3-14-2014

# A Comparison of RF-DNA Fingerprinting Using High/Low Value Receivers with ZigBee Devices

Tyler D. Stubbs


# A COMPARISON OF RF-DNA FINGERPRINTING USING HIGH/LOW VALUE RECEIVERS WITH ZIGBEE DEVICES

THESIS

Tyler D. Stubbs, Captain, USAF

AFIT-ENG-14-M-74

**DEPARTMENT OF THE AIR FORCE**
**AIR UNIVERSITY**

***AIR FORCE INSTITUTE OF TECHNOLOGY***

**Wright-Patterson Air Force Base, Ohio**

AFIT-ENG-14-M-74

# A COMPARISON OF RF-DNA FINGERPRINTING USING HIGH/LOW VALUE RECEIVERS WITH ZIGBEE 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

Tyler D. Stubbs, B.S.E.E.

Captain, USAF

March 2014

AFIT-ENG-14-M-74

# A COMPARISON OF RF-DNA FINGERPRINTING USING HIGH/LOW VALUE RECEIVERS WITH ZIGBEE DEVICES

Tyler D. Stubbs, B.S.E.E.
Captain, USAF

Approved:

| | |
|---|---|
| //signed// | 11 Mar 2014 |
| Michael A. Temple, PhD (Chairman) | Date |
| //signed// | 11 Mar 2014 |
| Lt Col. Jeffrey D. Clark, PhD (Member) | Date |
| //signed// | 11 Mar 2014 |
| Robert F. Mills, PhD (Member) | Date |

AFIT-ENG-14-M-74


## Abstract

The ZigBee specification provides a niche capability, extending the IEEE 802.15.4 standard to provide a wireless mesh network solution. ZigBee-based devices require minimal power and provide a relatively long-distance, inexpensive, and secure means of networking. The technology is heavily utilized, providing energy management, Industrial Control System (ICS) automation, and remote monitoring of Critical Infrastructure (CI) operations; it also supports application in military and civilian health care sectors. ZigBee networks lack security below the "Network" layer of the Open Systems Interconnect (OSI) model, leaving them vulnerable to open-source hacking tools that allow malicous attacks such as Media Access Control (MAC) spoofing or Denial of Service (DOS). A method known as Radio Frequency Distinct Native Attribute (RF-DNA) Fingerprinting provides an additional level of security at the Physical (PHY) level, where the transmitted waveform of a device is examined, rather than its bit-level credentials which can be easily manipulated. RF-DNA fingerprinting allows a unique human-like signature for a device to be obtained and a subsequent decision made whether to grant access or deny entry to a secure network.

Two National Instruments (NI) receivers were used here to simultaneously collect RF emissions from six Atmel AT86RF230 transceivers. The time-domain response of each device was used to extract features and generate unique RF-DNA fingerprints. These fingeprints were used to perform *Device Classification* using two discrimination processes known as Multiple Discriminant Analysis, Maximum Likelihood (MDA/ML) and Generalized Relevance Learning Vector Quantization-Improved (GRLVQI). Each process (classifier) was used to examine both the Full-Dimensional (FD) and reduced dimensional feature-sets for the high-value PCI Extension for Instrumentation Express (PXIe) and low-value Universal Software Radio Peripheral (USRP) receivers. The reduced feature-sets were determined using Dimensional Reduction Analysis (DRA) for

both quantitative and qualitative subsets. Additionally, each classifier performed *Device Classification* using a "hybrid" interleaved set of fingerprints from both receivers.

The FD feature-set used for *Device Classification* included $N_F$=297 features. When examining each single receiver seperately and averaging over both classifiers, FD analysis achieved an arbitrary benchmark of average correct classification $\%C$>90% (cross-device average) at $SNR$≈11.0 dB and $SNR$≈16.0 dB for PXIe and USRP receivers respectively. MDA/ML performed better for FD feature sets, with GRLVQI requiring $SNR$≈2.0 dB in additional gain to match MDA/ML performance. DRA was used to evaluate performance using both quantitatively ($N_F$=5, 10, 33, 66, 99) and qualitatively ($N_F$=99) reduced feature sets. Quantitative DRA performance favored the PXIe receiver which consistently achieved $\%C$>90% at $SNR$≈12.0 dB for $N_F$∈[10 297]. Qualitative DRA showed that irrespective of the receiver used, the *Phz*-only feature-set outperformed the *Frq*-only and *Amp*-only feature-sets. Additionally, when using FD $N_F$=297 and $N_F$=99 for both quantitative and qualitative feature-sets, $\%C_{FD} \approx \%C_{99Qnt} \approx \%C_{99Phz}$. Finally, when developing a *Hybrid Cross-Receiver* model using fingerprints from both receivers, testing with PXIe-only fingerprints proved to be the most effective method for performing *Device Classification*. Both classifiers performed better than in any other hybrid case, achieving the $\%C$>90% benchmark for $N_F$∈[5 297] and $N_F$∈[10 297] using GRLVQI and MDA/ML, respectively.

**Acknowledgments**

I would first and foremost like to thank my amazing wife and son. Without their love, patience, and encouragement, this dream never would have come to fruition.

I also would like to thank my advisor Dr. Temple for his guidance, wisdom and support throughout this research.

Tyler D. Stubbs

## Table of Contents

Page

## List of Figures

## List of Tables

## List of Symbols

| Symbol | Definition |
|---|---|
| $a$ | amplitude |
| $\%C_{99Amp}$ | 99-Feature Amplitude-Only Classification Benchmark |
| $\%C_{99Frq}$ | 99-Feature Frequency-Only Classification Benchmark |
| $\%C_{99Phz}$ | 99-Feature Phase-Only Classification Benchmark |
| $\%C_{99Qnt}$ | 99-Feature Quantitative Classification Benchmark |
| $\%C_{FD}$ | Full-Dimensional Classification Benchmark |
| $F$ | Fingerprint |
| $f_s$ | Sample Rate |
| $N_C$ | Number of Samples Collected |
| $N_{Ch}$ | Number of Instantaneous Responses |
| $N_{Cl}$ | Number of Classes |
| $N_D$ | Number of Dimensions |
| $N_{Dev}$ | Number of Devices |
| $N_F$ | Number of Features |
| $N_{IR}$ | Number of Independent Realizations |
| $N_M$ | Number of Statistical Metrics |
| $N_{Nz}$ | Number of Noise Realizations |
| $N_P$ | Number of Prototype Vectors |
| $N_R$ | Number of Regions |
| $N_{SHR}$ | Number of Synchronization Header Responses |
| $\phi$ | phase |
| $\Delta t$ | Sample Duration |

## List of Acronyms

| Acronym | Definition |
|---|---|
| A/D | Analog-to-Digital Converter |
| AFIT | Air Force Institute of Technology |
| AWGN | Additive White Gaussian Noise |
| DRA | Dimensional Reduction Analysis |
| GRLVQI | Generalized Relevance Learning Vector Quantization-Improved |
| ICS | Industrial Control System |
| IEEE | Institue of Electrical and Electronics Engineers |
| IP | Internet Protocol |
| I/Q | In-Phase and Quadrature |
| MAC | Media Access Control |
| MDA | Multiple Discriminant Analysis |
| MDA/ML | Multiple Discriminant Analysis, Maximum Likelihood |
| ML | Maximum Likelihood |
| MVG | Multivariate Guassian |
| NI | National Instruments |
| OSI | Open Systems Interconnect |
| PXIe | PCI Extension for Instrumentation Express |
| RF-DNA | Radio Frequency Distinct Native Attribute |
| ROI | Region of Interest |
| SFD | Start-of-Frame-Delimiter |
| SHR | Synchronization Header Response |
| USRP | Universal Software Radio Peripheral |
| WPAN | Wireless Personal Area Network |

A COMPARISON OF RF-DNA FINGERPRINTING USING HIGH/LOW VALUE RECEIVERS WITH ZIGBEE DEVICES

# I. Introduction

This chapter provides a brief introduction to the operationally motivated research of the ZigBee protocol and its applications in Section 1.1. Additionally, Section 1.2 provides the technical motivation for using the Air Force Institute of Technology (AFIT)'s Radio Frequency Distinct Native Attribute (RF-DNA) process. Specifically, Section 1.3 provides the current state of AFIT's RF-DNA fingerprinting process based on previous research [2–4, 6, 10, 11, 15, 20–23, 25–27, 29, 31–37, 39, 40, 45, 46] and advancements from the contributions of this research [30]. Finally, a breakdown of the document organization is presented in Section 1.4.

