

# Using DE-Optimized LFS Processing to Enhance 4G Communication Security

Paul K. Harmer, McKay D. Williams and Michael A. Temple

Department of Electrical and Computer Engineering  
Air Force Institute of Technology  
Wright-Patterson AFB, OH 45433 USA  
Email: [Paul.Harmer\*, McKay.Williams, Michael.Temple]@afit.edu  
\*Correspondence POC

**Abstract**—Wireless communication networks remain under attack with ill-intentioned “hackers” routinely gaining unauthorized access through Wireless Access Points—one of the most vulnerable points in an Information Technology (IT) system. The goal here is to demonstrate the feasibility of using Radio Frequency (RF) air monitoring to augment conventional bit-level security at WAPs. The specific networks of interest include those based on Orthogonal Frequency Division Multiplexing (OFDM), to include 802.11a/g WiFi and 4G 802.16 WiMAX. Proof-of-concept results are presented to demonstrate the effectiveness of a ‘Learning from Signals’ (LFS) classifier with Gaussian kernel bandwidth parameters optimally determined using Differential Evolution (DE). The resultant DE-optimized LFS classifier is implemented within an RF ‘Distinct Native Attribute’ (RF-DNA) fingerprinting process with both Time Domain (TD) and Spectral Domain (SD) features input to the classifier. The RF-DNA is used for intra-manufacturer (like-model devices from a given manufacturer) discrimination of IEEE compliant 802.11a WiFi devices and 802.16e WiMAX devices. A comparative performance assessment is provided using results from the proposed DE-optimized LFS classifier and a Bayesian-based Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classifier as used in previous demonstrations. The assessment is performed using identical TD and SD fingerprint features for both classifiers. Preliminary results of the DE-optimized classifier are very promising, with correct classification improvement of 15% to 40% realized over the range of signal to noise ratios considered.

**Index Terms**—Wireless, Security, Fingerprinting, Differential Evolution, Genetic, Algorithm, 4G, 802.16, WiMAX, 802.11, WiFi, Learning from Signals

## I. INTRODUCTION

As fourth generation (4G) communication systems such as last mile Worldwide Interoperability for Microwave Access (WiMAX) and Long Term Evolution (LTE) systems evolve, so does consumer exposure and risk of attack. The relative ease by which ill-intentioned “hackers” access these systems is enabled by a couple factors, including 1) the availability of relatively inexpensive, high power hacking equipment (workstations, servers, etc.) and 2) the fact that these systems fundamentally operate through Wireless Access Point (WAPs)—these are readily accessible and represent one of the most vulnerable points in an Information Technology (IT) network [1].

WAP vulnerability has been traditionally addressed through bit-level security mechanisms in upper Open Systems Interconnection (OSI) layers. For example, a majority of intrusion

detection systems operate at OSI Layer #3, the Network (NET) layer, or higher [2]. While providing some measure of security, these methods generally ignore potentially useful information that is in device Radio Frequency (RF) emissions. Thus, potential security benefits available within the lower OSI Physical (PHY) layer remains largely unexploited.

The task at hand is to exploit PHY information and improve 4G communication security by providing more robust device authentication for mitigating unauthorized system access. The goal is to augment bit-level protection mechanisms using RF air monitoring devices located at network access points [3]–[7]. 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. This application was targeted in [4], [5] for GSM signals and is thought to be directly applicable for similarly configured WiMAX and LTE systems.

Earlier related works demonstrated that RF “Distinct Native Attribute” (RF-DNA) features, as identified using various terminology, are indeed useful for identifying specific wireless devices [3]–[12]. The demonstrated promise of RF fingerprinting has already drawn the attention of counter-measure researchers who are taking the next step of assessing RF PHY layer security robustness [13]. As typically expected with RF signal processing techniques, overall device classification performance with RF-DNA fingerprints decreases as Signal-to-Noise Ratio (SNR) decreases. This is commonly addressed by either finding 1) more robust input features for a given classifier, or 2) a more robust classifier for given input features.

The second of these approaches is considered here using Time Domain (TD) and Spectral Domain (SD) signal features that have been successfully exploited in previous work [3]–[7], [14]. Given these features, the goal is to demonstrate a more powerful “classification engine” that is optimized through Differential Evolution (DE). Success of the resultant DE-optimized “Learning from Signals” (LFS) classifier is measured as either 1) improving device classification accuracy for a given SNR, or by 2) maintaining a given classification accuracy at a lower SNR.

Demonstration of DE-optimized LFS classifier capability is accomplished through comparative assessment of its classification accuracy with that of a Bayesian-based Multiple Discrim-

inant Analysis/Maximum Likelihood (MDA/ML) classifier. Assessment reliability is ensured by inputting *identical* TD and SD fingerprint features into the classifiers. The features are extracted from experimentally collected 802.11a WiFi and 802.16e WiMax 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 [3]–[6] and the greatest opportunity for technical contribution.

The remainder of the paper includes: Section II *Technical Background* on key technical aspects; Section III *Comparative Assessment Methodology* used to obtain results and conduct analysis; Section IV *Results* of classification performance; and Section V *Summary and Conclusions* for accomplishments.

## II. TECHNICAL BACKGROUND

The following subsections provide a summary of key technical concepts that were employed in the methodology to generate desired results. This includes a discussion of RF-DNA Fingerprinting in Section II-A and DE-optimized LFS Implementation in Section II-B.

