3-10-2010

Spectral Domain RF Fingerprinting for 802.11 Wireless Devices

Sheldon A. Munns

Spectral Domain RF Fingerprinting for 802.11 Wireless Devices

THESIS

Sheldon A. Munns, Captain, USAF

AFIT/GE/ENG/10-19

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GE/ENG/10-19

Spectral Domain RF Fingerprinting for 802.11 Wireless Devices

THESIS

Presented to the Faculty
Department of Electrical and Computer Engineering
Graduate School of Engineering and Management
Air Force Institute of Technology
Air University
Air Education and Training Command
in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Electrical Engineering

Sheldon A. Munns, BSEE
Captain, USAF

March 2010

AFIT/GE/ENG/10-19

Spectral Domain RF Fingerprinting

for 802.11 Wireless Devices

Sheldon A. Munns, BSEE
Captain, USAF

Approved:

//signed//	March 17, 2010
Michael A. Temple, PhD (Chairman)	Date
//signed//	March 17, 2010
Steven C. Gustafson, PhD (Member)	Date
//signed//	March 17, 2010
Maj. Michael J. Mendenhall, PhD (Member)	Date

AFIT/GE/ENG/10-19

Abstract

The increase in availability and reduction in cost of commercial communication devices (e.g. IEEE compliant such as 802.11, WiFi, 802.16, Blutooth etc.) has increased wireless user exposure and the need for techniques to properly identify/classify signals for increased security measures. Communication device emissions include intentional modulation that enables correct device operation. Hardware and environmental factors alter the ideal response and induce unintentional modulation effects. If these effects (features) are sufficiently unique, it becomes possible to identify a device using its fingerprint, with potential discrimination of not only the manufacturer but possibly the serial number for a given manufacturer.

Many techniques in many domains have been investigated to extract features, identify a fingerprint, classify signals, and each technique has certain benefits and limitations. Previous AFIT research has demonstrated the effectiveness of RF Fingerprinting using 802.11A signals with 1) spectral correlation on Power Spectral Density (PSD) fingerprints, 2) Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification with fingerprints obtained from Time Domain (TD) and Wavelet Domain (WD) statistical features. Performance "gain", defined as the difference in Signal-to-Noise ratio (SNR) required to achieve comparable classification performance, has been used to demonstrate considerable improvement. Spectral Domain (SD) fingerprinting uses PSD features for device discrimination. Results presented here show some improvement over the WD approach (gain $\approx$ 3 dB) and significant improvement over the TD approach (gain $\approx$ 8 dB).

Acknowledgements

First I owe all that I am to God, for without His constant guidance and blessings in my life I would be lost. I would also like to thank Dr. Temple, my advisor, whose door was always open for lengthy discussions and guidance on my research path. Many an hour have been spent discussing "process" and the importance of terminology when discussing anomalies or results. Following the "process" is what research is about and ultimately what produces results.

I am very thankful for my family, both near and far, who have supported me through this learning endeavor. My lovely wife was consistently supportive throughout our time here at AFIT and especially in the final preparations for the Thesis documentation when many hours were spent writing and reverification of results. She is a wonderful wife and a excellent mother and I am extremely blessed to have her in my life. I would also like to thank my children, who have been patient with all of the time spent without their father present.

Sheldon A. Munns

Table of Contents

Page

List of Figures

Figure Page

List of Tables

List of Symbols

Symbol		Page
$\Phi_{m,r}(k)$	Reference PSD Fingerprints	7
N_T	Collected Training Signals	7
$\Phi_i(k)$	Un-normalized PSD Sequence	7
Prop	Difference in Adjacent FFT Spectra	7
σ^2	Variance	11
γ	Skewness	11
κ	Kurtosis	11
N_R	Number of Regions	20

List of Abbreviations

Spectral Domain RF Fingerprinting

for 802.11 Wireless Devices

I. Introduction

1.1 Motivation

The increase in availability and reduction in cost of commercial communication devices (e.g. IEEE compliant such as 802.11, WiFi, 802.16, Blutooth etc.) has increased wireless user exposure and the need for techniques to properly identify/-classify signals for increased security. Communication device emissions include intentional modulation that enables correct device operation. This intentional modulation may be remotely intercepted, where the interceptor may be passive (listen, monitor, record, analyze, etc.) or become active such as "spoofing" or even inject traffic into the system.

A great deal of research has focused on traditional bit-level algorithmic approaches to mitigate spoofing and improve network security [8]. More recent research has been accomplished to detect and mitigate spoofing within or near the lower levels of the Open System Interconnection (OSI) architecture. One work suggests using a "lightweight security layer" within the Medium Access Control (MAC) layer for anomalous traffic and spoofing detection [8].

The goal of other recent work tries to exploit Radio Frequency (RF) characteristics at the Physical (PHY) layer that are difficult to mimic, thus minimizing spoofing opportunities [13]. The fundamental research goal in [15, 16, 17] involved developing RF fingerprinting techniques to obtain a Specific Emitter Identification (SEI) similar

to that used to distinguish radar emitters [9].

Spanning nearly twenty years, radar SEI uses parameters based on intentional modulation applied within a given pulse (intra-pulse modulation) or applied across multiple pulses (inter-pulse modulation). Hardware and environmental factors such as poor system design, improper operation, and physical device limitation alter the ideal signal response and induce unintentional modulation effects. At the waveform level, these unintentional modulation effects are similar to what occur in existing wireless communication systems that transmit burst-like waveforms representing digital information such as symbols, bits, or packets. If the unintentional modulation effects (features) are sufficiently unique it becomes possible to identify a given device using its fingerprint, with potential discrimination of not only the manufacturer but also serial number for a given manufacturer.

1.2 Problem Statement

The RF fingerprinting process is separated into four phases, including: 1) burst detection, 2) signal region of interest selection and feature extraction, 3) fingerprint generation, and 4) fingerprint classification of unknown received signals. These phases are the basis for many fingerprinting techniques, with each focusing on different signal features in different domains: Wavelet Domain (WD), Time Domain (TD) and/or Spectral Domain (SD).

Many techniques in many domains have been investigated to extract features, identify a fingerprint, classify signals, and each has certain benefits and limitations. This research uses the TD and WD process developed in previous research to correctly classify emissions from Orthogonal Frequency Division Multiplexing (OFDM) 802.11A signals using SD features. The process is then applied to a Direct Sequence Spread Spectrum (DSSS) 802.11B signal.

1.3 Related Research

This research builds on accomplishments from three previous works [1, 5, 15]. The work in [15] focused on detection and identification of GMRS/FRS press-to-talk radios and 802.11A network device RF transmission. The features included instantaneous amplitude, instantaneous phase, and instantaneous frequency. These were used to calculate statistics for feature characterization to identify unique fingerprints. Two methods of classification were used for 802.11A devices: spectral-based correlation which produced classification accuracies up to 74% for SNR = -3 to 6 dB , and Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML)-based classification which produced classification accuracies of 74% to 90% for the same values of SNRs.

The work in [5] explored burst detection techniques to identify the feasibility and repeatability of detecting and locating the start of a waveform burst. Two techniques were utilized: Fractal Baysian Step Change Detector (Fractal-BSCD) and Traditional Variance Trajectory (VT). A newly developed WD fingerprinting technique provided improved performance over previous TD techniques [15, 16, 17], with 2-7 dB of gain improvement realized at 80% classification.

The work in [1] proposed a new transient-based identification method for DSSS 802.15 CC2420 wireless sensor nodes and explored various transformation methods for input data into a Linear Discriminant Analysis (LDA) feature extractor. The transformation that yielded the highest recognition accuracy was based on the relative difference between adjacent Fast Fourier Transform (FFT) spectra. The so called *Prop* method produced recognition results with an Equal Error Rate (EER) as low as 0.24%.

As described in greater detail throughout this document, this research focuses on SD fingerprinting using Power Spectral Density (PSD) fingerprinting features gener-

ated from common statistics (variance, skewness, and kurtosis) to formulate unique fingerprints for signal classification.

1.4 Resources

AFIT provided a number of tools used throughout this research. All signal data were collected using the Agilent®-based RF Signal Intercept and Collection System (RFSICS). The RFSICS consists of the following pieces of equipment: Agilent® E3238s system hardware and an HP Compaq nc8430 laptop computer equipped with the Agilent® E3238s and Vector Signal Analyzer (VSA) software tools. Two Dell laptops were used and equipped with 802.11 wireless cards specified in Table 1.1. All post-processing was accomplished using MATLAB® version 7.7.0 (R2008b).

Table 1.1. Device manufacturer, serial number, and signal type (802.11A and 802.11B) used for generating Chapter 4 results.

Manu	Serial Number / Signal Type			
Cisco	N4U9 / A&B	N4UD / A&B	N4UW / A&B	N4PX / A&B
Linksys	0306 / B	0307 / B	361 / B	
Netgear	0209 / B	0217 / B	273 / B	

1.5 Thesis Organization

Chapter II provides background information on RF DNA fingerprinting, Fisher Linear Discriminant (FLD), Spectral Correlation, Baysian Decision Theory, and MDA/ML classification. Chapter III describes the research methodology and overall process for signal collection, post-collection processing, digital filtering, region of interest selection, SD signal transformation and fingerprint feature generation for MDA/ML classification. Chapter IV presents results obtained from the process discussed in Chapter III for the signals of interest. Chapter V provides conclusions based on results in Chapter IV and suggest areas for further investigation and research. Appendix A

provides a detailed process for RFSICS signal collection as used to obtain all data for this research.

II. Background

2.1 Overview

The material presented in this chapter lays the ground work for the methodology described in Chapter III along with the results presented in Chapter IV. Section 2.2 provides an introduction to RF fingerprinting. Section 2.3 discusses Power Spectral Density (PSD)-based fingerprinting, Section 2.4 discusses Bayes Decision Theory applied to classification, Section 2.5 discusses the feature statistics used to create the statistical fingerprints used for classification, and Section 2.6 provides insight into the Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification method used for generating classification results described in Chapter IV.

2.2 RF Fingerprinting

RF Distinct Native Attribute (DNA) fingerprinting is the process used to identify and classify unique radio transmission characteristics from a device of interest. RF fingerprint classification embodies four phases which include: burst detection, waveform feature generation (amplitude, phase, frequency, PSD), fingerprint extraction, and device classification. Feature extraction determines which domain (time, frequency, or spectral) yields specific signal information (features). Transient start detection is needed to determine where the signal starts for Region of Interest (ROI) selection.

Once the feature and ROI have been selected, statistics (mean, variance, skewness, kurtosis) can be calculated and extracted to determine the unique signal fingerprint. Fingerprint classification determines how well the fingerprint of one device can be identified or differentiated from another device.

2.3 PSD-based Fingerprinting

The PSD describes the distribution of signal power in the frequency domain [14], which is important because it identifies the frequency components having strong or weak variation. Since frequency is derived from a transformation of time responses, frequency domain variation provides alternative time domain processing. Previous work [15, 16, 17] used PSD fingerprints along with spectral correlation for device classification. The process involved generating reference PSD fingerprints $\{\Phi_{m,r}(k)\}$ for each class $m \in M$:

$$\Phi_{m,r}(k) = \frac{1}{N_T} \sum_{i=1}^{N_T} \Phi_i(k), \tag{1}$$

where N_T is the number of collected training signals and $\Phi_i(k)$ is the un-normalized PSD sequence of the ith collection from class m [15]. To eliminate any power bias present from the signal collection process, each reference PSD fingerprint is normalized to unit power.

Classification was accomplished by cross-correlating each PSD with the average reference fingerprint from each class [15, 16, 17]. At a Signal-to-Noise Ratio (SNR) approaching 6 dB, classification accuracies of 74% were achieved using this PSD-based spectral-correlation classification process [15, 16, 17].

Additional spectral-based work in [1] used FFT-based Fisher-features to fingerprint 802.15.4 CC2420 DSSS devices. Several transformation variants were investigated for recognition, and the so-called *Prop* method (difference between adjacent FFT spectra) yielded the highest recognition accuracy.

The feature extraction process in [1] involved extracting the transient part of the signal, where the amplitude of the signal l at time t is $f(t, l)$. Once the transient part

of the signal was extracted, a one-dimensional Fourier transform was calculated:

$$F(\omega, l) = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} f(t, l) exp(-2\pi i \frac{t\omega}{M}), \tag{2}$$

where $0 \leq t \leq M-1$ and M is the number of samples in the transient part of the signal. For the *Prop* method, the relative difference between adjacent FFT spectra in (2) was calculated using

$$\overrightarrow{s_l} = \left[|F(2,l)| - |F(1,l)|, |F(3,l)| - |F(2,l)|, \cdots, |F(\tfrac{M}{2}-1,l)| - |F(\tfrac{M}{2}-2,l)|\right] \tag{3}$$

with the DC component and the redundant half of the spectrum removed [1]. The Fisher-feature is a projection vector $\overrightarrow{g_l}$ extracted from the Fourier spectrum using the LDA matrix W_L, where

$$\overrightarrow{g_l} = W_L^t \overrightarrow{s_l}. \tag{4}$$

The Fisher-feature G for a given device of N captured signals is an array of g_l elements from (4) defined as

$$G = W_L^t S, \tag{5}$$

where S is a matrix such that $S = [s_0..s_1..s_N]$ (4). Finally, a feature template $\boldsymbol{h}$ is used for recognition calculated from the mean vector and covariance matrix of G. Using this process [1] reported results of EER 0.24%, meaning that the recognition system correctly identifies a sensor node with 99.5% accuracy.

2.4 Bayesian Decision Theory

The classification method of Bayesian decision theory [2] takes d-dimensional data belonging to one of c classes of data based on probability densities, prior probabilities, and any costs associated with making a classification decision [2]. Decision boundaries

are defined within the feature space that reduce the probability of misclassification of the input data from the c classes of data. The Gaussian density function is used as the probability model for Bayesian classification given by

$$p(y) = \frac{1}{\sqrt{2\pi}\sigma} exp\left[-\frac{1}{2}\left(\frac{y-\mu}{\sigma}\right)^2\right], \tag{6}$$

where σ is the standard deviation and μ is the mean.