## 1.1 Operational Motivation

The Institue of Electrical and Electronics Engineers (IEEE) 802.15 standard provides guidance for establishing a Wireless Personal Area Network (WPAN) [24]. WPAN provide a an effective way for anyone to establish a personal network to which a multitude of wireless devices can be connected for buisness or home use. The ZigBee specification provides a niche capability, quickly growing in popularity, within this standard as dictated by IEEE standard 802.15.4 [48]. ZigBee provides a low energy, low cost alternative that is relatively simple to set up. ZigBee devices also boast long battery life and the ability to perform secure networking. For these reasons, ZigBee is used in many industries, including commercial, military, and healthcare. Commercial industries [13, 43, 44] use ZigBee for Industrial Control System (ICS) and building automation, energy management and the

monitoring of critical infrastructure. The military has begun to utilize ZigBee for location and positioning [10] while medical usage includes life-support and patient monitoring [5]. Given the strong probability that personal, critical, and even military national security information could traverse ZigBee networks on a day-to-day basis, the requirement for strong network security remains high.

Wireless networks, such as ZigBee, all run off of the same basic premise of a seven layer model known as the Open Systems Interconnect (OSI) model , shown in Fig. 1.1 [1]. The focus for security tends to rely soley on the "Network" and "Data Link" layers. This basic security is where a network relies on device Media Access Control (MAC) or Internet Protocol (IP) information to be submitted and verified as authorized prior to being allowed into a network. There are various open source hacking tools that detect these mechanisms by spoofing (replicating and presenting) specific device bit-level credentials and gaining unauthorized network access. Once inside, a malicous device can perform various attacks such as denial or service, network key sniffing, or hostile takeover of the whole network. Of these hacking tools, there are a few that specifically target vulnerabilities of ZigBee devices including KillerBee [47] and Api-Do [38].

This increasing threat to WPANs, specifically ZigBee, has constituted establishing security at the most basic "Physical" level of the OSI model. This level deals with the the actual physical waveform a device emits when it transmits or receives information. Ongoing research at AFIT has attempted to establish a process known as RF-DNA fingerprinting whereby a specific device can be described by features unique only to it. A network can then use this prior-known information to compare to a device requesting entry into the secure network, assess its bit-level credentials, and deem it as *authorized* or *unauthorized* to enter. This process describes each device with a unique human-like RF

signature that allows for highly accurate *Device Classification* and makes replication of or faking identities very difficult. It is for this reason that additional RF-DNA security at the "Physical" layer is important to supplement existing "Network" and "Data Link" security, which may be easier to bypass.

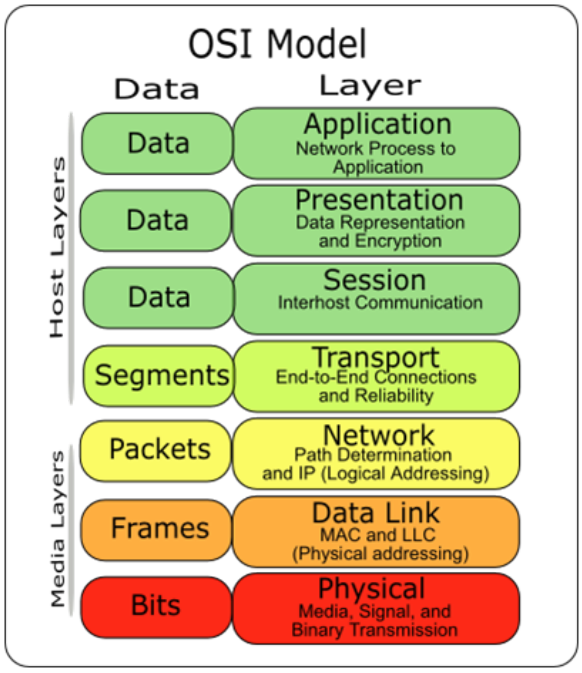


Figure 1.1: Seven-layer Open Systems Interconnect (OSI) Network Model [1].

## 1.2 Technical Motivation

This RF-DNA process has gone through multiple generations of evolution and currently stands as shown in Fig. 1.2 [9]. Each evolution of the process has incorporated different classification and verification methods, model development techniques, as well as introduced new receivers, signal types, and feature-sets. Each of these new or modified methods and hardware have been specifically addressed through previous work at AFIT [4, 6, 10, 11, 15, 20–23, 25–27, 29, 31–37, 39, 40, 45, 46], with the aim of supplementing research conducted outside of AFIT as well [2, 3, 6–8, 14–17]. Previous work specifically

on ZigBee has gone through one iteration [9], focusing mostly on *Device Verification* for a single receiver generated model from collections in multiple locations. The research here expands upon previous ZigBee work with the introduction of two new receivers, one of few current efforts to provide an extensive comparison of classification methods, and a first-look at generating a *Hybrid Cross-Receiver* model for use in *Device Classification*.

## 1.3 Previous vs. Current Research

Table 1.1 provides a summary of technical areas previously addressed in developing AFIT's RF-DNA process [2–4, 6, 10, 11, 15, 20–23, 25–27, 29, 31–37, 39, 40, 45, 46] and areas addressed by this research [30].

## 1.4 Document Organization

The remainder of this document is organized as follows:

Chapter 2 gives basic IEEE 802.15.4 ZigBee signal structure and outlines specific areas of interest as relevant to this research. Chapter 3 provides the research methodology used to implement the RF-DNA fingerprinting process for ZigBee wireless devices. Specifically discusses signal collection using a high-value and low-value receiver as well as post-collection signal processing and subsequent RF-DNA fingerprint generation using MATLAB. Finally, describes the Dimensional Reduction Analysis (DRA) process and details device discrimination techniques utilizing both Multiple Discriminant Analysis, Maximum Likelihood (MDA/ML) and Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) classification methods. Chapter 4 provides results and analysis for both full-dimensional and DRA (*qualitative* and *quantitative*) *Device Classification* performance for a single-receiver model. Additionally, a comparison of high-value versus low-value receiver performance is provided for two *Device Classification* methods, MDA/ML and GRLVQI. Finally, results and analysis is provided for both full-dimensional and quanti-