### A. RF-DNA Fingerprinting

RF-DNA fingerprinting is a PHY technique for uniquely identifying devices based on inherent emission differences. It has been shown that specific serial-numbered devices possess unique characteristics that result from minute differences in manufacturing (part type, part lot number, assembly processes, etc.). The goal here is to use fingerprints of these differences to uniquely identify, by serial number, hardware devices as an aid to network security and user authentication. Various RF fingerprinting techniques have been used previously to demonstrate this for various communication signals, including: 802.11 WiFi signals [3], [7], [15]–[18], GSM cell phone signals [5], [14], 802.16 WiMAX signals [6], 802.15 Bluetooth signals [8], and RFID signals [11], [19].

While these earlier cited works have considered several diverse methods for implementing RF fingerprinting, the techniques generally share some common functionality, including: 1) Signal Collection and Post-Collection Processing, 2) Fingerprint Feature Generation, and 3) Signal/Device Classification. Based on processes in [3]–[5], [7], these functions are collectively embodied in the RF-DNA fingerprinting process overview shown in Fig. 1 and described in the following subsections. This approach was adopted here to facilitate direct comparison of previous MDA/ML classification results with new DE-optimized LFS results to assess the impact of introducing an alternate “Signal Classification Engine.”

#### 1) Signal Collection and Post-Collection Processing:

The first step includes signal reception, digitization, and post-collection processing to prepare the TD signal response for feature extraction. Relative to the process overview in Fig. 1, this includes all processes up to the point where the desired analysis SNR ( $SNR_A$ ) is established and the analysis signal is passed on for statistical fingerprint generation.

All signals considered here were collected using an RF Signal Intercept and Collection System (RFSICS) based on Agilent’s E3238 system [20]. The devices under test were isolated from the RFSICS to minimize the introduction of unrepeatable environmental and interference effects. This is achieved by placing 1) some devices in an RF anechoic chamber, 2) some devices in separate rooms, 3) some RF absorbing material in strategic locations, and/or 4) combinations thereof. Data transfer is easily accomplished using a conventional File Transfer Protocol (FTP) to pass files between devices. When possible, device transmit powers are controlled to enable association of collected data with specific transmitting devices.

Accounting for all collection factors, the post-filtered collected SNR for signals collected under controlled conditions is on the order of  $SNR_C \in [30, 40]$  dB. This enables direct scaling ( $G_N$  in Fig. 1) and addition of like-filtered Additive White Gaussian Noise (AWGN) to generate analysis signals at the desired  $SNR_A$ . The resultant analysis signals are used for RF-DNA fingerprinting and device classification

2) **Fingerprint Feature Generation:** For fingerprint feature generation the input classifier features are either generated directly from the TD signal response or generated in an alternate feature domain through transforming the TD response, e.g., to the frequency domain via a Discrete Fourier Transform (DFT). Transformation is used to exploit additional discriminating features that may be present in an alternate domain. This work considers the collected TD response and DFT-based SD response. In both cases, the final classification features are generated by calculating statistical metrics over selected response regions.

For TD fingerprinting, there are  $N_{SR} = 3$  signal responses, the instantaneous amplitude, phase and frequency. The SD fingerprints are based on the power spectral density and so there is only  $N_{SR} = 1$  signal response. In both cases, the selected response(s) is parsed into  $N_R$  equal length subregions as illustrated in Fig. 2 for representative TD and SD responses of an 802.16e WiMAX signal. Features for the entire response are included as well, yielding a total number of feature regions of  $N_R^F = (N_R + 1)$ . Each of the  $N_{SR}$  signal responses are characterized using  $N_{SM}$  statistical measures of standard deviation ( $\sigma$ ), variance ( $\sigma^2$ ), skewness ( $\gamma$ ), and/or kurtosis ( $\kappa$ ). These statistics are used to form the  $i^{th}$  regional fingerprint given by

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

where  $i = 1, 2, \dots, N_R^F$  and only selected  $\sigma$ ,  $\sigma^2$ ,  $\gamma$ , and  $\kappa$  elements are included. The fingerprints from each region per (1) are concatenated to form the *composite statistical fingerprint* given by

$$\mathbf{F}_C = \begin{bmatrix} F_{R_1} & F_{R_2} & F_{R_3} & \dots & F_{R_{N_R^F+1}} \end{bmatrix}_{1 \times N_F}, \quad (2)$$

where  $N_F$  is the total number of fingerprint features (dimension) input to the classifier and given by