To minimize probability of misclassification, decision boundaries are formed using (6) as the distribution model for the vectors in the feature space. According to Bayes' rule, the posterior probability $P(\omega_j|\mathbf{y})$ is given by a set of c total classes,$\{\omega_1, ..., \omega_c\}$, and a d-dimensional feature vector $\mathbf{y}$ yield the equation

$$P(\omega_j|y) = \frac{p(\mathbf{y}|\omega_j P(\omega_j)}{p(\mathbf{y})}, \tag{7}$$

where class ω_j contain the feature vector, and

$$p(\mathbf{y}) = \sum_{j=1}^{c} p(\mathbf{y})P(\omega_j) \tag{8}$$

contains the conditional probability $p(\mathbf{y}|\omega_j)$ and prior probability $P(\omega_j)$. A decision rule is a goal that lessens the risk associated with making a decision. Assuming that action α_i is taken based on the occurrence of of $\mathbf{y}$ from ω_j, the conditional risk is

$$R(\alpha_i|\mathbf{y}) = \sum_{j=1}^{c} \lambda_{ij} P(\omega_j) \forall i = 1, ..., a, \tag{9}$$

where a is the number of possible action and the cost of choosing ω_i when ω_j occurred is λ_{ij}. The Bayes decision rule chooses the ω_j that minimizes $R(\alpha_i|\mathbf{y})$ for all actions a. To minimize the probability of misclassification and divide the feature space into c regions, $\mathbf{y}$ is assigned to the class with the minimum $R(\alpha_i|\mathbf{y})$, thus reducing the

decision rule to [2]

$$(\lambda_{jk} - \lambda_{kk})p(\mathbf{y}|\omega_k)P(\omega_k) \gtrless_{\omega_k}^{\omega_j} (\lambda_{kj} - \lambda_{jj})p(\mathbf{y}|\omega_j)P(\omega_j), \forall j \neq k. \tag{10}$$

Assuming uniform costs and equal prior probabilities, $(P(\omega_j) = P(\omega_k), \forall j \neq k)$, (10) the result is

$$p(\mathbf{y}|\omega_k) \gtrless_{\omega_k}^{\omega_j} p(\mathbf{y}|\omega_j), \forall j \neq k. \tag{11}$$

A point belonging to ω_j assigned to ω_k registers as a misclassification. The total probability of making a classification error is

$$P_E = \sum_{\substack{j,k \\ j \neq k}} = P\left[\text{Classify as } \omega_j | \omega_k \text{ is true}\right]. \tag{12}$$

The univariate Gaussian distribution presented in (6) is insufficient for multi-class analysis. The multivariate model used for two classes in d-dimensions given by

$$p(y) = \frac{1}{(2\pi)^{\frac{d}{2}} |\sum|^{\frac{1}{2}}} exp\left[-\frac{1}{2}(\mathbf{y} - \mu)^t \sum^{-1} (\mathbf{y} - \mu)\right], \tag{13}$$

where μ is the d-component mean vector, $\mathbf{y}$ is a d-component column vector, and $\sum$ is the $d \times d$ covariance matrix

$$\sum = E\left[(\mathbf{y} - \mu)^t (\mathbf{y} - \mu)\right]. \tag{14}$$

Here the $E[\cdot]$ notation represents the statistical expected value or sample mean. Figure 2.1 shows projected probability densities of the multivariate Gaussian model for a $c = 3$ class problem with $d = 2$ dimensional feature space. As shown projected onto the lower plane, the decision boundaries are used to calculate the total analytic probability of classification error.

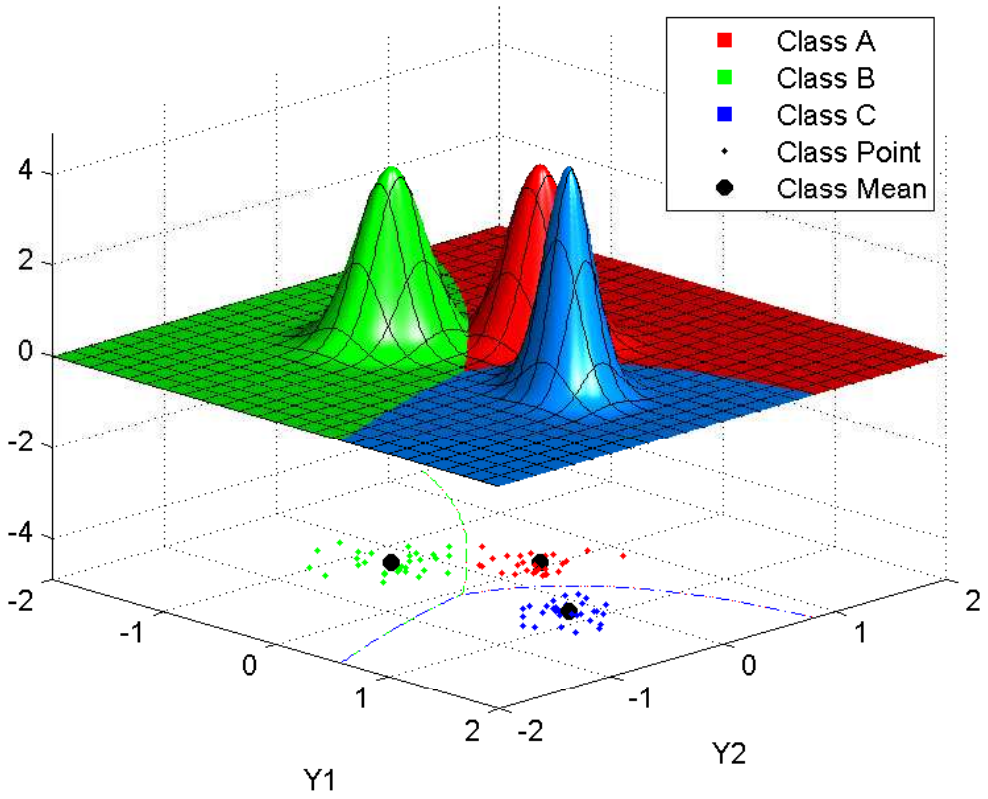


Figure 2.1. Example of the Multivariate Gaussian Model for a c=3 class problem and a d=2 dimensional feature space, where decision boundaries are shown projected onto lower plane.

2.5 Feature Statistics

Using the entire signal characteristic (feature) for the fingerprint, as described in Section 2.3, may be unrealistic if computational processing time or data storage is limited. Previous work [5, 6, 7, 11, 12, 15, 16, 17] made use of statistical behavior inherent in signal characteristics to reduce the dimensionality of the fingerprints. To coincide with previous work in [5, 6, 7], the statistics of variance (σ^2), skewness (γ), and kurtosis (κ) are used here to create statistical fingerprints for classification. These

statistics are obtained as follows:

$$\sigma_x^2 = \frac{1}{N_x} \sum_{k=1}^{N_x} \left[x(k) - \bar{x}\right]^2 \ , \tag{15}$$

$$\gamma_x = \frac{\frac{1}{N_x} \sum\limits_{k=1}^{N_x} \left[x(k) - \bar{x}\right]^3}{\left\{ \frac{1}{N_x} \sum\limits_{k=1}^{N_x} \left[x(k) - \bar{x}\right]^2 \right\}^{3/2}} \ , \tag{16}$$

$$\kappa_x = \frac{\frac{1}{N_x} \sum\limits_{k=1}^{N_x} \left[x(k) - \bar{x}\right]^4}{\left\{ \frac{1}{N_x} \sum\limits_{k=1}^{N_x} \left[x(k) - \bar{x}\right]^2 \right\}^{2}} \ , \tag{17}$$

where x is the sample mean of an arbitrary sequence $\{\mathrm{x(k)}\}$ and $k = 1, 2, ..., N_x$. The final RF statistical fingerprints were obtained in previous work [5, 6, 7, 11, 12, 15, 16, 17] by calculating these statistics from various signal characteristics (instantaneous amplitude, instantaneous phase, and or instantaneous frequency). For work presented here, the PSD statistics are used to form spectral-based fingerprints.

2.6 MDA/ML Classification

While there are many methods for classification, they all fundamentally involve using a subset of the input data to train the classifier and the remaining data for classification itself. Attempting to classify higher-dimensional data becomes difficult without the use of the Fisher Linear Discriminant (FLD), which projects higher-dimensional input data into a lower dimensional space while producing maximum separation between the classes [2].

Although FLD can be applied to any number of inputs, MDA/ML is an extension of FLD for three classes of input data [2, 3]. Discriminating between c classes of input data containing d-dimensions, linearly projecting the input vector $\mathbf{x}$ onto a

(d-1)-dimensional space can be obtained through

$$\mathbf{y} = \mathbf{W}^T\mathbf{x} \ , \tag{18}$$

where the vector of projected values $\mathbf{y}$ corresponds to the input vector $\mathbf{x}$ and the transformation matrix $\mathbf{W}$ has dimensionality $d \times (c - 1)$ [2]. Classification is accomplished using ML distributions to calculate 2-dimensional decision boundaries used on unknown input data. Figure 2.2 pictorially represents the MDA/ML training and classification process, where the decision boundaries are calculated from the ML distributions (top) and the projected data is used for classification (bottom).

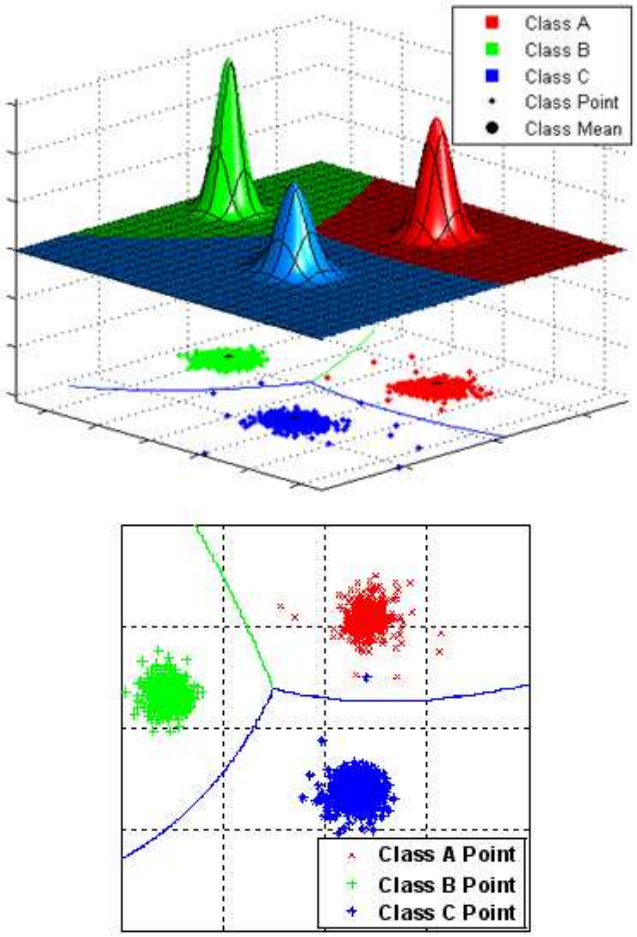


Figure 2.2. MDA/ML Training (top) and Classification (bottom) [5].

III. Methodology

3.1 Overview

This chapter describes signal detection and classification process used for this research. The process here is consistent with previous work [5, 6, 7] and is illustrated in Figure 3.1 [5, 6, 7]. Section 3.2 provides details for the Signal Collection process using AFIT's RF Signal Intercept and Collection System (RFSICS). Section 3.3 describes post-processing collection procedures, which include down-conversion, filtering, burst sorting, and analysis signal generation. Section 3.4 describes the process for RF statistical fingerprint generation, which includes PSD calculation, region of interest selection, and statistical feature calculation. Section 3.5 discusses the MDA/ML signal classification process which was used to generate all classification results presented in Chapter 4.

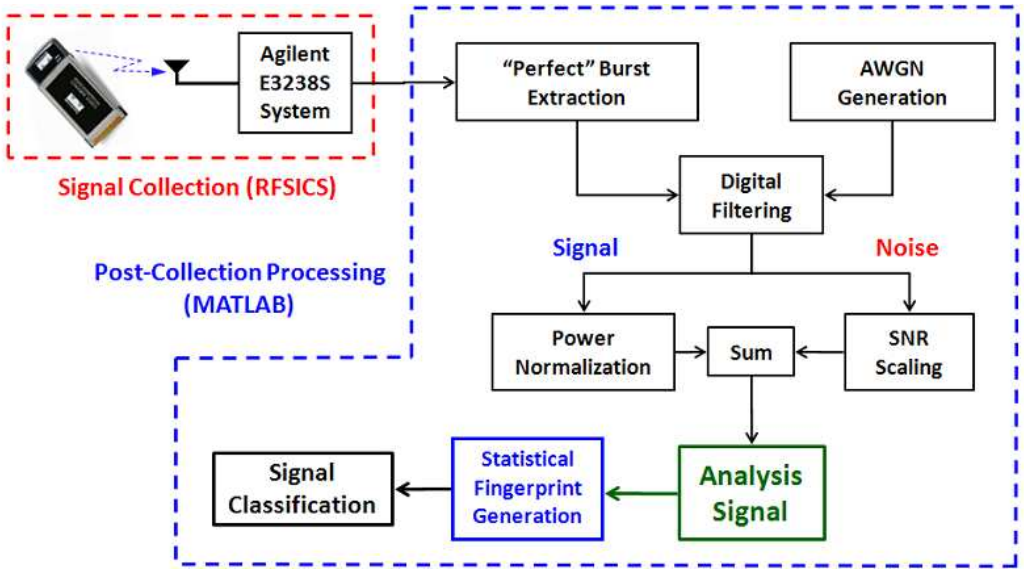


Figure 3.1. Process used for signal collection, detection, analysis signal generation, and classification of 802.11 signals [5, 6, 7].

3.2 Signal Collection

All data used for this research was collected in accordance with the RFSICS collection process outlined in Appendix A. Prior to making collections, two separate laptops were configured as a peer-to-peer network using 802.11 wireless cards. The cards were powered up, set to the appropriate operating mode (802.11A or 802.11B), and information is transferred from one to the other while the RFSICS is operating in collection mode.

The signal-of-interest (SOI) center frequency is located using a wide band search spanning 20.0 MHz and 6.0 GHz. After the SOI is located, the 36 MHz RFSICS front-end filter is tuned and centered on the dominant spectral response. To maximize the collected signal-to-noise ratio (SNR) and to reduce amplitude clipping, the RFSICS Analog-to-digital (ADC) dynamic range is set manually. The signal is then down-converted by the RFSICS, sampled by a 12-bit ADC, and stored as complex I-Q data.

The data is stored using an Agilent® proprietary "capture" (*.cap) format and subsequently converted to a MATLAB® (*.mat) format for post-collection processing. This research only used the real component of collected signals. Representative collected burst responses from 802.11A/B devices are shown in Figure 3.2.