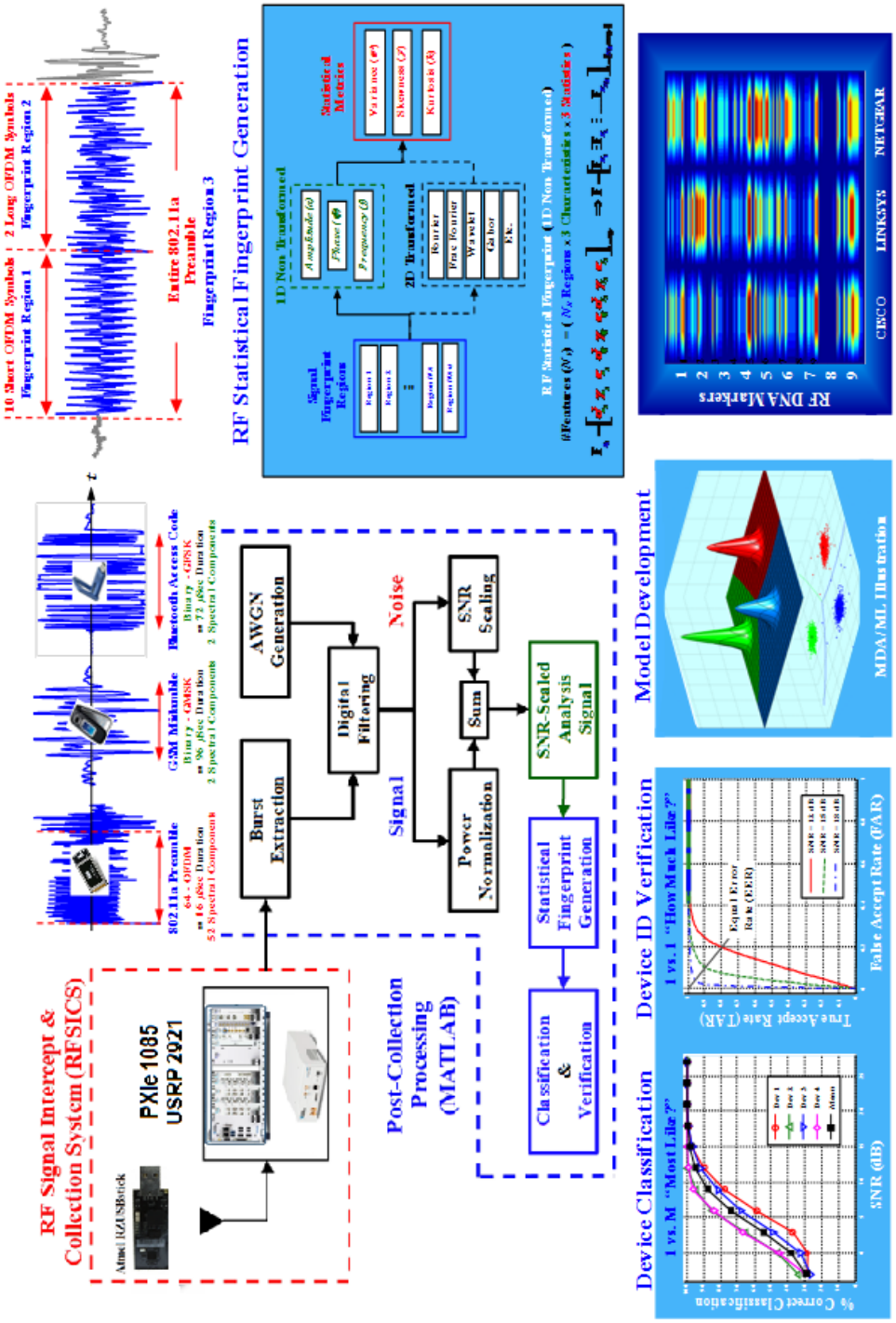


Figure 1.2: AFIT RF-DNA Fingerprinting Process [9].

tative DRA *Device Classification* using a *Hybrid Cross-Receiver* model for both MDA/ML and GRLVQI processes. The document concludes with Chapter 5 that summarizes research activity, highlights significant findings and provides recommendations for follow-on research.

Table 1.1: *Technical Areas* in *Previous* related work and *Current* research contributions. "×" denotes areas addressed.

| Technical Area | Previous Work | Current Research | |
|---|---|---|---|
| | Ref # | Addressed | Ref # |
| 1D Time Domain (TD) | [6, 15, 25, 26, 40, 45] [9–11, 39, 40, 45, 46] | × | [30] |
| 1D Spectral Domain (SD) | [35, 46] | | |
| 2D Wavelet Domain (WD) | [25–27] | | |
| 2D Gabor (GT/GWT) | [20, 32–35] | | |
| **Signal Type** | | | |
| 802.11a WiFi | [20, 25–27, 32, 46] | | |
| GSM Cellular | [36, 37, 45] | | |
| 802.16e WiMax | [32, 33, 35, 46] | | |
| 802.15.4 ZigBee | [9–11, 29] | × | [30] |
| **Classifier Type** | | | |
| MDA/ML | [25–27, 39, 40, 45, 46] [9–11, 20, 29, 33, 35–37] | × | [30] |
| GRLVQI | [20, 25, 26, 32, 34] | × | [30] |
| LFS | [2–4, 20–23] | | |
| **Dimensional Reduction Analysis (DRA)** | | | |
| GRLVQI | [9, 11, 25, 26, 31, 32, 34] | × | [30] |
| LFS | [19, 20] | | |
| KS-Test | [9, 11, 29] | | |
| **Device ID Verification** | | | |
| Authorized Device | [9, 11, 32, 34] | | |
| Rogue Device Rejection | [9, 11, 32, 34] | | |
| **Model Development** | | | |
| Hybrid Cross-Location | [9–11] | | |
| Hybrid Cross-Receiver | | × | [30] |

# II. Background

This chapter contains the technical background that serves as the framework for methodology described in Chap. 3. Section 2.1 describes the basic ZigBee signal structure as used in WPANs under IEEE 802.15.4. Section 2.2 introduces details for Air Force Institute of Technology (AFIT)'s Radio Frequency Distinct Native Attribute (RF-DNA) fingerprinting process, including fingerprint generation and calculation of statistical metrics from instantaneous time-domain signal responses. Section 2.3 describes elements of the Multiple Discriminant Analysis, Maximum Likelihood (MDA/ML) process and Section 2.4 describes the Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) process.

## 2.1 ZigBee Signal Characteristics

ZigBee-based networks adhere to guidelines provided in IEEE 802.15.4 [24], which specifies structure of "Physical" and "Data-Link" (specifically Media Access Control (MAC)-sublayer) layers for ZigBee device transmission. As shown in Fig.2.1 [24], ZigBee packets exhibit the data frame specification as provided in standards. The MAC sublayer contains the actual transmission including the associated addressing fields, sequence numbers, data being transmitted, etc. This research focuses on a specific Region of Interest (ROI) for exploitation known as the Synchronization Header Response (SHR) as shown in the "Physical" layer in Fig.2.1. This region is composed of a 5-octet, two sequence structure as shown in Fig.2.2. The SHR includes:

1. Preamble: A 4-octet (32-bit) binary string of 0's that is designed to provide symbol chip timing for the transmitting device.

2. Start-of-Frame-Delimiter (SFD): A 1-octet (8-bit) binary string that is predefined as (1 1 1 0 0 1 0 1). It is designed to signify the end of the preamble and thus the

beginning of the actual transmission, beginning with the “Frame Length”. The SFD is known alternatively as the “sync” frame, which is used throughout this paper.

