2 (α=1.8850). Notice that angle a=1 represents the frequency only plane and angles *a*=0.8 and *a*=1.2 represent symmetric rotations on either side of it (identity and

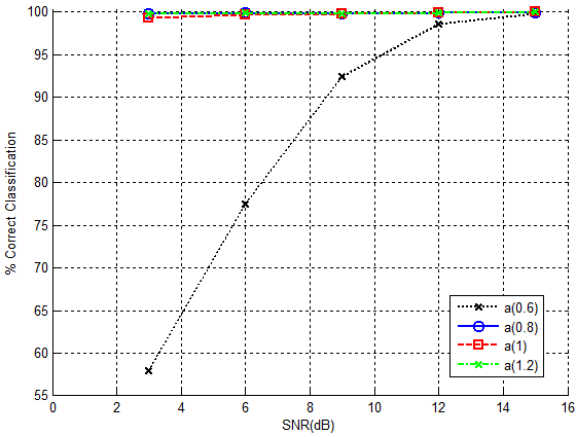

Figure 7. Testing results: % Correct Classification versus SNR for *a*=0.6 (α=0.9452), *a*=0.8 (α=1.2566) *a*=1 (α=1.5708) and *a*=1.2 (α=1.8850).

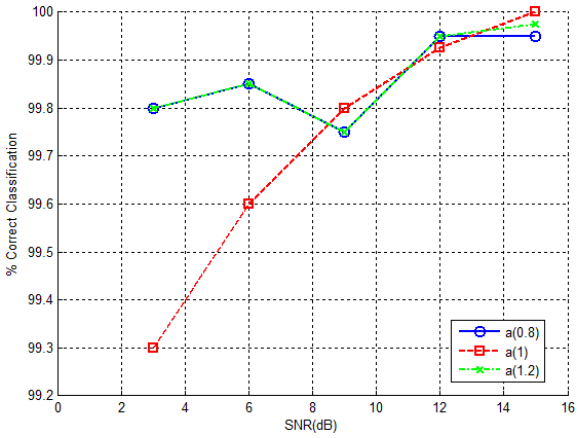

Figure 8. Close-up of testing results in Figure 7: % Correct Classification versus SNR for a=0.8 (α=1.2566) a=1 (α=1.5708) and a=1.2 (α=1.8850).

reflection respectively).

Figures 9 and 10 show the metric parameter obtained by DECG-LFS for FRFD fingerprints arranged by regions for SNR levels of 3, 6, 9, and 12 dB and order (angle) combinations of a=0.8 (α=1.2566) and a= 1 (α=1.5708) respectively.

One can infer the relative importance of a given feature based on the metric parameter h_i^2 – small h_i^2 values indicate irrelevant features, large h_i^2 values indicate relevant features. Using this knowledge one can create a low-rank model by eliminating irrelevant features.

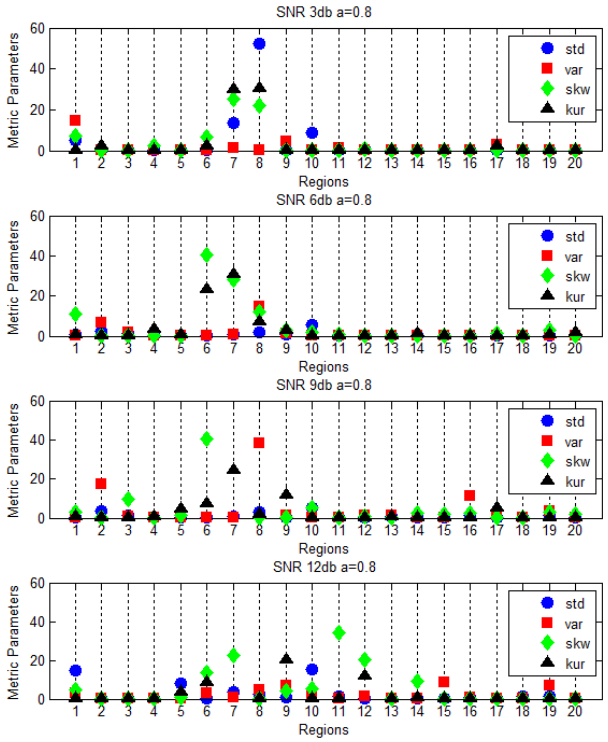

Figure 9. Metric Parameters (inverse bandwidth parameters) of the statistical features for each Region of the FRPSD for a=0.8 (α=1.2566) at SNR levels of 3, 6, 9 and 12 db.