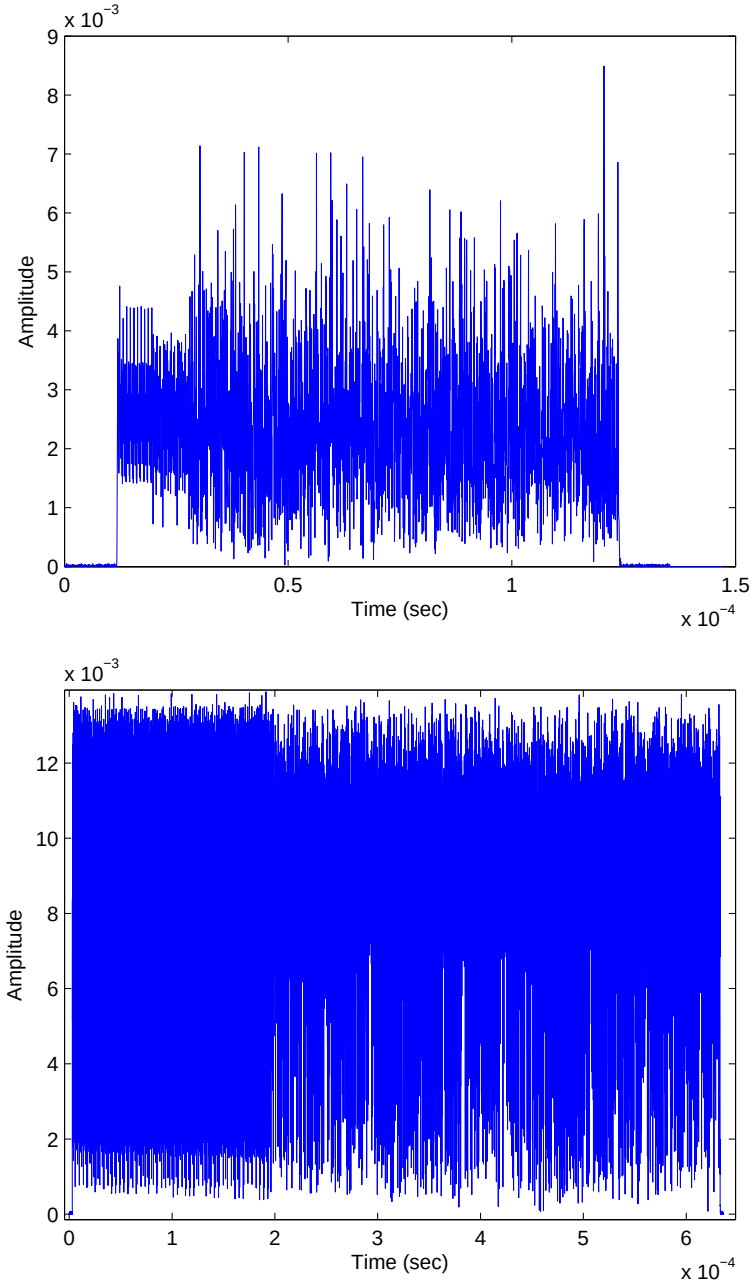


Figure 3.2. Representative magnitude responses for bursts collected from 802.11A (top) and 802.11B (bottom) devices.

3.3 Post-Collection Processing

The MATLAB® (*.mat) formatted data is a vector of sampled data for each burst. Pulse detection and sorting makes it possible for each burst to be examined separately. Each burst is extracted and stacked separately into one row of a given matrix for easy access and examination. Each collected burst response is baseband filtered using a 6th order Butterworth filter having a baseband bandwidth of BW = 7.7 MHz. Previous work [5, 6, 7] showed that BW = 7.7 MHz provides maximum classification performance when using the 802.11A preamble as the region of interest (ROI). After filtering, the preamble region is extracted and stored in a new matrix for subsequent fingerprint generation.

3.3.1 Pulse Detection and Sorting.

Collections of 802.11 data are initially in vector form, where each burst is extracted and placed into row matrix form. A pulse detection algorithm is used with adjustable characteristics (desired detection threshold, minimum/maximum length, number of bursts, smoothing factor) to extract and sort each burst and placed into a matrix. These adjustable characteristics are used since not all bursts in the collection fit the criteria (minimum/maximum length). The algorithm first smooths (averages) over a given number of samples, specified as the smoothing factor. It then detects a burst at the desired detection threshold value (t_D = -3 dB) and locates this point at both ends of the burst. Finally, it checks to see if the burst is wider than the minimum value but narrower than the maximum value. This process produces a matrix where all undesirable bursts have been removed, leaving bursts meeting the criteria for further post-processing. Figure 3.3 illustrates the process over a small region of the original 802.11B collected data.

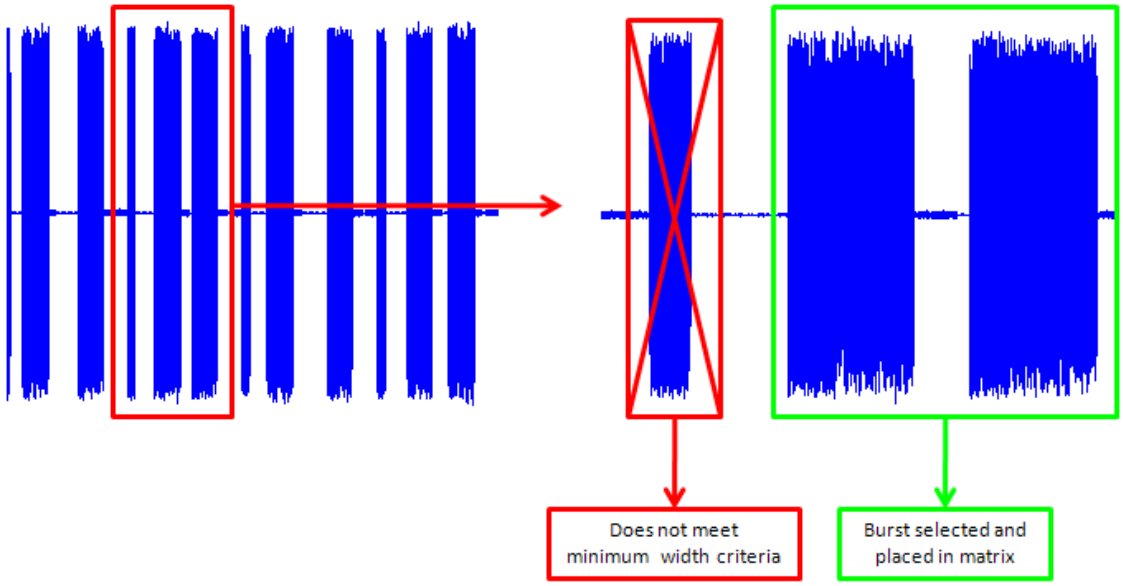


Figure 3.3. Representation of the burst extraction process, where a burst having insufficient width is rejected and bursts meeting pulse width criteria are placed in a matrix for post collection processing.

3.3.2 Preamble Region Extraction and Filtering.

According to 802.11A signal specifications, the preamble region contains information at the beginning of each burst to aid in diversity selection, timing/frequency acquisition, and channel estimation [4]. Figure 3.4 shows the preamble region of the 802.11A signal.

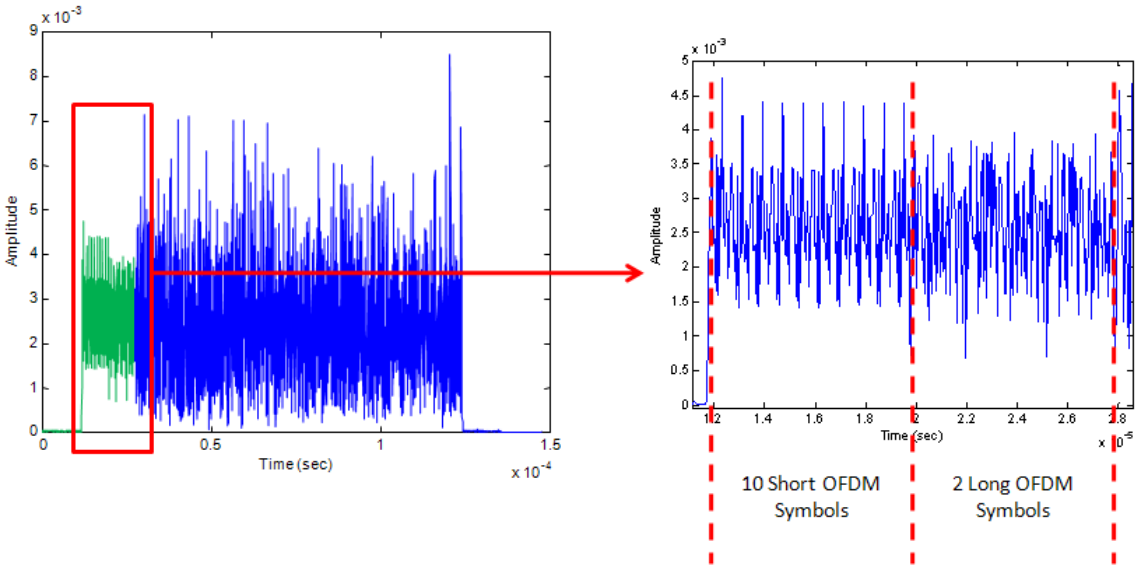


Figure 3.4. Representation 802.11A signal with preamble region highlighted (left) with structure (right).

3.4 Statistical Fingerprint Generation

Once the signal preamble region is filtered and extracted, the bursts are used to calculate statistical RF fingerprints that are input to the MDA/ML classification process. The PSD feature is first calculated and normalized according to (21). The DC component and redundant half of the data are removed. Regional variation analysis is then used to determine a specific number of regions (N_R) for subdividing the PSD feature. Consistent with previous work, the statistics of interest here include variance, skewness, and kurtosis. These features are calculated over each PSD region that makes up a fingerprint matrix which is input to the MDA/ML classification process.

3.4.1 Power Spectral Density (PSD) Calculation.

The PSD is obtained through the discrete Fourier transform (DFT) of a complex sequence $\{x(n)\}$,

$$X(k) = \frac{1}{N_x} \sum_{n=1}^{N_x} x(n) exp \left[-j(\frac{2\pi}{N_x})(n-1)(k-1) \right] \tag{19}$$

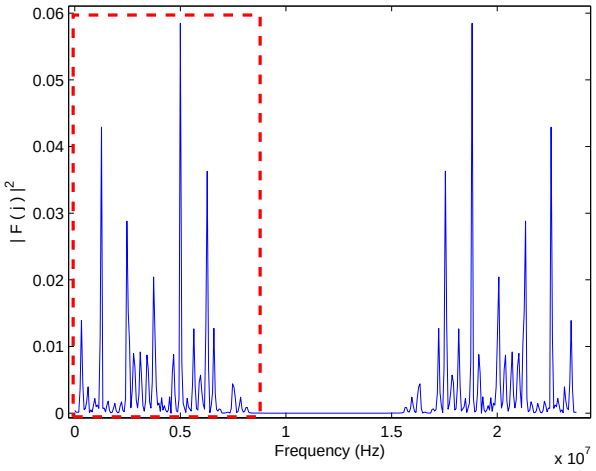
where $n = 1, 2, ..., N_x$ [10]. To reduce potential amplitude bias from the collection process, the normalized PSD is calculated. First, the total average power is calculated using

$$X_p = \frac{1}{N_x} \sum_{k=1}^{N_x} x(k) x^*(k), \tag{20}$$

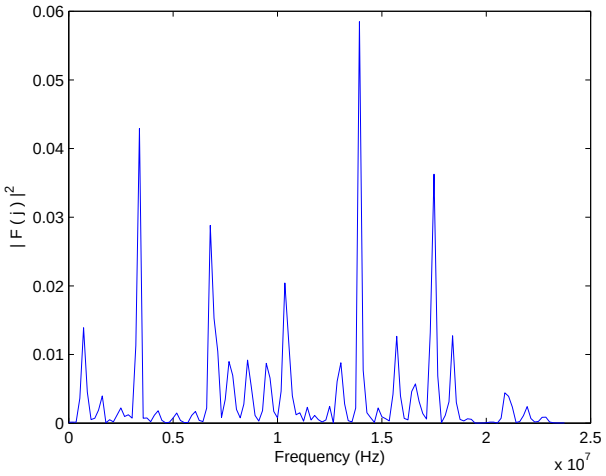
where $*$ denotes complex conjugate and N_x is the total number of samples. The expression in (20) along with the PSD expression in (19) is used to form the normalized PSD given by

$$\phi_x(k) = \frac{1}{X_p} |X(k)|^2 = \frac{1}{X_p} \{ Re^2 [X(k)] + Im^2 [X(k)] \}. \tag{21}$$

The DC component ($k = 0$) is removed, and the redundant half discarded ($k = 1, 2, ..., \frac{N_x}{2}$) to form statistical fingerprints. Figure 3.5 shows the calculated normalized PSD (Figure 3.5(a)) for an 802.11A signal from Figure 3.2 using (21) along with the portion (Figure 3.5(b)) used for fingerprint generation (DC component and redundant half removed, highlighted in Figure 3.5(a)).



(a) PSD of preamble region



(b) Redundant half of PSD (a) removed

Figure 3.5. Representative PSD responses (a) and portion (highlighted) used for fingerprint generation with redundant half removed (b).

3.4.2 Region Selection and Feature Calculation.

Region selection is based on analyzing the output of the classification process with the collected SNR = 40 dB and N_R varied from 3 to 21. Figure 3.7 shows classification performance for N_R variation at 40 dB. These results indicate that N_R = 13 is optimal and thus $N_R = 13$ was used for all 802.11A results presented in Chapter 4. The selected value N_R = 13 is used to subdivide (Figure 3.7) the preamble PSD

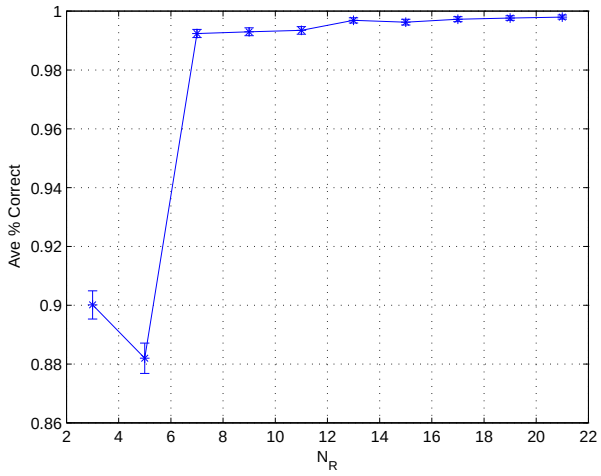


Figure 3.6. Classification performance versus number of regions (N_R) for SNR = 40 dB with N_R = 13 selected and used for all 802.11A results.

into 12 subregions which are then used to calculate the statistics for each region. The statistics for the entire preamble PSD are also calculated and appended at the end of the matrix to form an N_R = 13 regions with 12 subregions. For consistency with previous research on 802.11A data [5, 6, 7], the statistics of variance (σ^2), skewness (γ), and kurtosis (κ) are calculated over each region to form the statistical fingerprint as illustrated in (22). This process is repeated for each burst, then placed into a fingerprint matrix that is input into the classification process. Using the expression

in (22) with $N_R = 13$ regions, the fingerprint matrix

$$F_{R_i} = \left[\sigma_i^2 \ \gamma_i \ \kappa_i\right]_{i=1...N_R} \Rightarrow [F_{R_1} F_{R_2} ... F_{R_i}] \tag{22}$$

that is input to the Fisher Training Process represents 39-dimensional data (1 PSD Feature $\times$ 13 Regions $\times$ 3 Statistics).