The SHR waveform response serves as the ROI for this research because of its defined standard behavior, which is supposed to be identical for all devices, i.e., the SHR is the one part of any ZigBee transmission that remains constant [24]. Fully independent of device type, device ID, applications being performed, etc., the pre-defined bits and corresponding waveform response remain the same for all ZigBee transmissions. This independence is necessary in performing later model development and classification as described in Chap. 3. Previous research [10] failed to exploit the entire SHR, focusing soley on the “Preamble” for developing a model and performing classification. After further analysis, [9] found that exploitation of the entire SHR (Preamble + SFD) provided notably better *Device Classification* performance. It is under this auspice that research as described in Chap. 3 was performed and subsequent results in Chap. 4 reported.

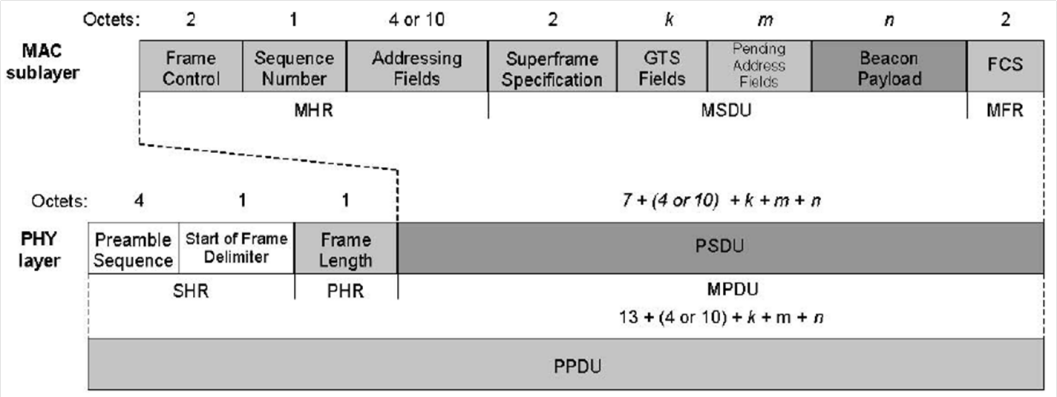


Figure 2.1: Physical Layer and MAC Sublayer Structure for a ZigBee Packet [24].

| Octets: 4 | 1 | 1 | | variable |
|---|---|---|---|---|
| Preamble | SFD | Frame length (7 bits) | Reserved (1 bit) | PSDU |
| SHR | | PHR | | PHY payload |

Figure 2.2: Physical Protocol Data Unit (PPDU) packet structure for IEEE 802.15.4 [24]. The SHR as specified on the left is the ROI for this research

## 2.2 RF-Fingerprint Generation

An RF-DNA fingerprint is the collective term used to describe a unique, human-like signature for a specific wireless device. Each fingerprint is generated in a two-step process that includes calculation of instantaneous time domain signal responses, and calculation of statistical metrics of those signal responses. Each step is further discussed below:

### *2.2.1 Time Domain Signal Responses.*

The ZigBee SHR contains a unique time-domain waveform in which instantaneous signal responses that describe it can be calculated. This research, as described and executed in [9–11, 27, 30, 31, 36, 37, 40, 46] focused on $N_{Ch} = 3$ characteristic instantaneous responses ($a$ = **amplitude**, $\phi$ = **phase**, $f$ = **frequency**) in a burst. Each collected signal is represented as complex In-Phase and Quadrature (I/Q) component pairs which both receivers collect and store in the form of 16-bit integers [28]:

$$[I_0, Q_0, I_1, Q_1, ..., I_{N_C}, Q_{N_C}] \, ,$$

where $N_C$ represents the total number of collected sample I/Q pairs. The corresponding instantaneous time-domain responses ($a$, $\phi$, $f$) are calculated as [30]:

$$a[n] = \sqrt{I[n]^2 + Q[n]^2}, \tag{2.1}$$

$$\phi[n] = \tan^{-1}\left[\frac{Q[n]}{I[n]}\right], \text{for } I[n] \neq 0, \tag{2.2}$$

$$f(n) = \frac{1}{2\pi}\left[\frac{d\phi(n)}{dt}\right], \tag{2.3}$$

for a given sample number $n = 1, 2, 3, \ldots, N_C$.

These calculated elements of the SHR are then normalized [27, 40] and their *mean* value removed. This is done by first removing the *mean* value for each element within a single response and then dividing (normalizing) the collection of remaining elements by the maximum value. This is accomplished for each response in (2.1), (2.2), and (2.3) and yields:

$$\bar{a}_c(n) = \frac{a[n] - \mu_a}{\max\limits_n\{a_c[n]\}}, \tag{2.4}$$

$$\bar{\phi}_c[n] = \frac{\phi[n] - \mu_\phi}{\max\limits_n\{\phi_c[n]\}}, \tag{2.5}$$

$$\bar{f}_c[n] = \frac{f[n] - \mu_f}{\max\limits_n\{f_c[n]\}}. \tag{2.6}$$

where (2.4), (2.5), (2.6) show the respective *mean* ($\mu_a$, $\mu_\phi$ and $\mu_f$) being removed and "max" notes the value by which each response is normalized; these are the normalized signal responses used for RF-DNA fingerprint generation.

### *2.2.2 Statistical Metrics.*

After each response is centered and normalized, statistical metrics are calculated. Following [9–11, 27, 30, 31, 36, 37, 40, 46], $N_M = 4$ statistical metrics can be calculated ($\sigma$ = **standard deviation** ,$\sigma^2$ = **variance**, $\gamma$ = **skewness**, $\kappa$ = **kurtosis**) for each response. This is done by:

1. Dividing the SHR into $N_R$ equal subregions subject to the constraint that $N_C/N_R$ is an integer. Additionally, the entire SHR is examined and treated as a region itself, yielding a total of $N_{R+1}$ regions.

2. Calculating $\sigma$, $\sigma^2$, $\gamma$, and $\kappa$ (as selected) for each response sequence $\bar{a}_c(n)$, $\bar{\phi}_c[n]$, and $\bar{f}_c[n]$ according to

$$\mu = \frac{1}{N}\sum_{n=1}^{N} x[n]\,, \tag{2.7}$$

$$\sigma = \sqrt{\frac{1}{N}\sum_{n=1}^{N}(x[n]-\mu)^2}\,, \tag{2.8}$$

$$\sigma^2 = \frac{1}{N}\sum_{n=1}^{N}(x[n]-\mu)^2\,, \tag{2.9}$$

$$\gamma = \frac{1}{N\sigma^3}\sum_{n=1}^{N}(x[n]-\mu)^3\,, \tag{2.10}$$

$$\kappa = \frac{1}{N\sigma^4}\sum_{n=1}^{N}(x[n]-\mu)^4\,, \tag{2.11}$$

where $N_C$ represents the total number of collected samples.

3. Arranging selected (2.8)-(2.11) metrics in a vector for each specific region as,

$$F_{R_i} = [\sigma_{R_i}\ \sigma^2_{R_i}\ \gamma_{R_i}\ \kappa_{R_i}]_{1\times 4}, \tag{2.12}$$

where $i = 1, 2, 3, \ldots, N_{R+1}$. An example of this process is shown in Fig. 2.3 [31].