5. SUMMARY AND CONCLUSSIONS

This work addresses the use of the joint time-frequency Fractional Fourier Transform based RF-DNA fingerprints for classifying intra-manufacture WiFi devices, i.e., identical model devices from a given manufacturer. It also introduces a DECG-LFS classifier which is envisioned for use in RF air monitors located at Wireless Access Points (WAPs). As one of the most vulnerable points in an Information Technology (IT) network, the goal is to provide a Physical (PHY) layer-aware multi-factor authentication approach to wireless network security at WAPs to augment bit-level mechanisms.

Classification performance was compared to TD, SD, and WD based fingerprints using an MDA/ML classifier for experimentally collected 802.11a WiFi signals.

Relative to MDA/ML classification using TD, SD and WD fingerprints LFS classification using FRFT was superior at all SNR levels. With the single exception of WD at the SNR=15 dB which was comparable probably because both the WD and FRFD features capture the TF characteristics of the particular OFDM 802.11a signal.

The performance of the FRFD fingerprints is likely attributable to the ability of the FRFT to capture the TF characteristics and the power of DECG-LFS to learn a robust model.

From these results we conclude that FRFD RF-DNA

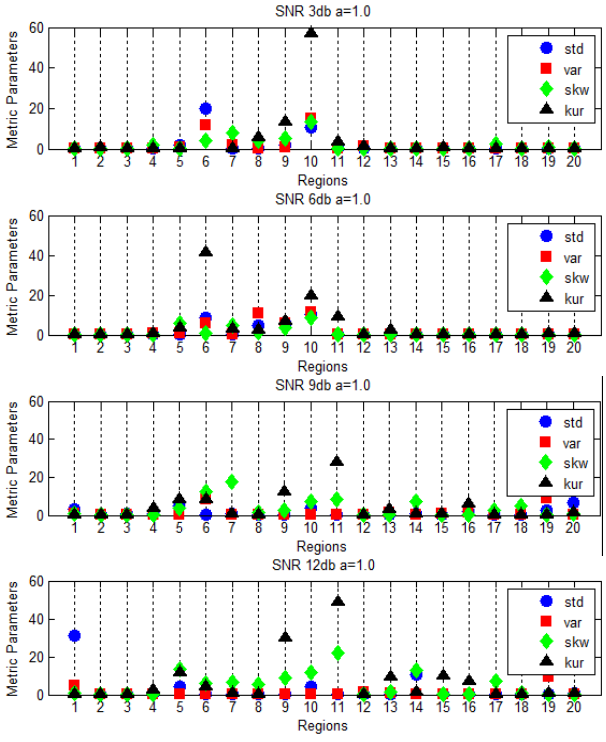

Figure 10. Metric Parameters (inverse bandwidth parameters) of the statistical features for each Region of the FRPSD for a=1.0 (α=1.5708) at SNR levels of 3, 6, 9 and 12 db.

fingerprints are viable candidates for PHY-layer-aware multi-factor authentication and warrant further investigation.

6. REFERENCES

[1] http://www.itworld.com/security/128078/password-cracking-cloud?source=ITWNLE_nlt_saas_2010-11-24

[2] H. Collins, "Top 10 network security threats," *Government Technology*, September 2010.

[3] T. D. Tarman and E. L. Witzke, "Intrusion detection considerations for switched networks," Enabling Technologies for Law Enforcement and Security, vol. 4232, no. 1, pp. 85–92, 2001. [Online]. Available: http://link.aip.org/link/?PSI/4232/85/1

[4] Federal Financial Institutions Examination Council. Supplement to "Authentication in an Internet Banking Environment." June 28, 2011. [Online]. Available: http://www.ffiec.gov/press/pr062811.htm

[5] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security," Jour of Communications and Networks: Secure Wireless Networking, vol. 11, no. 6, pp. 544–555, December 2009.

[6] D. Reising, M. Temple, and M. Mendenhall, "Improving intra-cellular security using air monitoring with RF fingerprints." IEEE Wireless Communications and Networking Conference (WCNC10), Apr 2010.

[7] M. D. Williams, M. A. Temple, and D. R. Reising, "Augmenting bitlevel network security using physical layer RF-DNA fingerprinting," in IEEE Global Communications Conference, December 2010.

[8] M. D. Williams, S. A. Munns, M. A. Temple, and M. J. Mendenhall, "RF-DNA fingerprinting for airport WiMAX communications security," in 4th International Conference on Network and Systems Security, September 2010.

[9] P. K. Harmer, M. A. Temple, M. A. Buckner, and E. Farquhar, "Using differential evolution to optimize 'learning from signals' and enhance network security," in Genetic and Evolutionary Computation Conference (GECCO), July 2011.