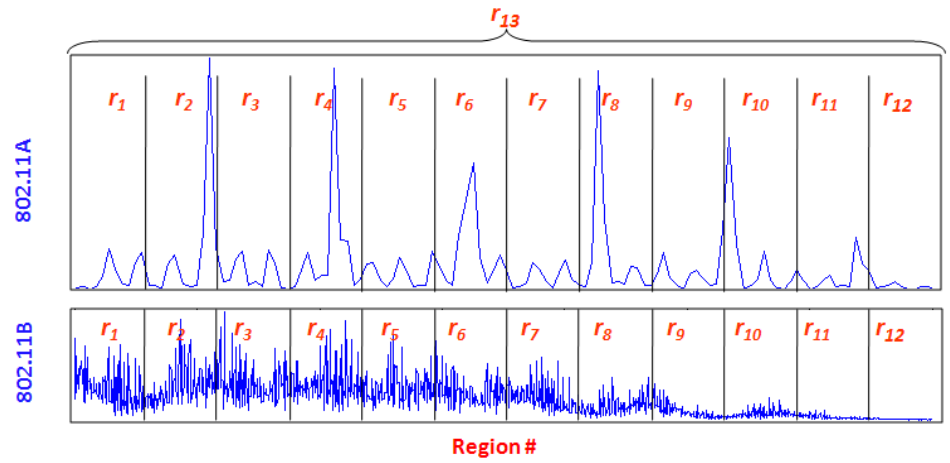


Figure 3.7. Subdivision of PSD in Figure 3.5 into $N_R = 13$ total regions for feature calculation.

3.5 Signal Classification

The 39-dimensional fingerprint data obtained from Section 3.4.2 is input to the MDA/ML training and classification process. The input data is calculated for three different classes, where each class represents bursts from a specific 802.11 device. Following the training process, signal classification is implemented as described in Section 3.3. Monte Carlo simulation (noise generation, scaling and addition) and K-fold cross validation are used in the MDA/ML signal classification process. Monte Carlo simulation ensures statistical significance of data by running the event multiple

times, while K-fold cross validation randomly partitions the original data into K blocks with K-1 blocks used for MDA/ML training and the remaining block used for ML classification. The overall process for MDA/ML training and classification is shown in Figure 3.8 [18].

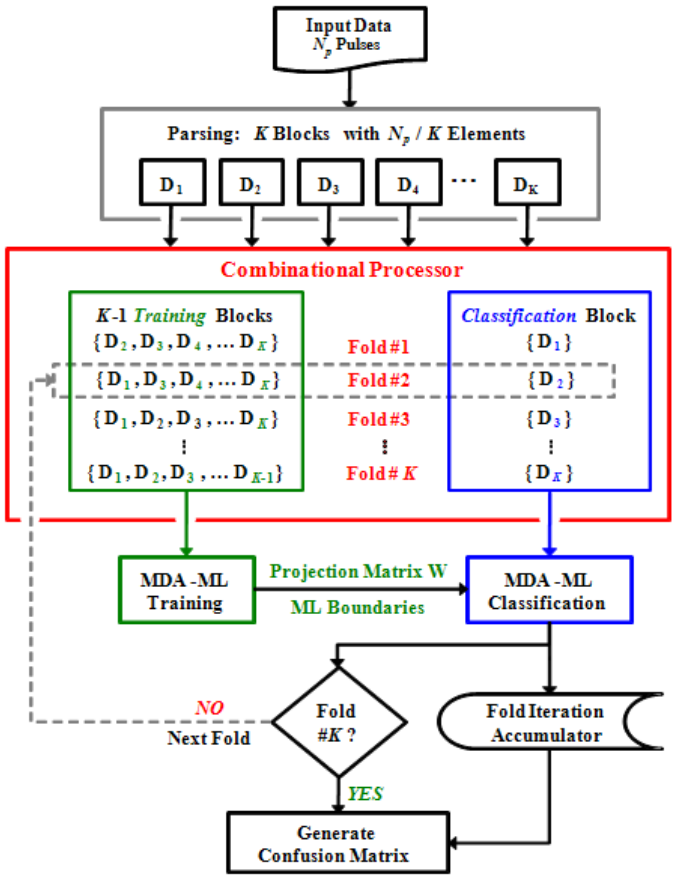


Figure 3.8. MDA/ML classification process with K-fold cross validation [18].

IV. Results and Analysis

4.1 Overview

This chapter provides results and analysis of classification performance for 802.11A/B signals based on processes outlined in Chapter 3. This research follows previous work [5, 6, 7, 11, 12, 17, 16, 15] for OFDM 802.11A signals using a PSD-based transformation. The process for 802.11A signals is repeated for DSSS 802.11B signals to see how well other signals can be identified and classified. This chapter includes a section for 802.11A SD performance results and comparison with WD and TD taken from [5, 6, 7], a section for 802.11B SD performance results including the *Prop* method discussed in [1], and finally a section for comparing 802.11A results with those of 802.11B.

4.2 SD Performance: 802.11A signals

Intra-manufacturer discrimination follows previous research [5, 6, 7] using four Cisco devices transmitting 802.11A signals, where the permutations are shown in Table 4.1. These are like-mode devices from the same manufacturer (Cisco) and only differ in serial number. It is assumed that they have been manufactured under identical environmental conditions, from identical lots, using identical components, with identical processes. Intra-manufacturer classification is generally the most difficult (as compared with inter-manufacturer) due to the devices having similar physical properties, varying slightly due to the make of the device (serial number discrimination).

Table 4.1. 802.11A Cisco intra-manufacturer permutations [5, 6, 7].

	Serial Number			
Perm	N4U9	N4UD	N4UW	N4PX
1	×	×	×	
2		×	×	×
3	×		×	×
4	×	×		×

According to results in [5, 6, 7], Permutation #1 presented the "most stressing" condition for classification and yielded poorest performance for all SNR = -3 to 40 dB. Figure 4.1 results are taken directly from [5, 6, 7] and illustrate intra-manufacturer classification accuracy for all four permutations in Table 4.1 using previous TD and WD fingerprinting techniques. As shown, Perm #1 reflects the poorest performance for both techniques. Considering permutation averages, WD provides approximately 6 dB of "gain" at 80% classification accuracy.

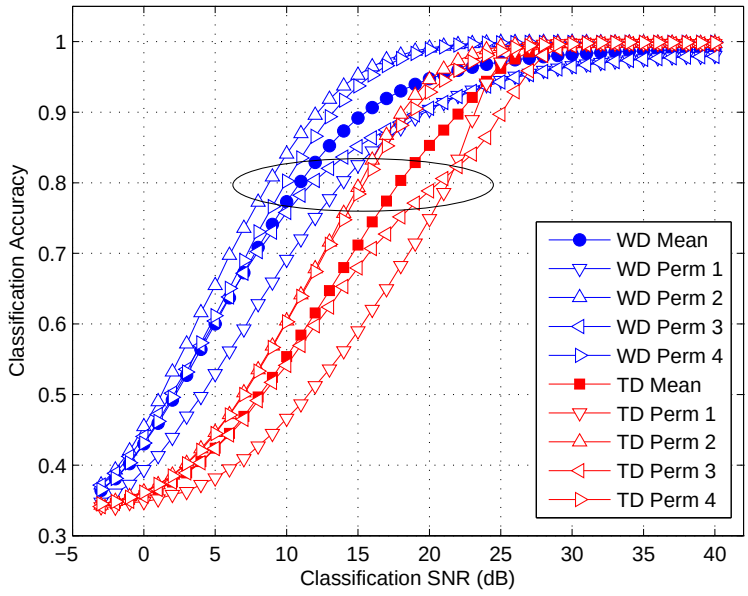


Figure 4.1. Intra-Manufacturer MDA/ML Classification using TD and WD fingerprints: All Permutations for Cisco devices transmitting 802.11A signals. Figure and results taken directly from [5, 6, 7].

Figure 4.2 shows new SD classification results for all four Cisco permutations in Table 4.1. The mean across all permutations is shown with filled markers. These results demonstrate that Permutation #1 and Permutation #3, both of which contain serial numbers N4UD and N4UW, present the most stressing cases of the four permutations. As with previous TD and WD results in [5, 6, 7], Perm #1 is again the "most stressing" case for most SNRs considered.

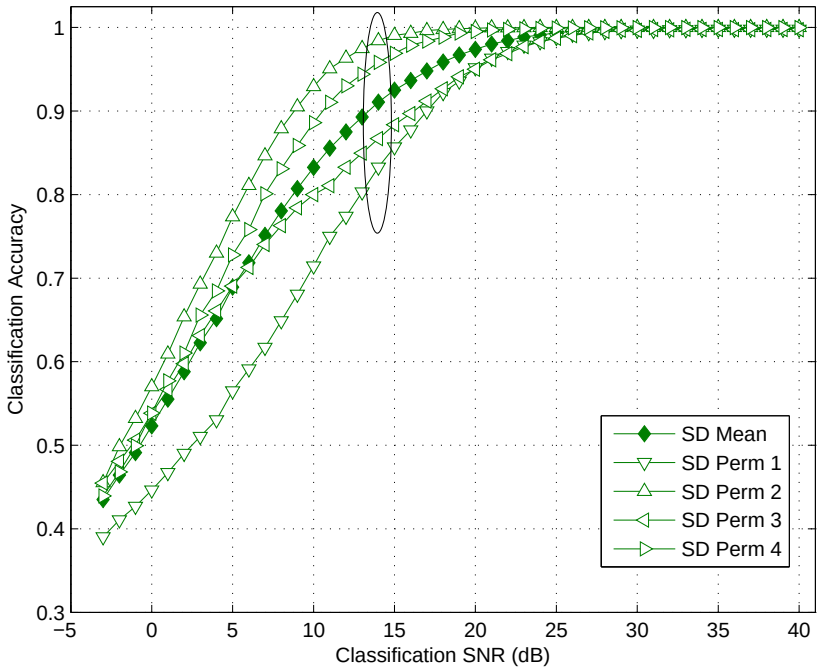


Figure 4.2. Intra-Manufacturer MDA/ML Classification using SD fingereprints: All Permutations for Cisco devices transmitting 802.11A signals.

Table 4.2 provides classification confusion matrices for Perm #1 of the Cisco devices for signals at $SNR = 14$ dB. Results for TD and WD are taken directly from [5, 6, 7] and provided for comparison. Classification accuracies for a specific class (device) are presented along the diagonal. The lower two matrices demonstrate performance differences between SD and TD/WD, respectively. SD provides improved performance over TD across all three devices, with greatest improvement of 28.5%

achieved for correctly classifying Class A. SD provides some improvement over WD for correctly classifying Class A (8.4%) and Class C (0.8%), and some degradation in classifying Class B.

Table 4.2. Intra-manufacturer confusion matrices for SD, TD and WD fingerprinting: Permutation #1 from Table 4.1 with 802.11A signals at $SNR = 14$ dB. (TD and WD results from [5, 6, 7]).

SD	Class Estimate		
Input Class	A	B	C
A	**77.9%**	5.2%	16.9%
B	6.0%	**93.9%**	0.1%
C	21.7%	0.3%	**78.0%**

TD	Class Estimate		
Input Class	A	B	C
A	**49.4%**	17.3%	33.3%
B	18.5%	**65.9%**	15.6%
C	34.2%	12.1%	**53.6%**

WD	Class Estimate		
Input Class	A	B	C
A	**69.5%**	5.9%	24.5%
B	5.3%	**94.0%**	0.7%
C	21.5%	1.3%	**77.2%**

SD - TD	Class Estimate		
Input Class	A	B	C
A	**28.5%**	-12.1%	-16.4%
B	-12.5%	**28.0%**	-15.5%
C	-12.5%	-11.8%	**24.4%**

SD - WD	Class Estimate		
Input Class	A	B	C
A	**8.4%**	-0.7%	-7.6%
B	-0.7%	**-0.1%**	-0.6%
C	0.2%	-1.0%	**0.8%**

Figure 4.3 shows average classification results across all four permutations for the three fingerprint generation methods WD, TD and SD, as taken from Figure 4.1 and Figure 4.2. At 80% classification accuracy, SD outperforms TD and provides a gain of approximately 8 dB. While the SD performance is generally consistent with WD performance, there is some statistical improvement (1%-3%) for SNR = -3 to 25 dB.

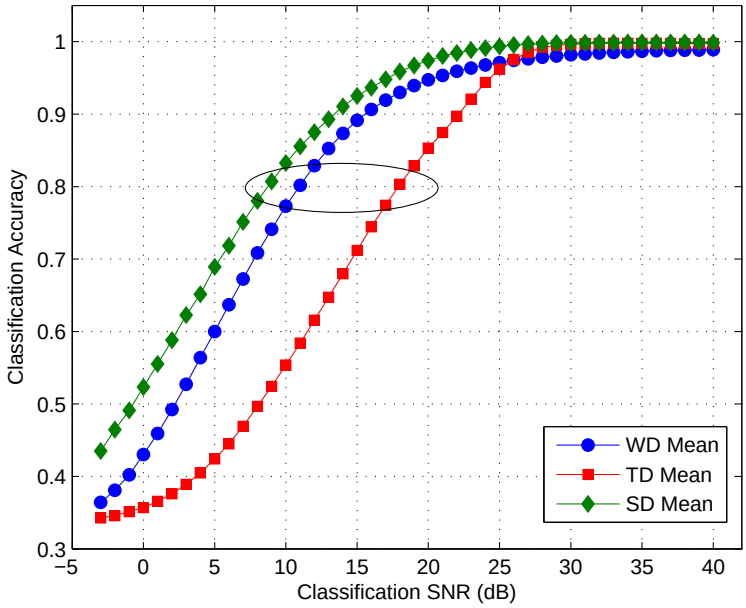


Figure 4.3. Intra-Manufacturer MDA/ML Classification: Average performance across all four permutations of four Cisco devices transmitting 802.11A signals. TD and WD results from 4.1 and SD results from 4.2.