$$N_F = N_{SM} \times N_{SR} \times (N_R + 1). \quad (3)$$

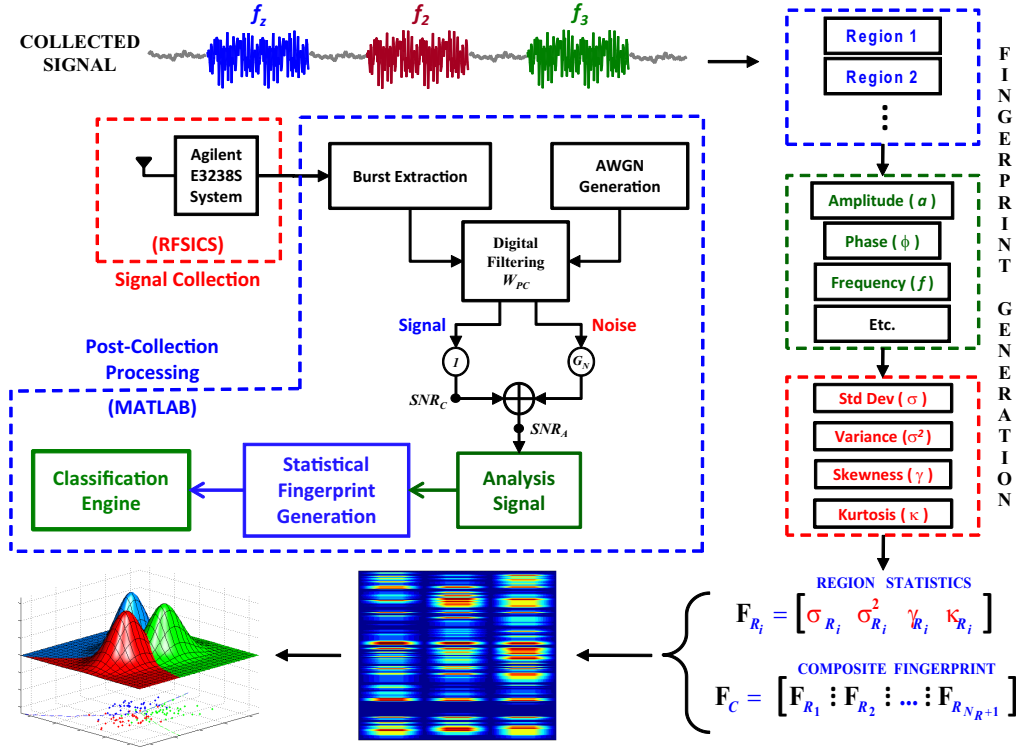


Fig. 1. RF-DNA Fingerprinting Process.

3) **Signal/Device Classification:** For signal/device classification a given classifier is implemented to separate and identify  $N_D$  devices (input classes) using selected input features. Classification approaches vary across the pattern recognition community and generally include methods based on cross-

correlation, vector distance measures, k-nearest neighbor metrics, support vector machines, and Fisher-based MDA/ML processing [3], [6], [8], [19], [21].

As adopted from [3], [5], [14] and used here, 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 ( $\mathbf{W}$ ) to reduce the input dimensionality. The MDA/ML process is that of finding  $\mathbf{W}$  such that projected inter-class separation is maximized and intra-class spread is minimized [22]. 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 multi-dimensional input data classified as being affiliated with 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 class label of the class likelihood yielding the maximum response. For ML classification, the prior probabilities are assumed to be equal and the costs uniform. This is best visualized for the  $N_D = 3$  class problem as illustrated in the lower left-hand corner of Figure 1 that shows Gaussian class likelihood functions and the resultant 2-dimensional decision space (lower surface) with ML boundaries.

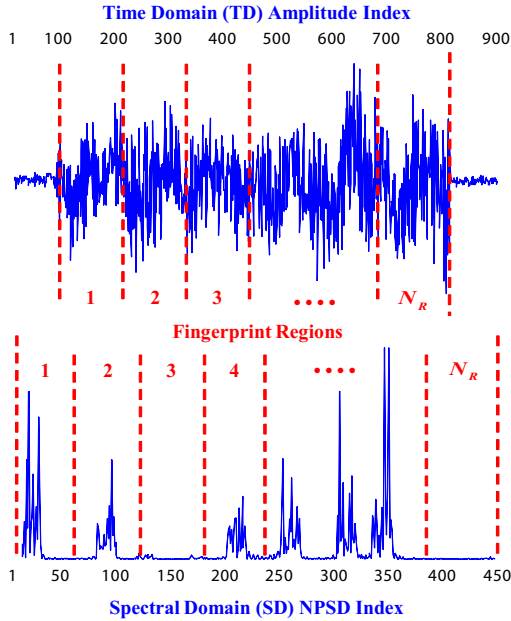


Fig. 2. Fingerprint Feature Regions: TD Amplitude Response and Corresponding SD Response Based on NPSD.

### B. DE-Optimized LFS Classification

The overall DE-optimized LFS classification process is shown in Fig. 3 and functionally includes three steps: 1) Input Data Formatting, 2) DE-Optimized Kernel Regression, and 3) Device Classification. LFS is an adaption of Learning From Data (LFD) techniques where the input training data is derived from samples of a given sensor response [7], [23], [24]. Details for inputting these samples into the LFS classifier are provided in Section II-B1.

The LFD process approximates an unknown system input-output relationship given known available data. Once the data model is “learned” it can be used with previously unseen inputs to approximate the modeled system’s output. The ultimate goal is to find useful information in the input data and exploit it when acting on future observed data [24]. This is done using the DE-optimized kernel regression process detailed in Section II-B2.

Similar to MDA/ML classification in Section II-A3, the DE-optimized LFS process can be used for subsequent device classification. Given a previously unseen input sample  $\mathbf{x}_i = (x_1, \dots, x_{N_F})$  having  $N_F$  feature elements, the LFS model classifies the new sample based on its similarity to previously seen samples.

1) **Input Data Formatting:** Given  $N_D$  devices to be classified, the classifier input data includes  $N_B$  fingerprint vectors per device with each fingerprint containing  $N_F$  features (dimensions) generated per Section II-A2. If perfect model training occurs, i.e., the DE-optimized process produces a model that perfectly represents the input data, the training data would be classified perfectly as illustrated in the upper righthand graphic in Fig. 3. Details for the classification mapping process are presented in Section II-B3.

2) **DE Optimized Kernel Regression:** It has been shown that a genetic algorithm (GA) can be used to improve LFD modeling. The concept is to improve the regression process using a GA to optimize the regularization parameters for each input dimension, rather than using a single, global value for all dimensions. The GA-optimized approach has been applied using more powerful Kernel Regression (KR) techniques [7], [23], [25] and is adopted here for LFS classification.