[10] D. Reising, M. Temple, and M. Mendenhall, "Improved wireless security for gmsk-based devices using RF fingerprinting," Int. J. Electronic Security and Digital Forensics, vol. 3, no. 1, pp. 41–59, Mar 2010.

[11] Szmajda, M., Górecki, K., & Mroczka, J. "Gabor Transform, SPWVD, Gabor-Wigner Transform and Wavelet Transform-Tools For Power Quality Monitoring," Metrology and Measurement Systems, XVII(3), pp. 383-396, 2010.

[12] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in Proc of the 14th ACM international conference on Mobile computing and networking, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 116–127. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409959

[13] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in Proc of the 13th annual ACM international conference on Mobile computing and networking, ser. MobiCom '07. New York, NY, USA: ACM, 2007, pp. 99–110. [Online]. Available: http://doi.acm.org/10.1145/1287853.1287866

[14] D. Takahashi, Y. Xiao, Y. Zhang, P. Chatzimisios, and H.-H. Chen, "IEEE 802.11 user fingerprinting and its applications for intrusion detection," Computers & Mathematics with Applications, vol. 60, no. 2, pp. 307 – 318, 2010, advances in Cryptography, Security and Applications for Future Computer Science. [Online]. Available: http://www.sciencedirect.com/science/article/B6TYJ-4YBVN48-1/2/02fc08e080dbf58edcc440f8db4ed9f3

[15] W.C. Suski II, M.A. Temple, M. J. Mendenhall, and R.F. Mills, "Radio frequency fingerprinting commercial communication devices to enhance electronic security," Int. J. Electron. Secur. Digit. Forensic, vol. 1, pp. 301–322, October 2008. [Online]. Available: http://portal.acm.org/citation.cfm?id=1454744.1454749

[16] J. Hall, M. Barbeau, and E. Kranakis, "Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting," in Communications and Computer Networks, 2006, pp. 108–113.

[17] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in Proc of the 2009 International Conference on Information Processing in Sensor Networks, ser. IPSN '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 25–36. [Online]. Available: http://portal.acm.org/citation.cfm?id=1602165.1602170

[18] D. Zanetti, B. Danev, and S. Capkun, "Physical-layer identification of UHF RFID tags," in Proc of the sixteenth annual international conference on Mobile computing and networking, ser. MobiCom '10. New York, NY, USA: ACM, 2010, pp. 353–364. [Online]. Available: http://doi.acm.org/10.1145/1859995.1860035

[19] Agilent, Agilent E3238 Signal Intercept and Collection Solutions: Family Overview, Publication 5989-1274EN, Agilent Technologies Inc., USA, 2004.

[20] R. O. Duda, P. E. Hart, and D. G. Stork, Pattern classification, 2nd ed. Wiley, November 2001.

[21] H.M. Ozaktas, O. Arikan, M.A. Kutay, and G. Bonzagi, "Digital computation of the fractional Fourier transforms," *IEEE Transactions on Signal Processing*, 44, 2141-2150, 1996.

[22] S.C. Pei, M.H. Yeh, and C.C. Tseng, "Discrete fractional Fourier transform based on orthogonal projections", *IEEE Transactions on Signal Processing*, 47, 1335-1348, 1999.

[23] G. Cariolario, T. Erseghe, P. Kraniauskas, and N. Laurenti, "A unified framework for the fractional Fourier transform", *IEEE Transactions on Signal Processing*, 46, 3206-3212, 1998.

[24] M. A. Buckner, "Learning from data with localized regression and differential evolution," Ph.D. dissertation, University of Tennessee, Knoxville, May 2003.

[25] V. S. Cherkassky and F. Mulier, Learning from data: concepts, theory, and methods, 2nd ed. Hoboken, HJ: Wiley & Sons, 2007.

[26] C. Goutte and J. Larsen. Adaptive metric kernel regression. Neural Networks for Signal Processing VIII -- Proceedings of the 1998 IEEE Workshop, VIII, (in press, Piscataway, New Jersey, 1998.

[27] C. Goutte and J. Larsen. Adaptive metric kernel regression, The Journal of VLSI Signal Processing, 26(1/2):155-67, 2000.

[28] M. A. Buckner, A. M. Urmanov, A. V. Gribok, and J. W. Hines, "Application of Localized Regularization Methods for

Nuclear Power Plant Sensor Calibration Monitoring," Technical Correspondence, 2002.
[29] K. Price, R. M. Storn, and J. A. Lampinen, Differential Evolution: A Practical Approach to Global Optimization (Natural Computing Series). Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005.