In operational situations where equipment may not be co-located, or operates in dissimilar environments (such as laboratory equipment) or when aligned at the 3db point of the collected signal, the collected signals and burst start location can be affected. This effect is referred to here as timing "jitter". When the collected signals are aligned "perfectly", or at the approximate identical sample number, the effect is referred to as "perfect". The "jitter" effect on classification performance is illustrated in Figure 4.4, where the signals were detected using a t_D = -3 dB threshold.

The "jitter" effect can be seen in Figure 4.5, which overlays the "perfect" align-

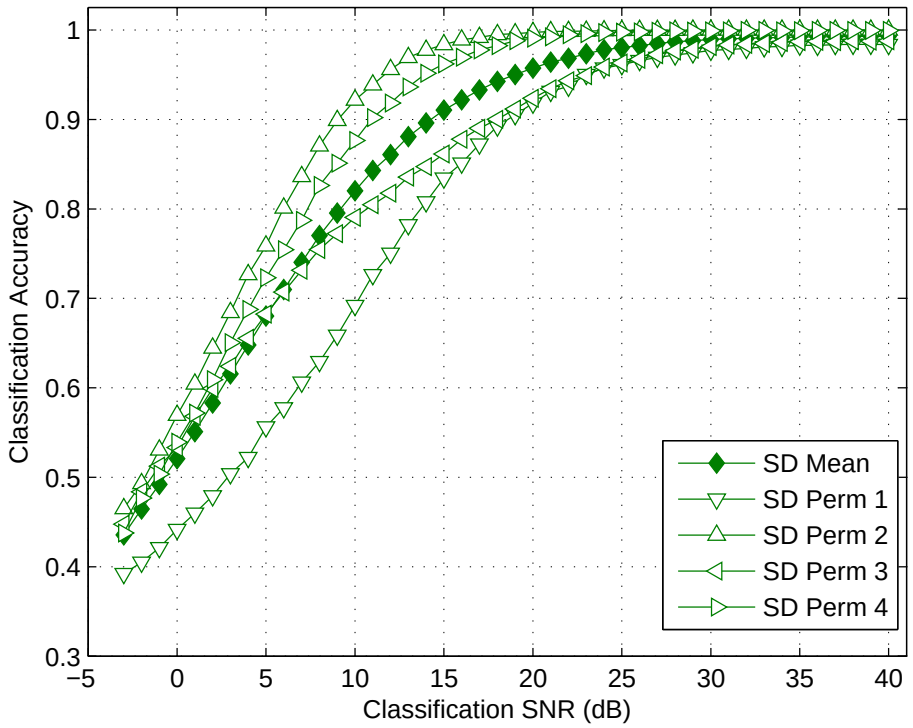


Figure 4.4. Intra-Manufacturer MDA/ML Classification: "Jittered" Classification Performance using all Permutations for Cisco devices transmitting 802.11A signals.

ment with that of the "jittered" collections. As can be seen, the effect at higher SNR values is more susceptibility to jitter than the lower SNR values, where the "jittered" results show minimal degradation. Intra-manufacturer classification results for all three fingerprinting methods (TD, WD, and SD) for observed burst location error "jitter" using Perm #2 from Table 4.1 are shown in Figure 4.6, where performance for TD and WD were taken directly from [5, 6, 7]. Results in Figure 4.6 also demonstrate SD performance improvement over TD and further show that SD is less susceptible to "jitter". The results reflect that the TD technique is susceptible to phase shift while the WD and SD are not.

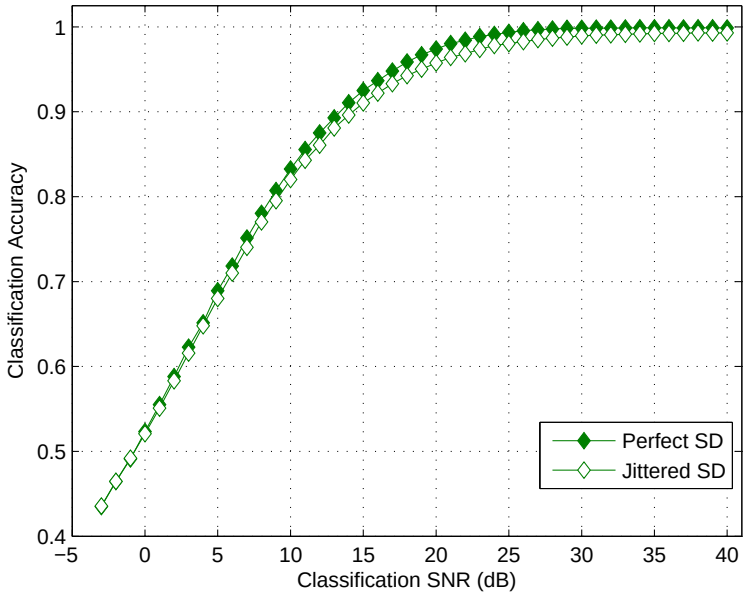


Figure 4.5. Average MDA/ML Classification accuracy for 802.11A intra-manufacturer discrimination using average "perfect" results from Figure 4.2and average "jittered" results from Figure 4.4.

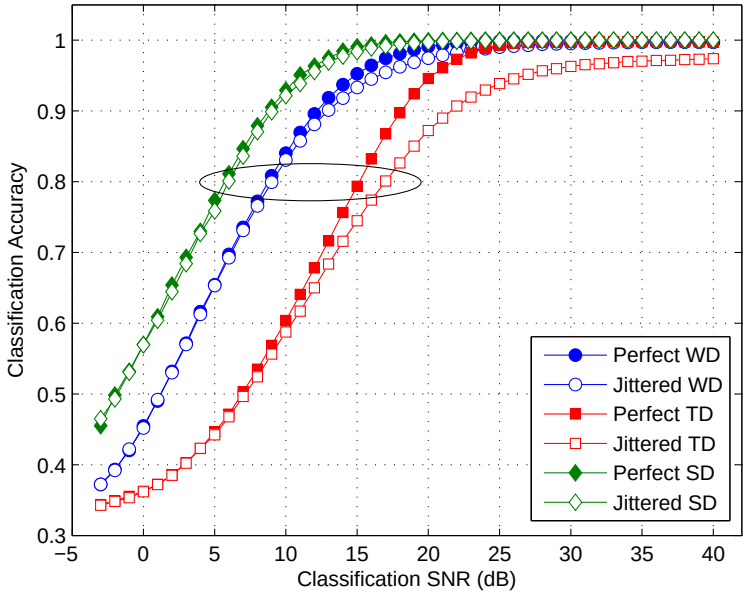


Figure 4.6. Average MDA/ML Classification: Comparison of "perfect" and "jittered" 802.11A intra-manufacturer discrimination using *observed* burst location error statistics. TD and WD results taken directly from [5, 6, 7].

4.3 SD Performance: 802.11B signals

This section is divided into two subsections and presents results on intra/inter-manufacturer performance using devices transmitting 802.11B signals. Intra-manufacturer discrimination follows Section 4.2 with devices transmitting 802.11B signals for all permutations and worst case Perm #1 shown in Table 4.1. To investigate and compare intra-manufacturer performance between manufacturer, three devices from each Linksys and Netgear were used as well as the three Cisco devices to see how well serial number discrimination can be performed using the SD fingerprint method. Table 4.3 shows all devices (used for 802.11B inter-manufacturer discrimination where the permutations are shown with the "×"s in the table).

Table 4.3. 802.11B inter-manufacturer permutations.

	Serial Number								
Manufacturer	Cisco			Linksys			Netgear		
Perm	N4U9	N4UD	N4UW	306	307	361	209	217	273
1	×			×			×		
2		×			×			×	
3			×			×			×

4.3.1 802.11B Intra-Manufacturer Performance.

Intra-manufacturer discrimination was performed using devices transmitting 802.11B signals for all four Cisco devices shown in Table 4.1 as well as all three Netgear and all three Linksys devices shown in Table 4.3. Figure 4.7 shows classification performance for all permutations, where the mean is shown with filled markers.

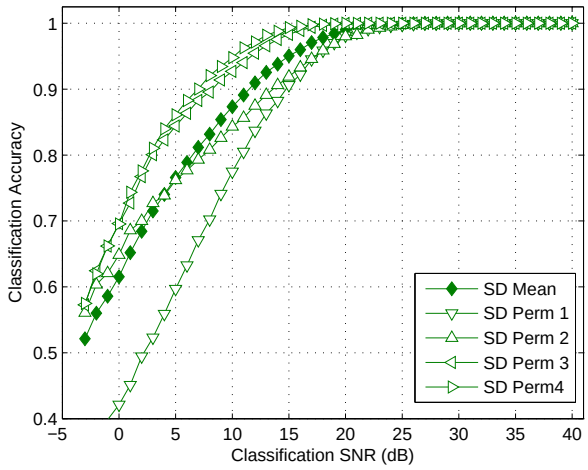


Figure 4.7. Intra-Manufacturer MDA/ML Classification using SD fingerprints: All Permutations for Cisco devices transmitting 802.11B signals.

Figure 4.8 shows classification performance using Cisco Perm #1 as well as all three devices for Linksys and Netgear shown in Table 4.3. As can be seen, the Cisco and Linksys devices are consistent, while the Netgear has a slight increase in performance. Since this is intra-manufacturer discrimination, the results indicate that the Netgear performance is actually poorer compared to the Cisco and Linksys results, because similar devices should be confused more with each other and performance degraded.

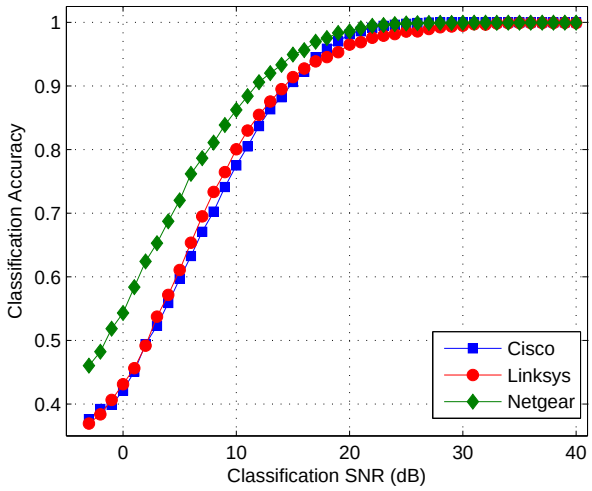


Figure 4.8. Intra-Manufacturer MDA/ML Classification using SD fingerprints: Three devices per manufacturer with serial numbers listed in Table 4.3 with devices transmitting 802.11B signals.

4.3.2 802.11B Inter-Manufacturer Performance.

Inter-manufacturer discrimination was performed using permutations in Table 4.3. Results for three permutation are illustrated in Figure 4.9. Perm #2 and Perm #3 demonstrate consistent results. At 80% classification accuracy, Perm #1 provides a gain of approximately 3 dB over Perms #2 and Perm #3.

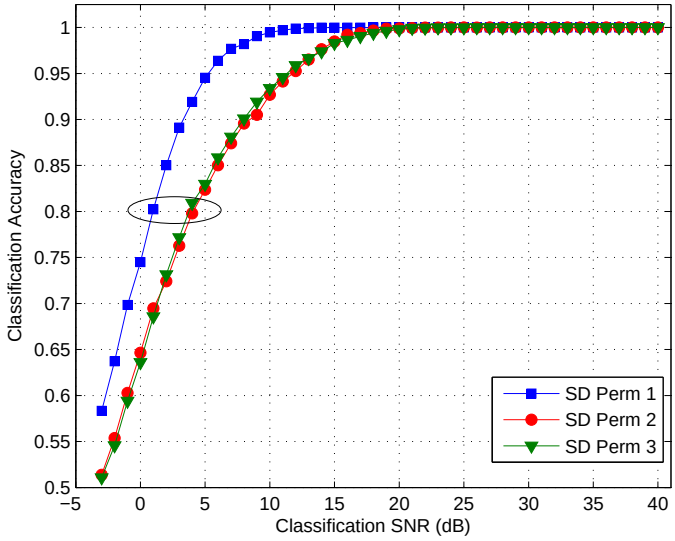


Figure 4.9. Inter-Manufacturer MDA/ML Classification using SD fingerprints: Permutations from Table 4.3 with devices transmitting 802.11B signals.

4.3.3 802.11B Prop Method Performance.

Work in [1] for DSSS-based 802.15.4 CC2420 devices used a *Prop* method (difference in adjacent FFT spectra) that provided the highest recognition accuracy of 99.5%. Figure 4.10 illustrates Perm #2 (top) and Perm #3 (bottom) of the inter-manufacturer permutations overlayed with their respective *Diff* method results. As can be seen, performance is consistent with the standard SD method. The results for Perm #2 (Figure 4.10 bottom) indicate that the *Prop* method achieves slight improvement from SNR = 4 to 15 dB, while the *Prop* method performance is poorer (approximately 2-3 dB) using the devices for Perm #3 (Figure 4.10 bottom).