In total, for each fingerprint composed of $N_{Ch}$ instantaneous responses and $N_M$ statistical metrics per response, over an SHR of $N_{R+1}$ regions, the number of "full-dimensional" (FD) features ($N_{FD}$) is calculated as,

$$N_{FD} = N_{Ch} \times N_M \times N_{R+1}, \tag{2.13}$$

where each full-dimensional fingerprint **F** is composed of the calculated statistics for each of the three instantaneous responses and shown as

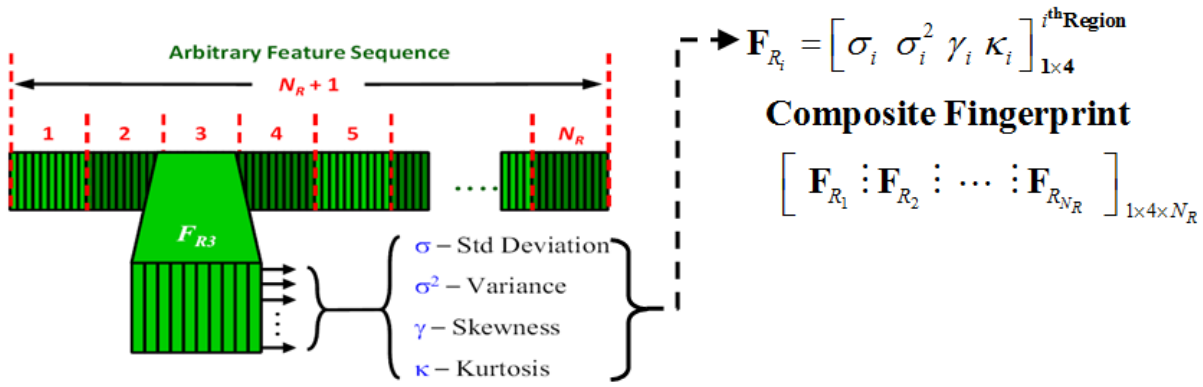


Figure 2.3: Process to generate a unique fingerprint utilizing statistical metrics for each instantaneous response over $N_{R+1}$ subregions [31].

$$\mathbf{F} = [\mathbf{F}^a \vdots \mathbf{F}^\phi \vdots \mathbf{F}^f]_{1\times N_{FD}}, \tag{2.14}$$

These full-dimensional RF-DNA fingerprints are then used for model development and classification for all devices (classes) using the two methods as described below.

## 2.3 MDA/ML Processing

The MDA/ML model development and classification process is comprised of two seperate processes including Multiple Discriminant Analysis (MDA) and Maximum Likelihood (ML) estimation. The description included here is based largely upon [9], with selected elements included here for completeness. MDA serves as a method to develop a model utilzing the *Training* RF-DNA fingerprints as will be discussed in Chap. 3. ML is a classification method that uses the *Testing* RF-DNA fingerprints to compare to the model generated by MDA and subsequently perform *Device Classification*. Both processes are presented in further detail below.

### *2.3.1 Multiple Discriminant Analysis (MDA) Model Development.*

This section describes how a model, later used for classification, is developed using MDA. MDA is a process, based on Fisher's Linear Discriminant, that linearly projects a high-dimensional data space into a lower-dimensional one. The desired effect is to follow the method of least-squares whereby a generalized linear model can be generated [12]. Unlike the Fisher method, which only works for discrimination of a $N_{Cl} \leq 2$ class problem, MDA works to reduce the feature dimensionality describing an RF-DNA fingerprint through projection for $N_{Cl} > 2$. MDA takes a specified number of feature ($N_F$)-dimensional described input, and projects it into a subspace that is characterized by $N_D$ dimensions. It is noted that through the remainder of this document, the term "class" is interchangable with a single "device" and accordingly with $N_{Dev} = 6$ devices as described in Section 3.1, $N_{Cl} = 6$ classes. The overall goal of this projection is to maximize the distance of the space describing each class from another while simultaneously minimizing the spread within a class. Mathematically, this directly translates to a desired maximum distance between the *mean* of each class, while minimizing the *variance* within a single class [12].

Two scatter matrices required for MDA are the out-of-class (inter-class, $\mathbf{S}_b$) and in-class (intra-class, $\mathbf{S}_w$) matrices [42]. These two matrices are used to assemble the required projection matrix, referred to as $\mathbf{W}$. It is this matrix that is used to project a fingerprint $\mathbf{F}$, and maintain an optimal balance ratio between inter-class *means* and intra-class *variances* as described in [12]. These scatter matrices, as well as their components are computed as [42],

$$\mathbf{S}_b = \sum_{i=1}^{N_{Cl}} P_i \mathbf{\Sigma}_i \,, \tag{2.15}$$

$$\mathbf{S}_w = \sum_{i=1}^{N_{Cl}} P_i (\mu_i - \mu_0)(\mu_i - \mu_0)^T \,, \tag{2.16}$$

where class covariance ($\mathbf{\Sigma}_i$) and the global *mean* of all classes ($\mu_0$) are calculated as

$$\Sigma_i = E[(x - \mu_i)(x - \mu_i)^T] \,, \tag{2.17}$$

$$\mu_0 = \sum_{i=1}^{N_{Cl}} P_i \mu_i \,. \tag{2.18}$$

$\mu_i$ and $P_i$ as referenced in (2.18) are the *mean* and prior probability for each class respectively. The intra-class scatter matrix in (2.16) provides a measure of the sum of probability-weighted class feature *variances* for each individual class while the inter-class scatter matrix in (2.15) provides a measure of the average distance (over all of the classes combined) between individual class *means* from the respective calculated global *mean* of all classes combined.

The $N_F$-dimensional input RF-DNA fingerprint vectors, shown as $\mathbf{F}$ from (2.14), are then projected into the lower ($N_D$)-dimensional subspace using the projection operator matrix, shown below as

$$\hat{\mathbf{f}} = \mathbf{W}^T \mathbf{F} \,. \tag{2.19}$$

$\mathbf{W}$ is the $N_F \times N_D$ projection matrix formed from the $N_{Cl}-1$ eigenvectors of $\mathbf{S}_w^{-1}\mathbf{S}_b$, and $\hat{\mathbf{f}}$ is the resulting RF-DNA fingerprint after projection into the new subspace [42]. Each of these fingerprints $\hat{\mathbf{f}}$ will then be split into *Training* and *Testing* sets as described in methodology in Chap. 3. An example of MDA projection is shown in Fig. 2.4. Here, $N_{Cl}$=3 classes are represented, resulting in a $N_D$ = 2-dimensional subspace. $\mathbf{W}_1$ and $\mathbf{W}_2$ respectively represent the two projection matrices described above. In this illustration, following the desired maximum *mean* seperation for the MDA process, $\mathbf{W}_1$ represents the "best" class separation with no overlap among the three classes. Once the best projection matrix (referred to as the actual "model") has been determined by MDA, and all *Training* RF-DNA fingerprints describing each class have been projected onto their respective subspaces,

model creation is finished and the process of *Device Classification* begins using ML and the projected *Testing* RF-DNA fingerprints.

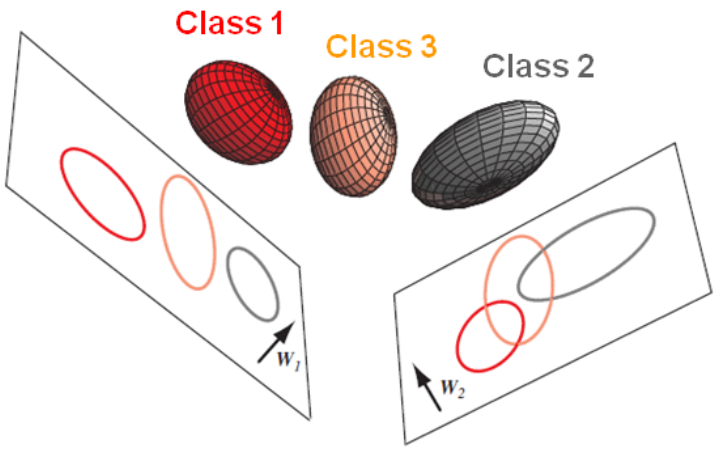


Figure 2.4: MDA Projection Representation for $N_{Cl}$=3 Classes corresponding to projection onto 2-dimensional subspaces using $\mathbf{W}_1$ and $\mathbf{W}_2$ [12] operators; Showing maximum seperation (no overlap among the different classes), $\mathbf{W}_1$ is the optimal projection matrix (model) in this case.