Unlike conventional linear regression, a local KR function is estimated over the entire input domain by fitting a simple model at every query point. Only observations that are close to the query point are used to fit the model. The local models are built using a distance weighting kernel function,  $K(d^2(\mathbf{x}_i, \mathbf{q}))$ , that assigns a weight based on the distance between the input samples,  $\mathbf{x}_i$ , and query point,  $\mathbf{q}$ . There are many possible kernel functions that could be used, but for demonstration here a multidimensional Gaussian kernel is implemented given by

$$K(d_{\mathbf{H}}^2(\mathbf{x}_i, \mathbf{q})) = \exp^{-0.5 \cdot d_{\mathbf{H}}^2(\mathbf{x}_i, \mathbf{q})}, \quad (4)$$

where  $\mathbf{H} = \text{diag}(h_1, h_2, \dots, h_{N_F})$ ,  $h_i$  is the Gaussian bandwidth parameter for the  $i^{\text{th}}$  dimension ( $i = 1, 2, \dots, N_F$ ), and all off-diagonal elements in  $\mathbf{H}$  are zero. Distance function  $d^2(\mathbf{x}_i, \mathbf{q})$  defines the neighborhood of points around  $\mathbf{q}$ , which is implemented here as the squared Euclidean distance.

DE is a form of GA processing that performs a population-based global search to optimize a given objective function. More specifically, DE is a form of evolutionary strategy, but as with any GA, a group of solutions are retained in the current population which is iteratively updated until specific termination criteria are satisfied. Upon termination, the population member with the best fitness is the one that best optimizes the objective function and it is selected as the solution. Algorithm details for DE processing differ from conventional GA processing primarily in the manner by which future generations are produced [7], [23], [26].

The DE process for this work was implemented using a population of  $N_P$  members, with each member containing a vector of Gaussian bandwidth parameters  $h_i$ ,  $i = 1, 2, \dots, N_F$ . Generation-to-generation fitness is determined using KR and Mean Square Error (MSE) criteria, with termination occurring after either 1) reaching a maximum number of generations  $N_{Gen}$ , or 2) the minimum specified MSE. Vector-based crossover is implemented by crossing each population member (parent)  $X_i$  with three other randomly selected individuals (mates) based on the crossover decision threshold  $CR$ . The child’s final attributes in a given feature dimension is deter-

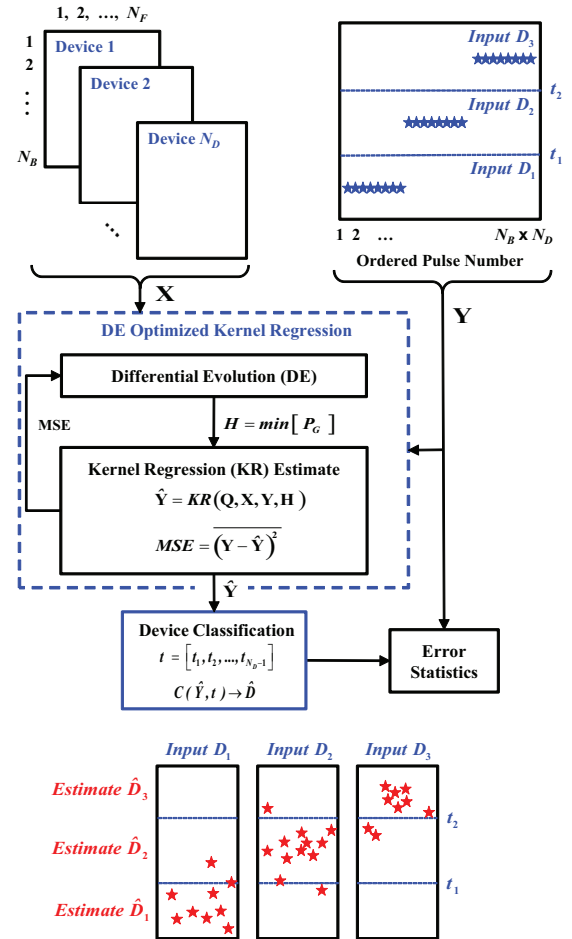


Fig. 3. DE-optimized LFS classification process.

mined using a linear combination of weighted parent and mate differences with multipliers of  $F_1$  and  $F_2$ . The resultant child population contains  $N_P$  members having assigned KR MSE calculated fitness values.

As demonstrated in [7], [23], [25] and used here, KR optimization effectively “learns” the best bandwidth parameter  $h_i$  to use for each dimension and improve LFS classifier performance. One can also infer the relative importance of a given dimension/parameter based on  $h_i$ , i.e., a “smaller”  $h_i$  indicates greater importance as the samples in that dimension have less variance and cluster together to form a tighter neighborhood.