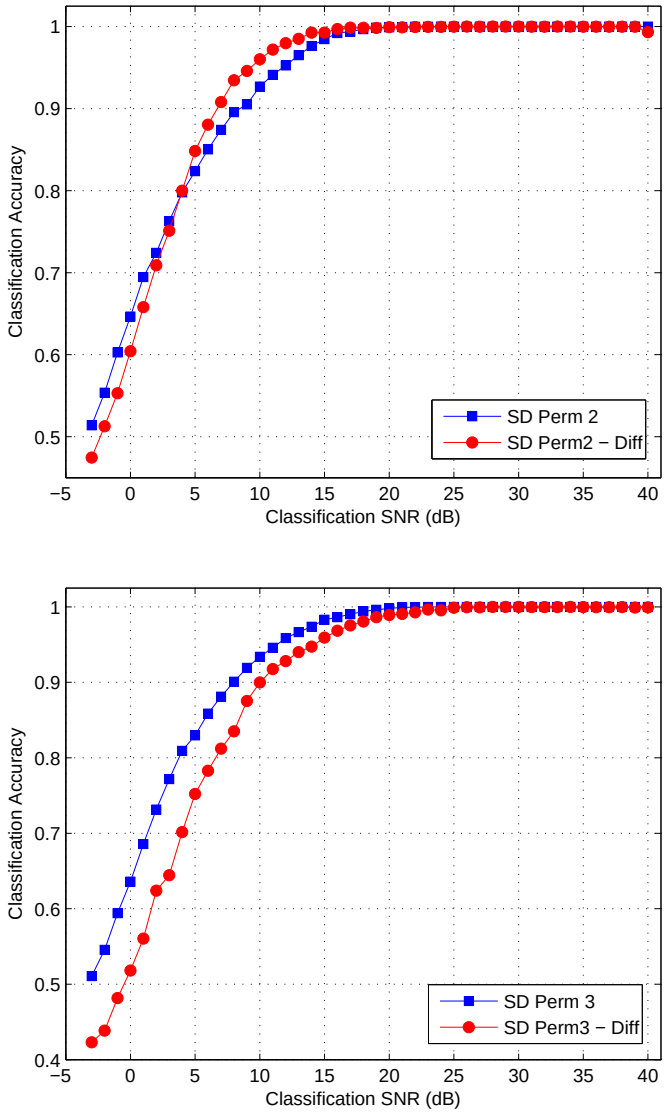


Figure 4.10. Inter-Manufacturer MDA/ML Classification using SD fingerprints: SD comparison with *Prop* using Perms #2 (top) and Perm #3 (bottom) from Table 4.3 with devices transmitting 802.11B signals.

4.4 SD Performance Comparison: 802.11A/B signals

Figure 4.11 shows a comparison of the SD technique performance for the worst case Perm #1 of 802.11A compared with Perm #1 of 802.11B, where the devices in each permutation contain identical serial numbers (Table 4.3 and Table 4.1). As can be seen, the SD method applied to 802.11B signals provides an improved gain of approximately 3 dB (although 802.11B preamble lacks the structure of the 802.11A signals), and there are clearly discriminating characteristics in this region to provide these classification results.

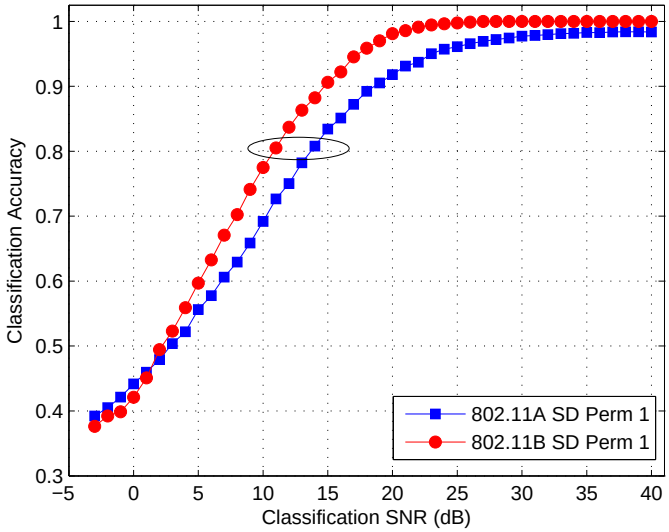


Figure 4.11. Intra-Manufacturer MDA/ML Classification using SD fingerprints: SD performance comparison of 802.11A with 802.11B signals for worst case Perm #1.

Figure 4.12 shows mean results taken from Figure 4.4 and Figure 4.7. These results demonstrate overall improved performance among 802.11B signals at SNR = 30 to -3 dB, and approximately 3 dB gain at 80% classification accuracy.

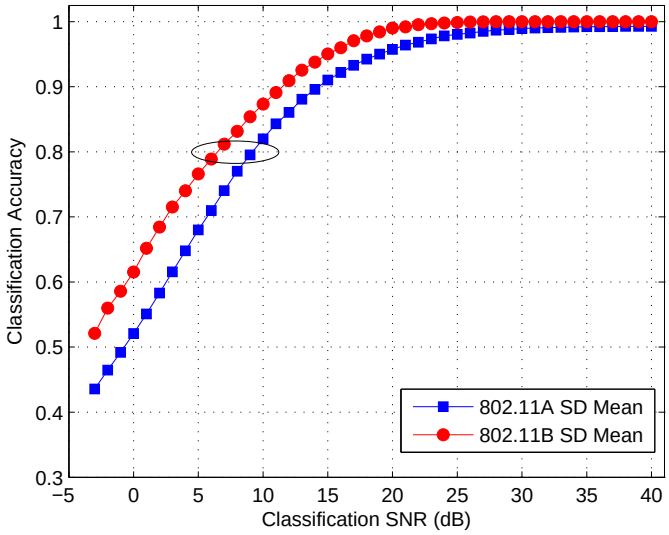


Figure 4.12. Intra-Manufacturer MDA/ML Classification using SD fingerprints: SD performance comparison of 802.11A with 802.11B signals for permutation means taken from Figure 4.4 and Figure 4.7.

Table 4.4 provides classification confusion matrices for Perm #1 (Table 4.1) of the Cisco devices for signals at $SNR = 14$ dB, where the results for 802.11A were taken from Table 4.2. Classification accuracies for a specific class (device) are presented along the diagonal, where 802.11B achieves an 88.3% classification accuracy and 802.11A achieves 83.3% (Figure 4.11). The lower matrix demonstrate performance differences between 802.11B and 802.11A. As can be seen, 802.11B provides improved performance over 802.11A across devices A and C, with the greatest improvement of 17.6% achieved for correctly classifying Class A. The lower matrix also demonstrates some degradation in classifying Class B for 802.11B vs 802.11A.

Table 4.4. Intra-manufacturer confusion matrices for 802.11A, and 802.11B fingerprinting: Permutation #1 from Table 4.1 with signals at $SNR = 14$ dB.

802.11A	Class Estimate		
Input Class	A	B	C
A	**77.9%**	5.2%	16.9%
B	6.0%	**93.9%**	0.1%
C	21.7%	0.3%	**78.0%**

802.11B	Class Estimate		
Input Class	A	B	C
A	**95.5%**	0.8%	3.7%
B	1.2%	**88.9%**	9.9%
C	2.9%	16.7%	**80.4%**

B - A	Class Estimate		
Input Class	A	B	C
A	**17.6%**	-4.4%	-13.2%
B	-4.8%	**-5.0%**	-9.8%
C	-18.2%	13.8%	**2.4%**

The uniqueness of fingerprint statistical features is illustrated in Figure 4.13. These RF DNA plots were generated by randomly selecting 200 collected bursts for each device, scaling them to achieve SNR = 14 dB, and averaging the corresponding statistical fingerprints. The number of DNA markers per segment is identical for both 802.11A and 802.11B. The y-axis labels correspond to the statistical measures defined in Section 2.5. The RF fingerprints (Figure 4.13) are from one manufacturer (Cisco) where the serial numbers are identified on the x-axis. Previous results in this chapter showed that greater uniqueness translates to better overall classification performance. When comparing Table 4.4 with Figure 4.13 for 802.11A, it can be seen that Class A and C are most confused.

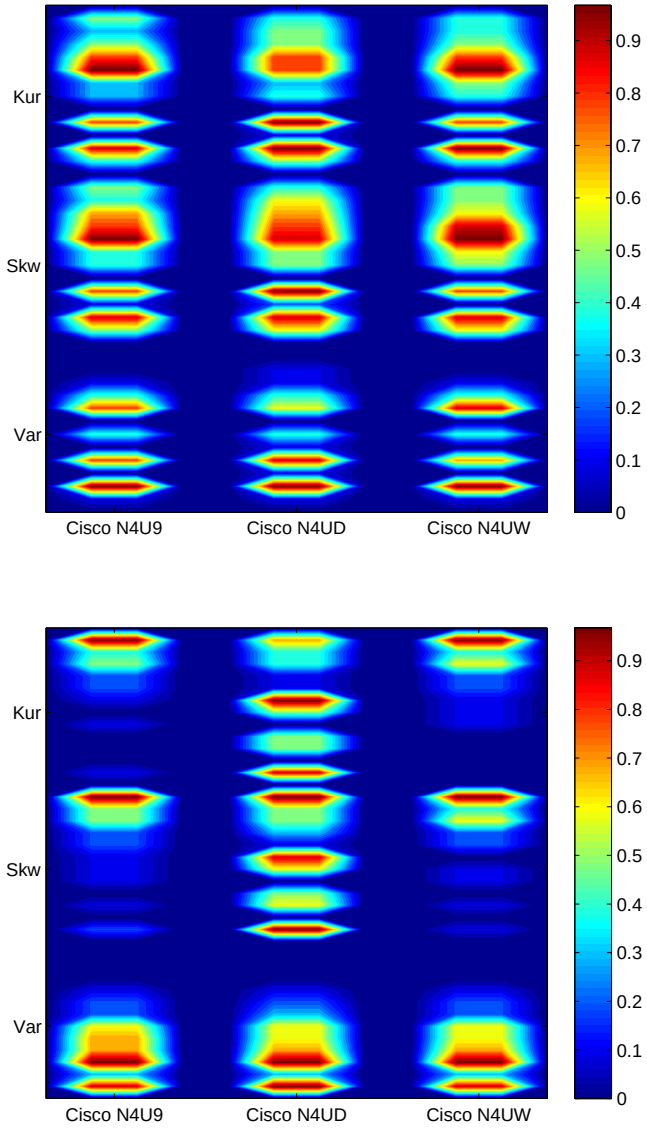


Figure 4.13. Intra-manufacturer RF fingerprint DNA plots showing worst case Perm #1 of (a) 802.11A and (b) 802.11B fingerprints based on 200 randomly selected bursts at SNR = 14 dB.

V. Conclusions and Future Work

5.1 Conclusions

The increase in availability and reduction in cost of commercial communication devices (IEEE compliant such as 802.11, 802.15 Bluetooth, 802.16, WiMax, etc) has increased wireless user exposure and the need for techniques to properly identify signals for increased security. Fundamental emissions from a device enable it to correctly operate and may provide unique fingerprints through unintentional modulation due to alterations caused by hardware and environmental factors. These unique fingerprints (features) enable the identification of the device manufacturer down to specific serial number. This research follows previous work [5, 6, 7, 11, 12, 15, 16, 17] and introduces unique Spectral Domain (SD) fingerprinting for classifying 802.11 wireless devices. This research focuses on proof-of-concept, versus optimization of parameters. The following provides a summary of results presented in Chapter IV.

5.1.1 802.11A Classification Performance.

Relative to other research [5, 6, 7], SD RF DNA fingerprint classification performance is consistent with the WD approach while demonstrating improved classification accuracy over the TD approach for 802.11A signals. In most cases, classification accuracy is greater than 80% at SNR $>$ 5 dB. At 80% classification accuracy, SD provides a gain of approximately 8 dB over the TD technique and some improvement (1%-3%) over the WD technique for SNR = -3 to 25 dB (lower SNRs are more consistent with operational environments). Using a spectral differencing *Prop* method discussed in [1], some improvement in performance is observed for specific cases, but generally fails to improve overall classification performance for the majority of permutations completed.

5.1.2 802.11B Classification Performance.

All parameters used to process 802.11B signals are taken directly from those used for 802.11A processing. The resulting performance of SD fingerprinting with 802.11B signals, using the worst case intra-manufacturer permutation, provides a significant improvement from that of 802.11A. An improved 802.11B gain of approximately 3 dB is demonstrated over 802.11A classification, which shows that the SD fingerprinting technique is a viable classification method, providing improved overall classification performance.

5.2 Recommendations for Further Research

This section provides recommendations for further research on SD RF DNA fingerprinting. Comparing results from previous research using 802.11A signals, SD fingerprinting provides performance consistent with the WD approach in [5] while providing less computational challenges. The following provides recommendation for further research with the SD approach:

1. **Bandwidth Sensitivity Analysis**: A post-collection filter bandwidth of BW = 7.7 MHz was used in this research and was chosen to be consistent with pervious work in [5, 6, 7]. Since the SD method has proven merit, there may be another bandwidth which provides more benefit and consistency.

2. **Specific Waveform Characteristics**: This research focuses on using standard PSD features for SD fingerprints, while previous research used instantaneous amplitude, instantaneous phase, and instantaneous frequency for TD fingerprints [5, 6, 7, 11, 12, 15, 16, 17]. Other waveform characteristics may improve accuracy and make the SD method more robust. Previous work [11, 15] also used standard deviation along with variance, skewness, and kurtosis. The

later three statistics were chosen here for consistency with [5, 6, 7] and were not chosen with any optimality criteria. There may be combinations of statistics and statistics used over specific subregions that provide greater device/class separability and improved classification accuracy. The number of regions (N_R = 13) was chosen based on analysis at the collected SNR = 40 dB. Different N_R may be better for other SNR values.

3. **Process and Parameter Optimization**: The process used for this research was adopted from [5, 6, 7, 11, 12, 15, 16, 17] while not focusing on a single parameter in the process. From burst detection and processing to signal classification, many parameters were chosen based on prior work [5, 6, 7] without focusing on any given factor, parameter, or combinations thereof. Analysis of specific parameters and combinations thereof may be beneficial.

4. **Different Signals of Interest**: 802.11A OFDM-based and 802.11B DSSS-based signals were used here based on work in [1, 5, 15]. Different OFDM or DSSS signals that are emerging for next generation applications may be discriminable with SD fingerprinting as well. Additional work could be done using SD RF fingerprinting with these emerging signals and their appropriate applications.

Appendix A. Detailed Signal Collection Procedures

The original collection procedures presented in Appendix A of [15, 11] are presented in this work for completeness. These collection procedures provide a detailed process for identifying a signal of interest, collecting its transient signal features, and converting it to MATLAB®using the Agilent E3238S RFSICS and Vector Signal Analyzer. The directions below reference screen-shots from the E3238S software for completeness.

1. Power on the Agilent E3238S RFSICS.
2. Open E3238S application (Figure A.1).
3. Power on the device under test and configure it as necessary.
4. Activate device transmitter and locate its peak in the wide-band search window (Figure A.2).
5. Zoom in on the signal of interest (right-click and drag to zoom in spectrum display).
6. Right-click in the left border and select "Tune to Trace" (Figure A.3).
7. Right-click in the left border again, Select "Marker" and Move Radio Button to "On" (Figure A.4).
8. Move the marker to the current peak of the spectrum display using the icon in the bottom right of the window (Figure A.5). The marker dictates the collection center.
9. Right-click in the left border again, Select "Marker to..." and Select "Center Freq" (Figure A.6).