### *2.3.2 Maximum Likelihood (ML) Classification.*

ML is a method of *Device Classification* that uses the model developed with MDA. As previously stated, after a model is created using the *Training* RF-DNA fingerprints, ML takes the remaining (and unused) fingerprints describing the *Testing* data set, and performs *Device Classification*. ML classification begins once the best "model" or projection matrix ($\mathbf{W}$) is determined, and the *Testing* fingerprints for each class are projected onto the subspace. At this point in the process, the *Training* fingerprints have been projected, and the *mean* ($\hat{\mu}_i$), and *covariance* ($\hat{\Sigma}_i$) for each individual class have been computed for $i$=1, 2, . . . , $N_{Cl}$. ML operates off the assumption that all of the projected data is a Multivariate Guassian (MVG) distribution and hence each class can be described by its own class-dependent $\hat{\mu}_i$ and $\hat{\Sigma}_i$. Additionally, the ML process can assume that the covariance for

each class is identical and thus, a collective estimated covariance describing all classes can be shown as

$$\hat{\Sigma}_P = \frac{1}{N_{Cl}} \sum_{i=1}^{N_{Cl}} \hat{\Sigma}_i \ . \tag{2.20}$$

With the assumption of each class as a MVG distribution, posterior conditional probabilities can be calculated for each *Testing* fingerprint $\hat{\mathbf{f}}$ and used to provide a measurement of class ($c_i$) likelihood. Following the MVG distribution and collective covariance (2.20) estimate, likelihood estimation can be implemented as [31, 42],

$$P\left(\hat{\mathbf{f}}|N_{Cli}\right) = \frac{1}{(2\pi)^{(N_{Cl}-1)/2} \det\left(\hat{\Sigma}_P\right)^{1/2}} \cdot \exp(\mathcal{F}_e) \ , \tag{2.21}$$

where $\mathcal{F}_e$ is calculated as

$$\mathcal{F}_e = -\frac{1}{2}\left(\hat{\mathbf{f}} - \hat{\mu}_i\right)^T \left(\hat{\mathbf{\Sigma}}_P\right)^{-1} \left(\hat{\mathbf{f}} - \hat{\mu}_i\right) \ . \tag{2.22}$$

$c_i$ likelihood values as used for ML are based on a Bayesian decision theory. Each $\hat{\mathbf{f}}$ from the *Testing* data set is assigned to a specific $c_i$ by

$$P\left(c_i|\hat{\mathbf{f}}\right) > P\left(c_j|\hat{\mathbf{f}}\right) \quad \forall j \neq i \ . \tag{2.23}$$

Again, $i$=1, 2, . . . , $N_{Cl}$ and here, $P\left(c_i|\hat{\mathbf{f}}\right)$ is known as the the conditional posterior probability that a given $\hat{\mathbf{f}}$ belongs to a specific class $c_i$. The conditional posterior probability $P\left(c_i|\hat{\mathbf{f}}\right)$ in (2.23) is calculated using Bayes' Rule using specific $c_i$ likelihood values as shown below [31, 42]:

$$P\left(c_i|\hat{\mathbf{f}}\right) = \frac{P\left(\hat{\mathbf{f}}|c_i\right)P(c_i)}{P\left(\hat{\mathbf{f}}\right)}. \tag{2.24}$$

It is assumed that $P(c_i)=1/N_{Cl}$, meaning that all prior probabilities are equal for all classes. This, coupled with the fact that for any given $\hat{\mathbf{f}}$ fingerprint, $P\left(\hat{\mathbf{f}}\right)$ is the same for all $c_i$ as applied to (2.24), allows for simplication when making a comparison using (2.23). Classification is then performed on a single *Testing* $\hat{\mathbf{f}}$ using criteria in (2.23). Each $\hat{\mathbf{f}}$ is assigned a specific $c_i$ "label" based on maximum posterior probability. A "correct classification" occurs if the assigned $c_i$ label matches the true or known $c_i$ label. This process is repeated on all *Testing* fingerprints.

## 2.4 GRLVQI Processing

The second method considered for model development and classification is GRLVQI. The description included here is based largely upon [31], with selected elements included here for completeness. Unlike MDA/ML which is a two-stage process of model development and classification, GRLVQI is a one-stage process that develops a model and performs classification simultaneously. GRLVQI provides some advantages over MDA/ML, including:

1. No required assumption of MVG distribution; GRLVQI does not require knowledge of or assumption of any specific statistical distribution.

2. Model Development and *Device Classification* are performed jointly, rather than as independent processes.

3. Each input feature is assigned a relevance value ($\lambda$) that allows for feature ranking and Dimensional Reduction Analysis (DRA), as described in Section 3.4.

The model generated by GRLVQI utilizes prototype vectors that describe a specific space for each class. The number of prototype vectors $N_P$ is pre-defined before model

development and classification take place. $N_P$ is the same for all classes and each prototype vector used is comprised of $N_F$ features. The collection of all prototype vectors that describe the classes is represented by $\mathbf{p}^n$, and given by [18]

$$\mathbf{p}^n = [\mathbf{P}]_{(N_{Cl} \cdot N_P) \times N_F}, \tag{2.25}$$

where $N_{Cl}$ is the number of classes and $\mathbf{P}$ is a matrix that defines the classification boundaries for the prototype vectors. The overall goal is to minimize Bayesian risk by iteratively shifting the intra-class ($\mathbf{p}^n$) and inter-class ($\mathbf{p}^o$) prototype vectors that describe the space for all classes until a "best fit model" is achieved. This shift, $d_\lambda^n$, is computed as [18]

$$d_\lambda^n = \sum_{i=1}^{N_F} \lambda_i (\hat{\mathbf{f}}_i^m - \mathbf{p}_i^n)^2 \,, \tag{2.26}$$

where $\hat{\mathbf{f}}^m$ is a randomly chosen *Training* input fingerprint to start the process, and $n$ is the prototype vector from (2.25) such that $n = 1, 2, 3, \ldots, N_P$. $\lambda_i$ is also randomly chosen when the process is started.