3) **Device Classification:** Device classification in Figure 3 is implemented as a non-linear mapping between the “best”  $\hat{\mathbf{Y}}$  output from the DE-optimized LFS process and possible input devices (classes):  $D \in \{D_1, D_2, \dots, D_{N_D}\}$ . The resultant classification decision is based on learned boundaries defined by threshold values:  $\mathbf{t} = (t_1, t_2, \dots, t_{N_D-1})$ . A comparison of each  $\hat{Y}_i$  in  $\hat{\mathbf{Y}}$  with threshold values in  $\mathbf{t}$  produces a device estimate  $\hat{D}_i$  per the following:

$$\begin{aligned} C(\hat{\mathbf{Y}}, \mathbf{t}) &\rightarrow \hat{\mathbf{D}} \\ t &\in [t_1, t_2, \dots, t_{N_D-1}] , \hat{D}_i \in [D_1, D_2, \dots, D_{N_D}] \\ \hat{Y}_i &\leq t_1 \rightarrow \hat{D}_1 \\ t_j &< \hat{Y}_i < t_{j+1} \rightarrow \hat{D}_j \text{ for } 2 \leq j \leq N_D - 1 \\ \hat{Y}_i &\geq t_{N_D-1} \rightarrow \hat{D}_{N_D} . \end{aligned} \quad (5)$$

The mapping process in (5) is graphically illustrated in the bottom portion of Figure 3 for the  $N_D = 3$  case. These plots indicate less-than-perfect classification performance with the actual *Input* device number shown on the top and resultant *Estimated* device number on the left hand side.

### III. COMPARATIVE ASSESSMENT METHODOLOGY

For reliable comparative assessment, *identical* fingerprint features were generated per Section II-A2 and input to each classifier. This was done for both TD and SD signal responses. The TD signal responses were generated per the method in [3] as centered and normalized instantaneous responses. The SD signal response was generated using the method in [6]—a Fourier-based Normalized Power Spectral Density (NPSD).

The comparison is based on Monte Carlo simulation with both classifiers trained and tested under identical conditions, including: 1) *identical* TD and SD input feature vectors from  $N_B = 500$  bursts per device, 2)  $N_z = 10$  independent like-filtered AWGN realizations per burst at each  $SNR$ , and 3)  $SNR$  increments of  $\Delta_{dB} = 3.0$  dB. It is important to note that *none* of these demonstration parameter values are based on optimal selection criteria. Rather, they were chosen for computational efficiency to enable reliable proof-of-concept demonstration. Optimization and characterization of computational intensity trade-offs between MDA/ML and DE-optimized LFS classifiers remains an area of interest for ongoing research.

The MDA/ML classifier was implemented per Section II-A3 using *K-fold cross-validation* with  $K = 5$  to ensure statistically significant classification results were obtained. The required value of  $K$  can be data dependent and pilot studies confirmed that  $K = 5$  was sufficient to ensure reliability. This value is consistent with common practice that suggests values of  $K = 5$  and  $K = 10$  are appropriate [27].

The DE-optimized LFS classifier was implemented per Section II-B using initial parameter values of  $N_P = 40$  population members, a cross-over threshold of  $CR = 0.2$ , crossover multipliers of  $F_1 : N(0,1)$ ,  $F_2 = 0.8$ , and  $N_{Gen} = 200$  generations. For all results, DE optimization was terminated after reaching  $N_{Gen} = 200$ . This termination strategy differs from conventional DE termination that is generally based on satisfying pre-defined MSE constraints. These initial DE parameter values were empirically determined using a series of pilot studies at a given  $SNR$  and provide consistent classification performance within reasonable computation times.

Classifier performance is first assessed using average % *Correct Classification* versus  $SNR$ , with MDA/ML performance serving as the comparative baseline for subsequent DE-optimized LFS results. This enables a one-on-one assessment of overall “classification engine” power. Performance of the DE-optimized LFS classifier is then analyzed using *Classification Error* versus number of DE generations  $N_{Gen}$  where % *Classification Error* =  $100\% - \text{Correct Classification}$ . This analysis enables efficient selection of  $N_{Gen}$  for achieving a desired % *Correct Classification* while at the same time reducing computation time.

## IV. RESULTS

Classifier assessment results are presented here for each of the OFDM-based signals of interest: 802.11a WiFi in Section IV-A and 802.16e WiMAX in Section IV-B. The presentation order of results and analysis are identical in the sections, with % *Correct Classification* versus  $SNR$  results provided first and followed by *Classification Error* versus  $N_{Gen}$ . A cross-signal assessment is provided at the end.

### A. 802.11a WiFi Devices

Signals for 802.11a WiFi demonstration were collected from 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 collected 802.11a bursts were detected using a simple amplitude detection method with a threshold of  $t_D = -6$  dB. The detected bursts were post-collection filtered using a 6<sup>th</sup>-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 required for  $SNR$  scaling.

For WiFi TD fingerprinting,  $N_{SR} = 3$  signal responses were used (instantaneous amplitude, phase and frequency) with  $N_R = 10$  subregions/response and  $N_{SM} = 3$  statistics/region (variance, skewness and kurtosis). Therefore, the resultant number of fingerprint features (classifier input dimensions) was  $N_F = 99$  per (3). The same number of subregions and

statistics were used for WiFi SD fingerprinting ( $N_{SR} = 1$ ), resulting in  $N_F = 33$  fingerprint features—a three-fold reduction in features relative to TD.

As presented in Fig. 4, 802.11a WiFi device classification is highly dependent on fingerprint type and somewhat unexpected. The DE-optimized LFS classifier with SD input features performs much poorer than 1) the MDA/ML classifier with equivalent input SD features, and 2) itself when using TD input features. Upon further review of simulated conditions, the poorer DE-optimized LFS performance with SD features was initially attributed to the fact that there are one-third fewer SD features than TD features ( $N_F = 33$  SD versus  $N_F = 99$  TD). SD classification performance actually degrades to that of random guessing (33%) for  $SNR \leq 12$  dB.