10. Now, set the dynamic range of the ADC by going to "Configure", "Search Receivers", "ADC", "Input Range" and setting it to the lowest value (Figure A.7).

11. Activate the transmitter and check for ADC overload, if the block in the upper left corner is red, increase "Input Range" value one step at a time until the block remains solid blue (Figure A.8).

12. Right-click on grayed out camera in bottom right corner of the main window to modify the "Snapshot" settings.

13. Change "Status" to "Active", "Span" to the desired bandwidth, "Duration" to the desired duration of the collection, "Filename" to the desired, descriptive filename, click "OK" (Figure A.9).

14. Deactivate the transmitter (if necessary).

15. Click on the now Yellow Camera in bottom right to begin collection.

16. While collection is proceeding, activate the transmitter to collect transient signal data (Figure A.10).

The collection is then stored as a "Capture" file with the extension "*.cap". This file must now be converted to a "*.mat" file for post-collection processing in MATLAB®. The Vector Signal Analyzer software can be used to do this conversion.

1. Open the Vector Signal Analyzer application.

2. Select "File", "Recall Recording" and choose the desired "Capture" file.

3. Next, select "File", "Save Recording" and save as "*.mat".

The "*.mat" file contains twelve parameters. *FreqValidMax* and *FreqValidMin* are the highest and lowest frequencies of the collection. *InputCenter* is the center frequency of the collection. *XDelta* is the time change between each sample. *InputRefImped* is the input impedance. *XUnit* and *YUnit* are the units of measure for the x- and y-axes of the collection, which are seconds and volts, respectively. *Y* is complex signal data of type "single." *InputRange*, *InputZoom*, *XDomain* and *XStart* are additional unused parameters.

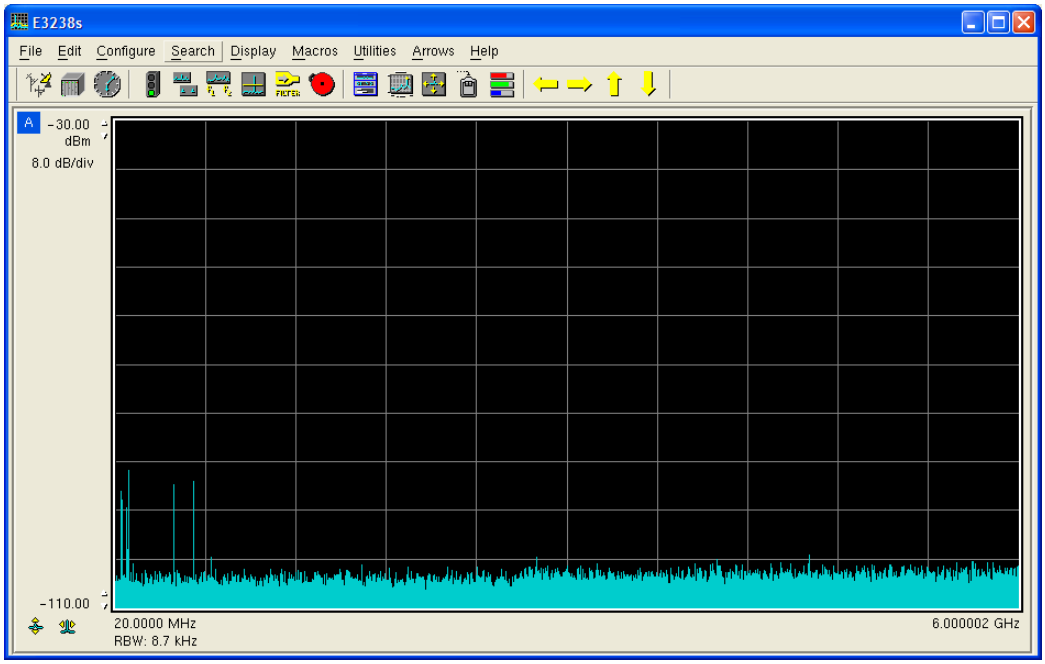


Figure A.1. Initial screen of RFSICS collection

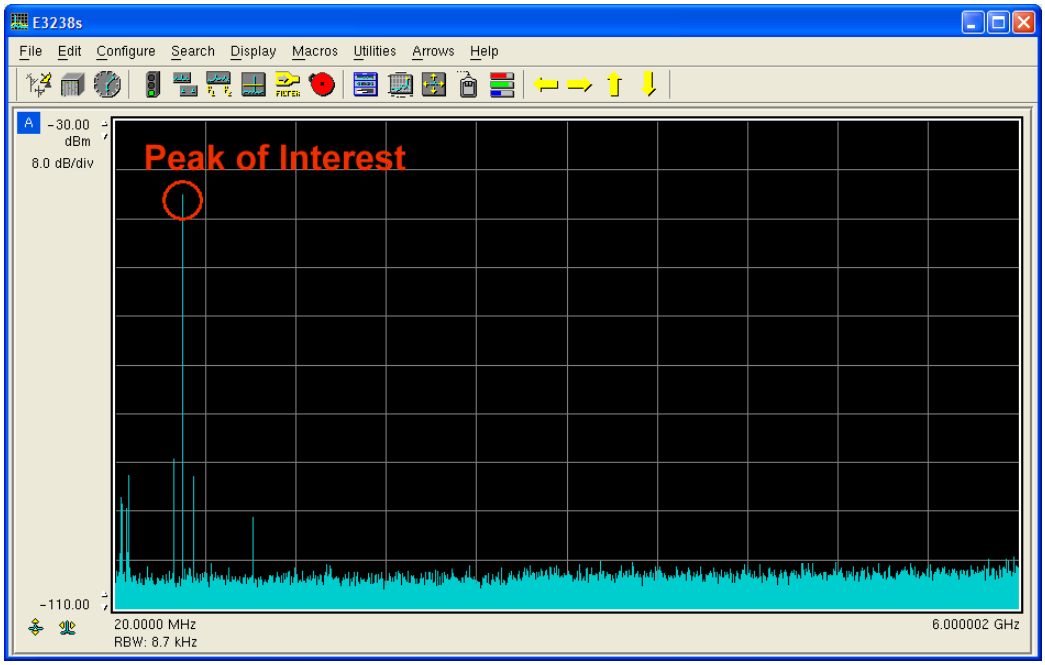


Figure A.2. Wide-band spectral response of the signal of interest.

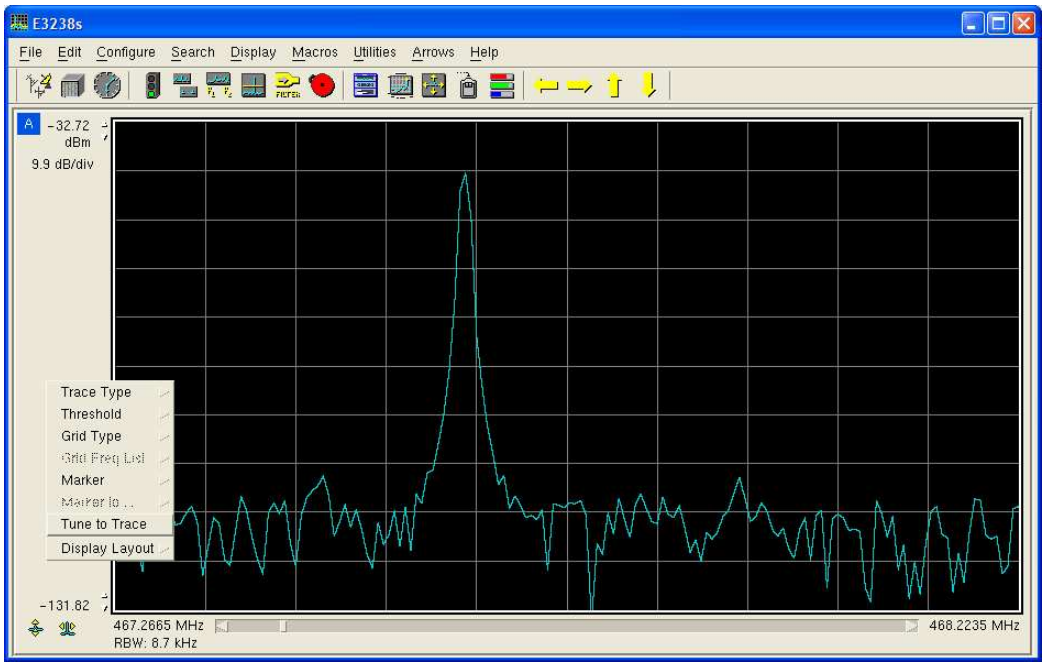


Figure A.3. Choose "Tune to Trace" as described in Step 6. Narrow-band view of the Frequency Content of the Signal of Interest.

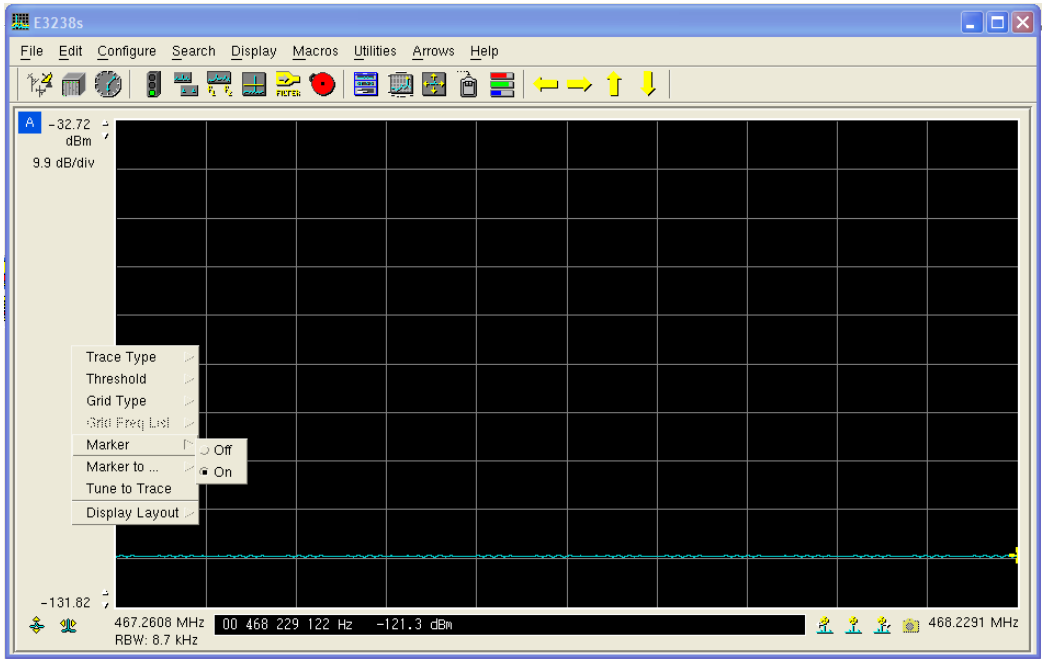


Figure A.4. Turn the "Marker" on as described in Step 7.

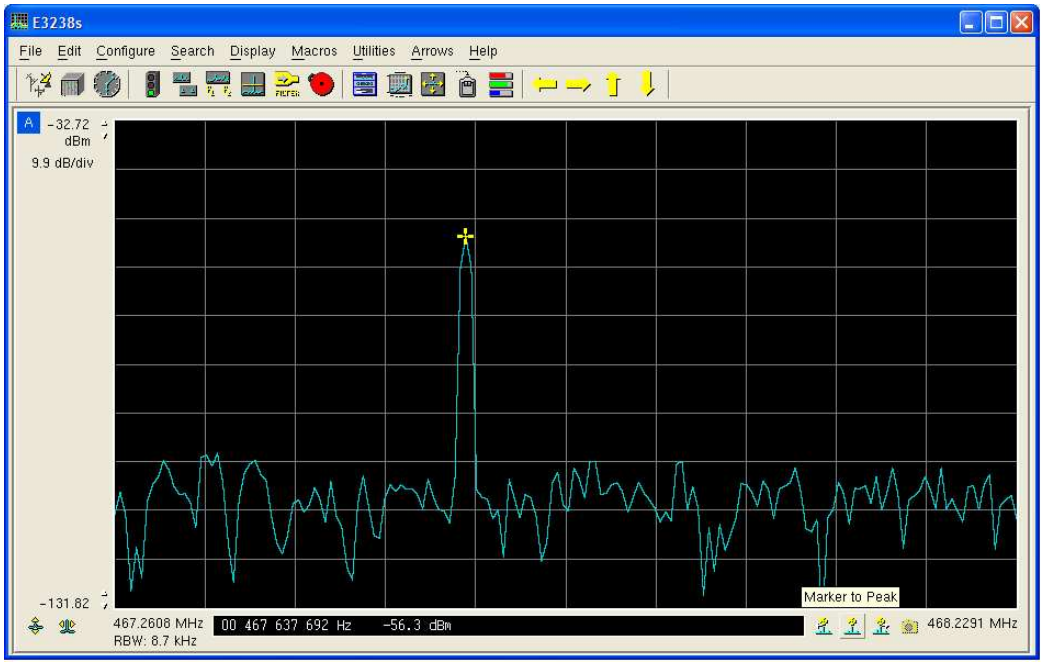


Figure A.5. Set the marker to the peak of the display as described in Step 8.