This iterative process continues [31] until the prototype vectors are arranged in a best-fit model and the corresponding $\lambda_i$ values determined. Each $\lambda_i$ receives a ranking (number) that indicates its importance in classification; each $i$ is known as an "index number" and directly corresponds to a single feature. All $\lambda_i$'s are organized into a single vector known as $\lambda_B$ where it is possible for different index numbers (different features) to have the same relevance ranking ($\lambda$) value, however,

$$\sum_{i=1}^{N_F} \lambda_i = \lambda_B \equiv 1.$$

The higher the $\lambda_i$ value, the more important or relevant it is in performing *Device Classification* as will later be discussed in Section 3.4. Finally, the *Testing* fingerprints ($\hat{\mathbf{f}}$) are placed in 2.26 one at a time according to the best model, and the euclidean-distance, between each $\hat{\mathbf{f}}$ and the prototype vectors, is calculated as shown in Fig. 2.5 [31]. The classification (assignment of that particular $\hat{\mathbf{f}}$ to a specific $c_i$) follows according to [31]

$$c_i : \min_{i,j}(d_\lambda^p(\mathbf{p}_{i,j}, \hat{\mathbf{f}})) \tag{2.27}$$

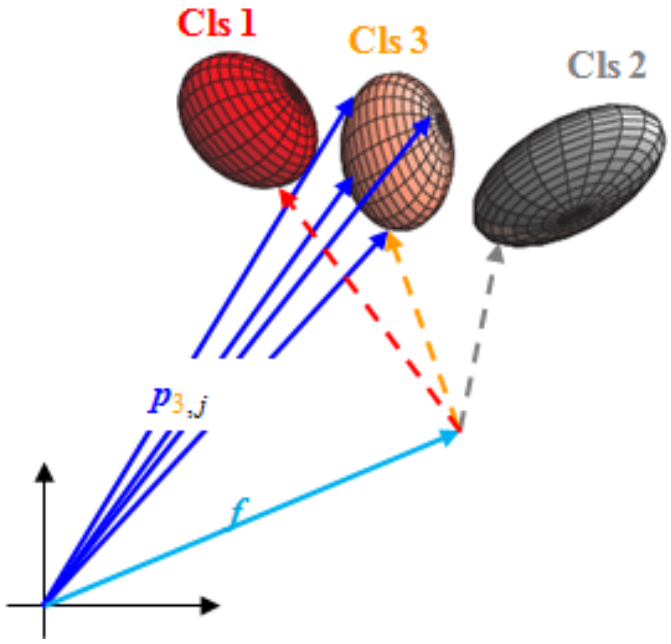


Figure 2.5: GRLVQI Projection Representation for a single fingerprint $\hat{\mathbf{f}}$ for $N_{Cl}$=3 Classes[31].

# III. Methodology

This chapter contains the methodology utilized while conducting this research in order to obtain the results as presented in Chap. 4. Simultaneous emissions collections were taken by both receivers for a single device at a time. These emissions, stored by the receivers as basic In-Phase and Quadrature (I/Q) components, were then converted into complex values for ease in signal processing. MATLAB was then used to compute instantaneous responses of detected bursts over the entirety of the Region of Interest (ROI) and used to detect and extract "bursts." The ROI, or ZigBee Synchronization Header Response (SHR), was then down-converted to base-band and filtered with a $8^{th}$-order Butterworth filter to remove background channel noise. Simultaneously, Additive White Gaussian Noise (AWGN) was generated, like-filtered, and added to the filtered SHR to appropriately power-scale and achieve $SNR \in [0\ 24]$ dB. This resulting signal, comprised of the sum of the down-converted and filtered SHR and AWGN, was then broken into $N_R$ subregions. These subregions were then used to calculate statistical metrics based off of the instantaneous time-domain signal responses. These are statistical "features" used to generate a unique Radio Frequency Distinct Native Attribute (RF-DNA) fingerprint that was used in *Device Classification* using both Multiple Discriminant Analysis, Maximum Likelihood (MDA/ML) and Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) processes. Section 4.1 describes the setup for collecting emissions. Section 4.2 discusses all post-signal collection processing, including burst detection, filtering, and AWGN-aided $SNR$ scaling. Section 4.3 discusses how an RF fingerprint was generated for a full-dimensional feature-set, while Section 4.4 discusses the process known as Dimensional Reduction Analysis (DRA). Finally, Section 4.4 discusses device discrimination, using both MDA/ML and GRLVQI model generation and

classification techniques. Accounting for specific receivers used here, AFIT's entire RF-DNA Fingerprinting process is as shown in Fig. 3.1 [9].

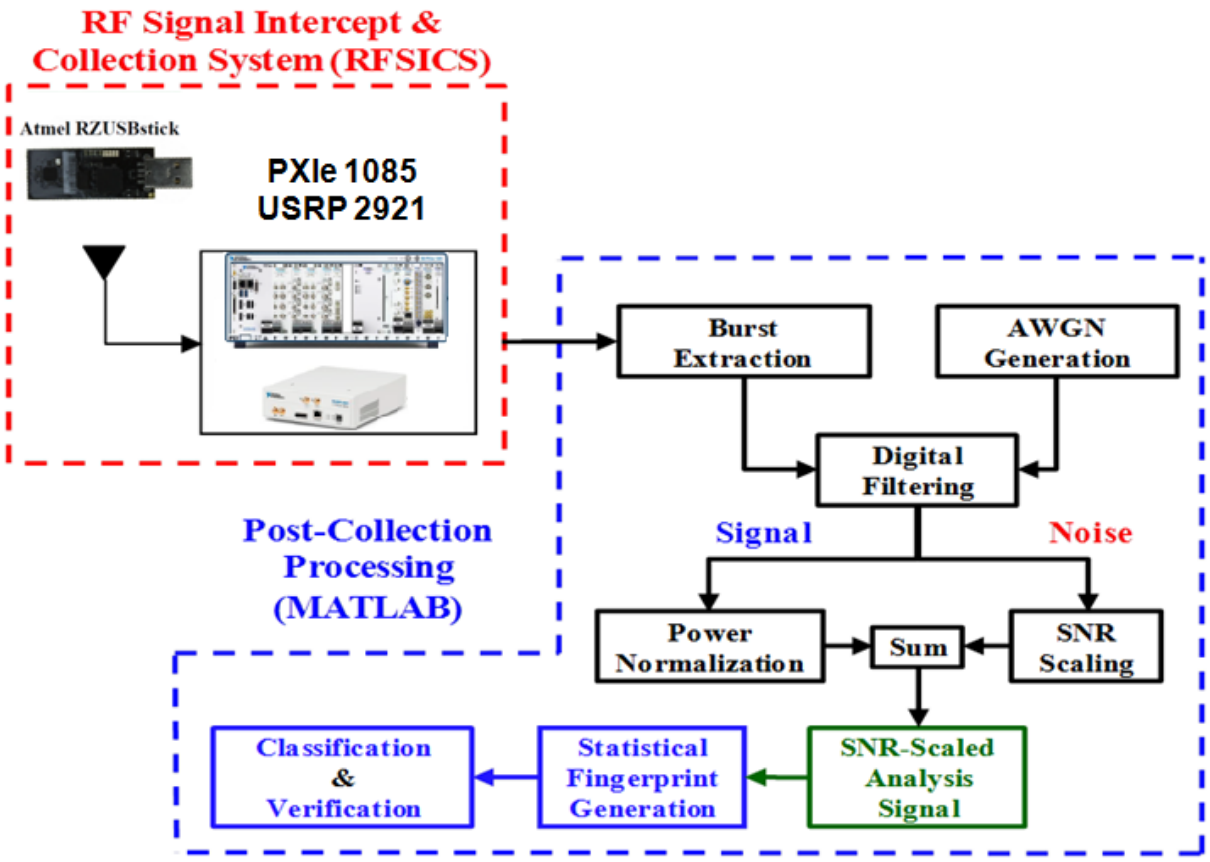


Figure 3.1: AFITs Fingerprinting Process [9]

## 3.1 Signal Collection

Two receivers, the National Instruments (NI) PCI Extension for Instrumentation Express (PXIe)-1085 and Universal Software Radio Peripheral (USRP)-2921, each with a 16-bit Analog-to-Digital Converter (A/D), were used to collect RF emissions from six Atmel AT86RF230 KillerBee ZigBee transceivers transmitting at 2.48 GHz per IEEE 802.15.4. Each device (collectively referred to henceforth as Atmel RZUSBstick or seperately as