The DE-optimized LFS classifier provided notable improvement with TD fingerprints and outperformed MDA/ML for  $SNR \leq 15$  dB. This includes greater than 40% classification improvement at the lowest  $SNR$  considered. The anomalous decrease in TD performance at  $SNR = 21$  dB was unexpected and warranted further investigation to determine if this behavior was due to simulation error or inherent in the overall DE-optimized LFS RF-DNA fingerprinting process. This was first addressed by considering the effect of setting the DE termination criteria to a fixed number of generations,  $N_{Gen} = 200$ . Recall that  $N_{Gen}$  is only one of several parameters that were empirically selected for initial proof-of-concept demonstration.

The effect of fixing  $N_{Gen}$  was addressed by considering % Classification Error versus  $N_{Gen}$  for  $N_{Gen} \in [10, 900]$ . The other simulation parameters ( $N_B$ ,  $N_P$ ,  $CR$ ,  $F_1$ ,  $F_2$ , and  $N_z$ ) remained the same as used to generate Fig. 4 results. The % Classification Error results are provided in Fig. 5 for SD fingerprinting at  $SNR = 15$  dB and TD fingerprinting at  $SNR = 21$  dB. As expected, the error exhibits an overall decreasing trend as  $N_{Gen}$  increases, with DE achieving a % Classification Error of approximately 4% for TD and 15% for SD at  $N_{Gen} = 900$ .

Two things are worth noting in Fig. 5. First, the TD response at  $N_{Gen} = 200$  shows % Classification Error  $\approx 12\%$  which corresponds directly to the minimum % Correct Classification  $\approx 87\%$  anomaly in Fig. 4. Therefore, the TD behavior in Fig. 4 is believed to be inherent in the DE-optimized LFS RF-DNA fingerprinting process, i.e.,  $N_{Gen} = 200$  iterations is simply insufficient at some  $SNR$  to realize potential DE-optimized LFS benefits. Second, it appears that SD is asymptotically approaching a lower bound of % Classification Error  $\approx 14\%$ . Investigating the effects of varying  $N_{Gen}$  and other parameters remains an area of interest in ongoing research.

### B. 802.16e WiMAX Devices

Signals for 802.16e WiMAX demonstration were collected from an Alvarion-based test bed that included one Base Station (BS) transceiver (model XTRM-BS-1DIV-5.4-90D) and six like-model Subscriber Station (SS) transceivers (model XTRM-SU-OD-1D-4.9-UL-A). This is commercially available equipment that provides unlicensed operation in two bands:  $f_c \in [4900, 5350]$  MHz and  $f_c \in [5470, 5950]$  MHz [28].

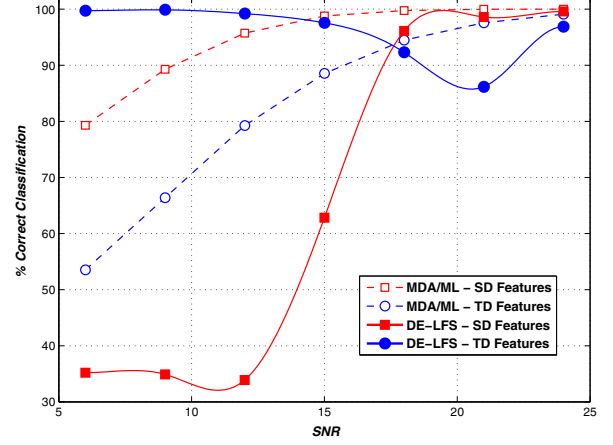


Fig. 4. Average % Correct Classification versus  $SNR$  for the **802.11a** WiFi signal. Results shown for TD (circle markers) and SD (square markers) fingerprint features. Previous MDA/ML classifier (unfilled markers) [3] and new DE-optimized LFS classifier (filled markers) [7].

Consistent with governing IEEE 802.16 standards [29], the experimental system supports channel bandwidths of 5 MHz and 10 MHz. Results here are based on a 5 MHz channel bandwidth at  $f_c = 5475$  MHz with time division duplexing (TDD) providing separation of BS and SS transmissions.

Consistent with the goal of RF air monitoring at WAPs, the WiMAX SS-to-BS transmissions were of interest here. The observed signal structure within each WiMAX TDD frame spanned approximately  $t_{TDD} = 5.0$  ms and included a BS subframe of  $t_{BS} = 3.0$  ms followed by an SS subframe of  $t_{SS} = 2.0$  ms. In addition, the SS subframe contained two distinct responses, with the first response of  $t_{Rng} \approx 300$   $\mu$ s used for ranging (dynamic network maintenance) and the second region used for user data transfer. Considering the various TDD subframe responses that are available for RF-DNA fingerprinting, empirical studies showed that the SS subframe

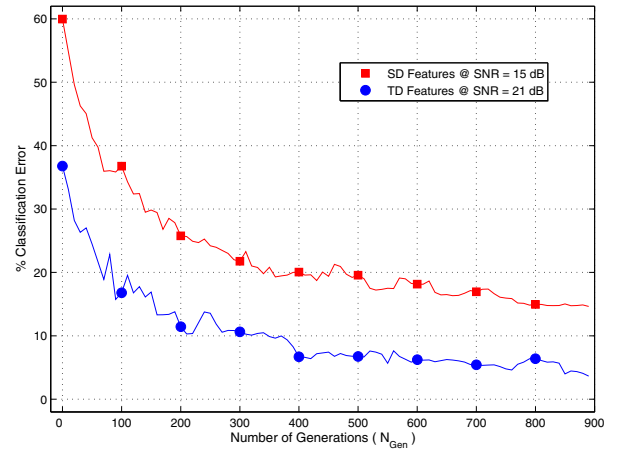


Fig. 5. Average % Classification Error versus Number of DE Generations ( $N_{Gen}$ ) for the **802.11a** WiFi signal using TD features (circle markers) at  $SNR = 21$  dB and SD features (square markers) at  $SNR = 15$  dB [7].