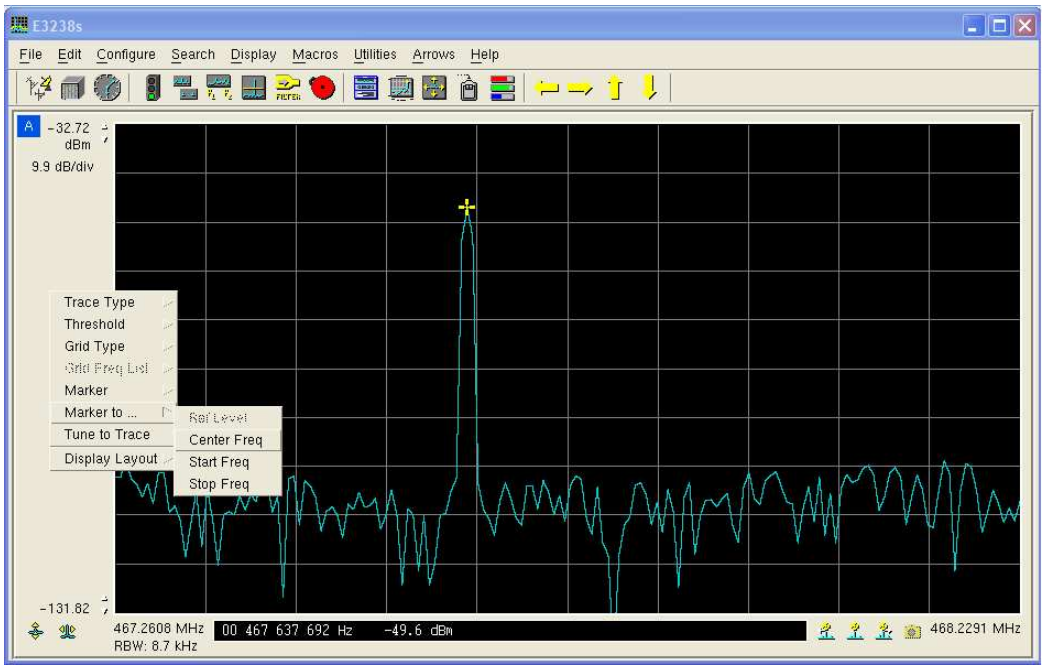


Figure A.6. Force the current frequency of the marker to the center of the display as described in Step 9.

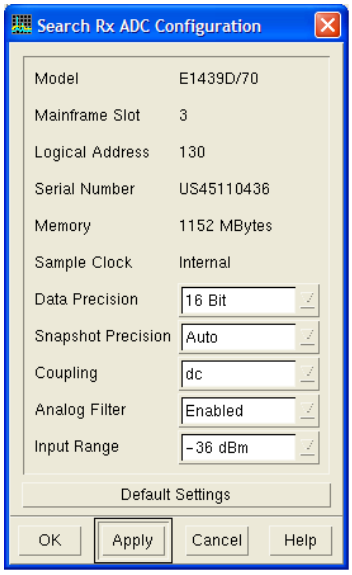


Figure A.7. Set the dynamic range of the ADC as described in Step 10.

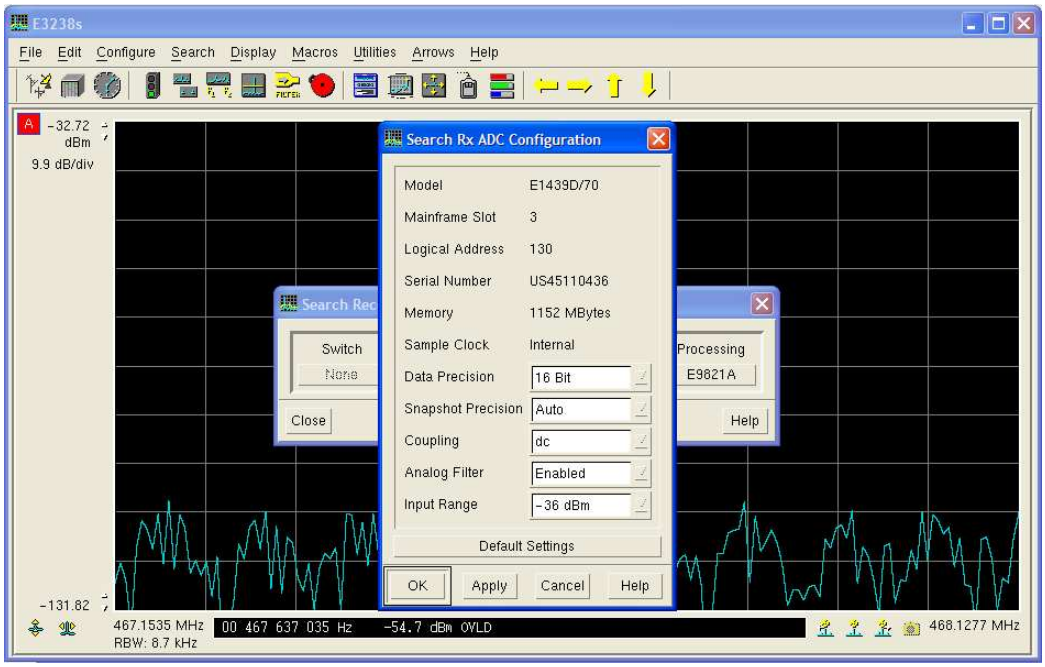


Figure A.8. Continue setting the dynamic range of the ADC by checking for overload as described in Step 11.

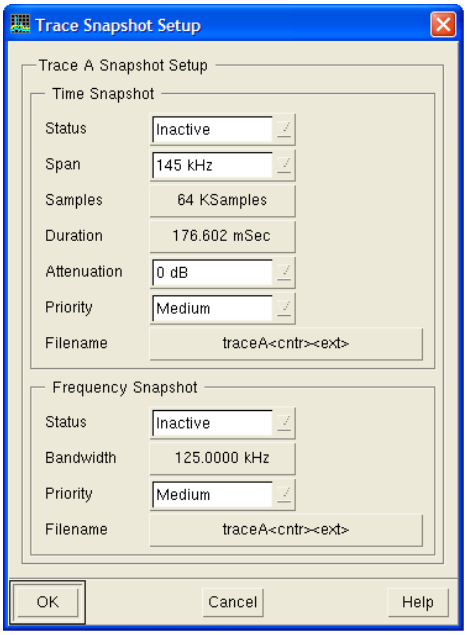


Figure A.9. Configuring the "Snapshot" details as described in Step 13.

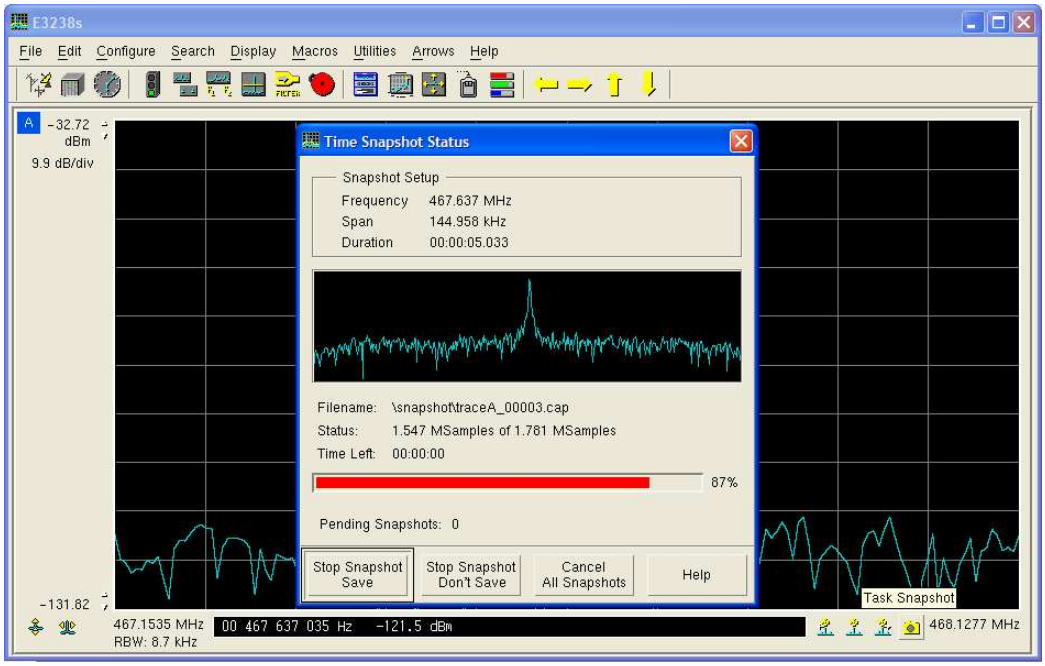


Figure A.10. Activate the transmitter while the "Snapshot" is being collected as described in Step 16.

Bibliography

1. Danev, B. and S. Capkun. "Transient-based identification of wireless sensor nodes". *IPSN '09: Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*, 25–36. IEEE Computer Society, Washington, DC, USA, 2009. ISBN 978-1-4244-5108-1.

2. Duda, R.O., P.E. Hart, and D.G. Stork. *Pattern Recognition*. John Wiley and Sons Inc., 2nd edition, 2001.

3. Gimelshteyn, M. *Classifying Commercial Receiver Emissions Using Fisher Discriminant Analysis*. Master's thesis, Air Force Institute of Technology, 2950 Hobson Way, WPAFB, OH, Mar 2006.

4. IEEE Computer Society. *IEEE Std 802.11-2007*, Jun 2007.

5. Klein, R.W. *Application of Dual-Tree Complex Wavelet Transforms to Burst Detection and RF Fingerprint Classification*. Ph.D. dissertation, Graduate School of Engineering, Air Force Institute of Technology (AETC), Wright-Patterson AFB OH, 2009. AFIT/DEE/ENG/09-12.

6. Klein, R.W., M.A. Temple, and M.J. Mendenhall. "Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security". *Journal of Communications and Networks*, 11(6):544–555, December 2009.

7. Klein, R.W., M.A. Temple, M.J. Mendenhall, and D.R. Reising. "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance". *Proceedings of the 2009 IEEE International Conference on Communications*. Jun 2009.

8. Li, Q. and W. Trappe. "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Rresistant Relationships". *IEEE Trans on Information Forensics and Security*, 2(4):793–808, Dec 2007.

9. MilitaryPeriscope.com. "SEI – SPECIFIC EMITTER IDENTIFICATION". URL http://www.periscope.ucg.com/terms/t0000271.html.

10. Proakis, J.G. *Digital Communications*. McGraw-Hill, New York, NY, 4th edition, 2001. ISBN 0-07-232111-3.

11. Reising, D.R. *Classifying Emissions From Global System For Mobile (GSM) Communication Devices Using Radio Frequency (RF) Fingerprints*. Masters thesis, Graduate School of Engineering, Air Force Institute of Technology (AETC), Wright-Patterson AFB OH, 2009. AFIT/GE/ENG/09-37.

12. Reising, D.R., M.A. Temple, and M.J. Mendenhall. "Improved wireless security for GMSK-based devices using RF fingerprinting". *Int. J. Electronic Security and Digital Forensics,*, 3(1):41–59, March 2010.

13. Sheng, Y., K. Tan, G. Chen, D. Kotz, and A. Campbell. "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength". *IEEE 27th Annual Conference on Computer Comm.* Apr 2008.

14. Sklar, B. *Digital Communications: Fundamentals and Applications.* Prentice Hall PTR, 2nd edition, 2001.

15. Suski, W.C. *Radio Fequency (RF) Fingerprinting Applied to Transient Signal Features from Commercial Communication Devices.* Masters thesis, Graduate School of Engineering, Air Force Institute of Technology (AETC), Wright-Patterson AFB OH, 2008. AFIT/GE/ENG/08-31.

16. Suski, W.C., M.A. Temple, M.J. Mendenhall, and R.F. Mills. "Radio Frequency Fingerprinting Commercial Communication Devices to Enhance Electronic Security". *International Journal Electronic Security and Digital Forensics*, 1(3):301–322, 2008.

17. Suski, W.C., M.A. Temple, M.J. Mendenhall, and R.F. Mills. "Using Spectral Fingerprints to Improve Wireless Network Security". *Proceedings of the 2008 IEEE Global Communications Conference.* Nov 2008.

18. Woelfle, M., M.A. Temple, M. Mullins, and M.J. Mendenhall. "Detecting, Identifying and Locating Bluetooth Devices Using RF Fingerprints". *2009 Military Communications Conference (MILCOM 2009).* Oct 2009.

Vita

Capt Sheldon Munns was born in Logan, Utah. After joining the Air Force in January of 1999, Sheldon attended technical school at Keesler AFB to train as a Guidance and Control Technician. After completion of technical school, Sheldon and family traveled to Grand Forks AFB in North Dakota to work on KC-135R model aircraft. At Grand Forks, Sheldon learned about the Airman Education and Commissioning Program (AECP) that would allow him to pursue a higher education degree and eventually receive a commission in the Air Force. In May of 2002 Sheldon was accepted and moved his family to Logan Utah in August 2002 to attend Utah State University to pursue a degree in Electrical Engineering. He graduated with his Bachelor's Degree in Electrical Engineering in August of 2005 and commissioned into the United States Air Force through Reserve Officer Training Corp (ROTC). Following his commission he was assigned to the F-16 Systems Group (Program Office) at Wright Patterson AFB Ohio where he worked in weapons integration for the F-16. Capt Munns was selected for graduate school at the Air Force Institute of Technology (AFIT) in August of 2008 and is currently completing his Master's Degree. His anticipated follow-on assignment is to the Sensors Division of the Air Force Research Labs (AFRL/RY) at Wright Patterson AFB, Ohio.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
25–03–2010	Master's Thesis	Aug 2008 — Mar 2010

4. TITLE AND SUBTITLE

Spectral Domain RF Fingerprinting for 802.11 Wireless Devices

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Sheldon A. Munns, Capt, USAF

5d. PROJECT NUMBER

JON 10-166

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GE/ENG/10-19

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory, Sensors Directorate (Vasu Chakravarthy)
2241 Avionics Circle
WPAFB, OH 45433-7765
(937) 904-9039, vasu.chakravarthy@WPAFB.AF.MIL

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYRE

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The increase in availability and reduction in cost of commercial communication devices (IEEE compliant such as 802.11, 802.16, etc) has increased wireless user exposure and the need for techniques to properly identify/classify signals for increased security measures. A communication device's emission includes intentional modulation that enables correct device operation. Hardware and environmental factors alter the ideal response and induce unintentional modulation effects. If these effects (features) are sufficiently unique it becomes possible to identify a device using its fingerprint, with potential discrimination of not only manufacturers but possibly serial numbers for a given manufacturer. Previous AFIT research has demonstrated effectiveness at RF Fingerprinting using 802.11A signals with 1) spectral correlation on Power Spectral Density (PSD) fingerprints, 2) Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification with fingerprints obtained from Time Domain (TD) and Wavelet Domain (WD) statistical features.As used here, Spectral Domain (SD) fingerprinting uses the Fourier Transform to calculate PSD features for device discrimination. Results here show some improvement over the WD approach (gain $\approx$ 3 dB) and significant improvement over the TD approach (gain $\approx$ 8 dB gain).

15. SUBJECT TERMS

Spectral Domain (SD), Radio Frequency (RF) Fingerprinting, Distinct native Attribute (DNA), Orthogonal Frequency Division Multiplexing (OFDM), Direct Sequence Spread Spectrum (DSSS)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Michael A. Temple, AFIT/ENGC
U	U	U	U	70	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x4279; michael.temple@afit.edu