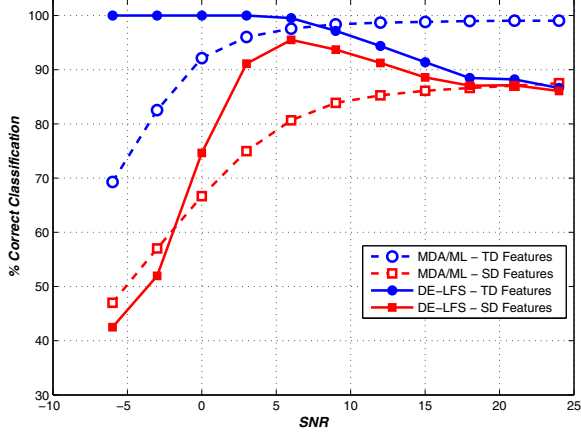


Fig. 6. Average % Correct Classification versus  $SNR$  for the **802.16e** WiMAX signal using the SS *range-only* response. Results shown for TD (circle markers) and SD (square markers) features using the MDA/ML classifier (unfilled markers) and the DE-optimized LFS classifier (filled markers).

*ranging only* was most promising for RF air monitoring and thus it was considered here for demonstration.

The WiMAX signals were collected using the RFSICS and detected using a simple amplitude detection method with a threshold of  $t_D = -12$  dB. Once detected, the SS *ranging only* region of the subframes was extracted and post-collection filtered using a 6<sup>th</sup>-order Butterworth filter having a  $-3$  dB bandwidth of  $W_{PC} = 3.0$  MHz. This same filter was used for generating the like-filtered AWGN required for  $SNR$  scaling.

For WiMAX TD fingerprinting,  $N_{SR} = 3$  signal responses (amplitude, phase and frequency) were used with  $N_R = 12$  subregions per response and  $N_{SM} = 3$  statistics/region (variance, skewness and kurtosis). Therefore, the resultant number of TD fingerprint features (classifier input dimensions) is  $N_F = 117$  per (3). The same number of subregions and statistics were used for WiMAX SD fingerprinting ( $N_{SR} = 1$ ), resulting in  $N_F = 39$  SD fingerprint features—again, a three-fold reduction in features relative to TD.

As presented in Fig. 6, results show that the DE-optimized LFS classifier performed well using WiMAX SS *ranging-only* responses. Most notably, the DE-optimized LFS classifier outperformed the MDA/ML classifier for  $SNR \leq 6$  dB using TD features. In addition, the DE-optimized LFS classifier with TD features yielded nearly 100% *Correct Classification* at lower  $SNR$ , with as much as 30% improvement noted at  $SNR = -6$  dB. DE-optimized LFS classifier was less effective with SD features as classification but outperformed MDA/ML over the range  $0 \text{ dB} < SNR < 15 \text{ dB}$ . As with WiFi device classification, the poorer performance with SD features is partially attributed to the reduces number of features ( $N_F = 39$  SD versus  $N_F = 117$  TD). Future work is planned to address the effects of dimensional TD-SD differences.

As with earlier 802.11a results in Fig. 4, the effect of fixing  $N_{Gen}$  with WiMAX signals was addressed using % *Classification Error* versus  $N_{Gen}$  for  $N_{Gen} \in [10, 900]$ .

The other simulation parameters ( $N_B$ ,  $N_P$ ,  $CR$ ,  $F_1$ ,  $F_2$ , and  $N_z$ ) remained the same. In this case,  $SNR = 18$  dB was used for both TD and SD features. The results of this analysis are presented Fig. 7. As shown, performance with SD features converged very quickly to approximately 13% average % *Classification Error*. The number of generations,  $N_{Gen} = 200$  was clearly sufficient for generating results in Fig.6.

For TD features, the % *Classification Error* versus  $N_{Gen}$  trend in Fig 7 for the WiMAX signal is similar to what was observed in Fig. 5 with WiFi signals, with % *Classification Error* of TD features beginning to approach an asymptotic lower bound of approximately 3% after  $N_{Gen} = 800$  generations. Given this lower bound,  $N_{Gen} = 200$  was not sufficient for maximizing performance at  $SNR = 18$  dB. Clearly, in some cases, increased “learning” through more generations can improve classification performance. The limits of this approach as well as the effects of other parameters on system performance is an area of future research.

## V. SUMMARY AND CONCLUSIONS

This work addresses the use of Differential Evolution (DE) to optimize performance of a Learning From Signals (LFS) classification engine when used for identifying devices using RF “Distinct Native Attributes” (RF-DNA). The DE-optimized LFS classifier is envisioned for use in RF air monitors located at Wireless Access Points (WAPs) in 4G communication systems. As one of the most vulnerable points in an Information Technology (IT) network, the goal is to provide additional Physical (PHY) security at WAPs to augment bit-level mechanisms that are commonly attacked. Of particular interest here are systems based on Orthogonal Frequency Division Multiplexing (OFDM), e.g., existing 802.11a/g WiFi and emerging 4G 802.16 WiMAX and LTE variants.

A comparative classification performance assessment is provided for the DE-optimized LFS classifier relative to

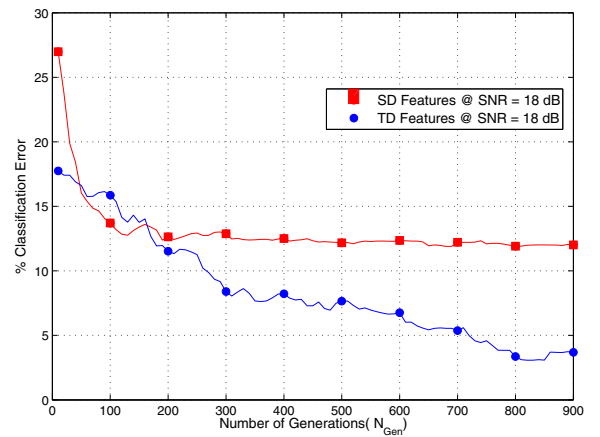


Fig. 7. Average % *Classification Error* versus *Number of DE Generations* ( $N_{Gen}$ ) for the **802.16e** WiMAX signal using TD features (circle markers) and SD features (square markers) both at  $SNR = 18$  dB.

a common Bayesian-based Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classifier. The assessment is performed using *identical* classifier input features extracted from experimentally collected 802.11a WiFi and 802.16 WiMAX signals. The specific features are derived from statistical RF-DNA extracted from both Time Domain (TD) and Spectral Domain (SD) signal responses.

Relative to MDA/ML classification, DE-optimized LFS classification performance was generally superior at lower SNR and provided considerable improvement of over 40% in classification accuracy for some cases considered. This best case classification improvement was realized with TD fingerprint features. While not quite as effective, DE-optimized LFS classification with SD fingerprinting was notable with the difference between TD and SD performance initially attributed to feature dimension differences as there were one-third fewer SD features than TD features.

Analysis based on % Classification Error versus the number of DE generations  $N_{Gen}$  showed that the anomalous behavior of TD and SD fingerprinting at higher signal-dominated SNR, as well as the poorer performance with TD fingerprinting, can be inherent in the DE-optimized LFS RF-DNA fingerprinting process and directly attributable to fixing  $N_{Gen} = 200$  for DE termination. Investigation continues into the effects of varying  $N_{Gen}$  and other parameters that were fixed here for initial proof-of-concept demonstration.

## VI. ACKNOWLEDGMENT

Work sponsored by the Sensors Directorate, Air Force Research Laboratory, Wright-Patterson AFB, OH, and the Laboratory for Telecommunications Sciences, US Department of Defense.

## REFERENCES

- [1] H. Collins, "Top 10 network security threats," *Government Technology*, September 2010.
- [2] T. D. Tarmar 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>
- [3] 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.
- [4] 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.
- [5] M. D. Williams, M. A. Temple, and D. R. Reising, "Augmenting bit-level network security using physical layer RF-DNA fingerprinting," in *IEEE Global Communications Conference*, December 2010.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] —, "Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase." 2003 IASTED Int'l Conference on Wireless and Optical Communications (WOCC), May 2003.
- [10] —, "Using Transceiverprints for Anomaly Based Intrusion Detection." 2004 IASTED Int'l Conference on Communications, Internet and Information Technology (CIIT), November 2004.
- [11] 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>
- [12] B. Danev, T. S. Heydt-Benjamin, and S. Čapkun, "Physical-layer identification of RFID devices," in *Proc of the 18th conference on USENIX security symposium*, ser. SSYM'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 199–214. [Online]. Available: <http://portal.acm.org/citation.cfm?id=1855768.1855781>
- [13] B. Danev, H. Luecken, S. Čapkun, and K. El Defrawy, "Attacks on Physical-Layer Identification," in *Proc of the 3rd ACM Conference on Wireless Network Security*, ser. WiSec'10. ACM, 2010.
- [14] D. Reising, M. Temple, and M. Mendenhall, "Improved wireless security for gsm-based devices using RF fingerprinting," *Int. J. Electronic Security and Digital Forensics*, vol. 3, no. 1, pp. 41–59, Mar 2010.
- [15] 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>
- [16] 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>
- [17] 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>
- [18] 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>
- [19] 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>
- [20] Agilent, *Agilent E3238 Signal Intercept and Collection Solutions: Family Overview*, Publication 5989-1274EN, Agilent Technologies Inc., USA, 2004.
- [21] J. Toonstra and W. Kinsner, "A radio transmitter fingerprinting system ODO-1," in *Electrical and Computer Engineering, 1996. Canadian Conference on*, vol. 1, May 1996, pp. 60 –63 vol.1.
- [22] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern classification*, 2nd ed. Wiley, November 2001.
- [23] 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.
- [24] V. S. Cherkassky and F. Mulier, *Learning from data: concepts, theory, and methods*, 2nd ed. Hoboken, NJ: Wiley & Sons, 2007.
- [25] M. A. Buckner, "Learning from data with localized regression and differential evolution," Ph.D. dissertation, University of Tennessee, Knoxville, May 2003.
- [26] 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.
- [27] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning; Data Mining, Inference, and Prediction*. Springer-Verlag, New York, New York, USA, 2001.
- [28] Alvarion Ltd, *Alvarion BreezeMAX Extreme 5000: WiMAX 16e Pioneer for the License-Exempt Market*, Pub #215373, Rev. A, 2009.
- [29] *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.