Dev1, Dev2,...,Dev6) was placed 2.0m away from and in direct line-of-sight (LOS) of each receiver as depicted in Fig. 3.2 [30]. To present the "most challenging" scenario possible for *Device Discrimination* and obtain an accurate comparison between the higher-value PXIe (≈ $150K) and lower-value USRP (≈ $2K), multiple controls for the collection process were established, including:

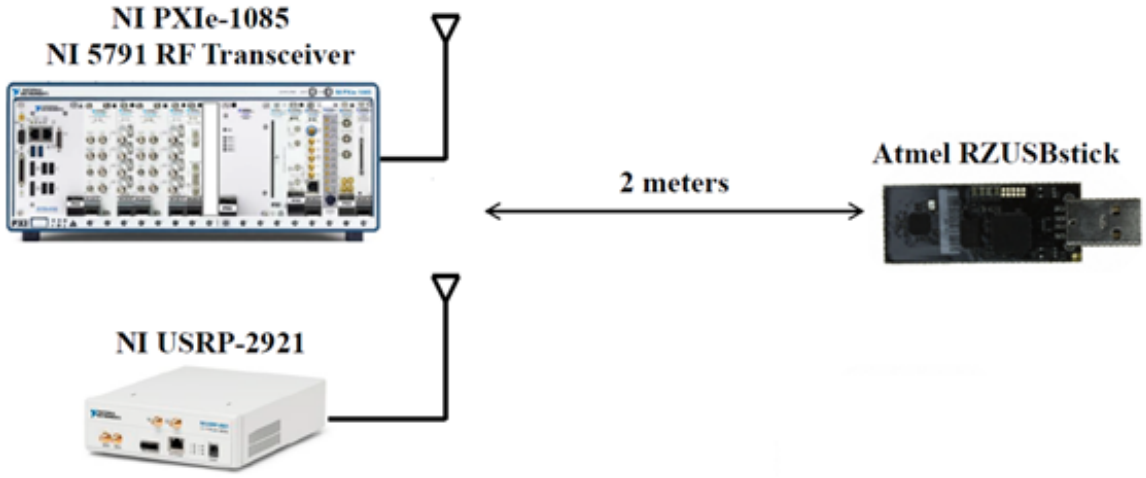


Figure 3.2: Setup to collect Atmel RZUSBstick emissions using PXIe and USRP receivers [30].

1. Emissions collected on one device at a time
2. Simultaneous collections of the same device emissions by both receivers
3. Possible receiver clock presence (Fig. 3.3) affecting collection center frequency addressed with 3MHz offset

Accounting for all of these factors, emissions (also referred to as bursts) were collected for each device at a sample rate of $f_s = 20$ Msps. Fig. 3.4 shows a one-sided, expanded

view of Fig. 3.3.

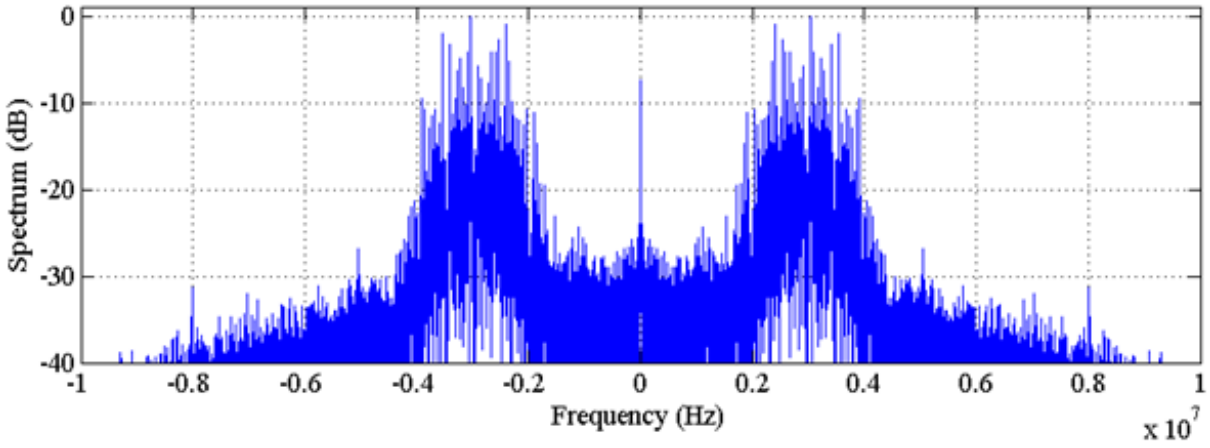


Figure 3.3: Normalized PSD of *Atmel RZUSBstick* collection noting clock presence near $f = 0$ Hz.

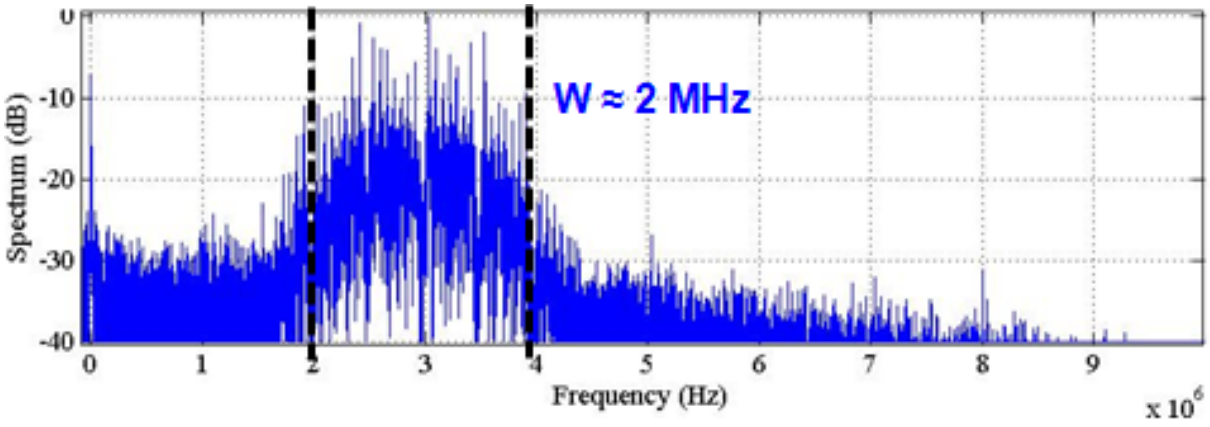


Figure 3.4: Normalized PSD response from Fig. 3.3 with 3MHz center frequency offset. Collections taken at $f_s = 20$ Msps.

## 3.2 Post-Collection Processing

Following emission collections on all ZigBee devices using both receivers, a series of post-collection processing steps were performed using MATLAB before RF-DNA fingerprint generation. Collected bursts were first put through an amplitude-based detection process, with bursts meeting specific criteria "extracted," and those not discarded. Extracted bursts were down-converted (center frequency shifted to $f = 0$), and subsequently placed through a baseband filter to remove background noise. Finally AWGN was generated, like-filtered, power-scaled, and added to the bursts to achieve a desired $SNR \in [0\ 24]$ dB. Each of these steps followed those from previous work [9, 30, 31], and are described specific to this research next.

### *3.2.1 Burst Detection.*

As discussed in Section 2.2.1, collected emissions from both receivers were stored as interleaved I/Q components according to [28]:

$$[I_0, Q_0, I_1, Q_1, ..., I_{N_C}, Q_{N_C}]; \tag{3.1}$$

where $N_C$ is the total number of collected samples. For easier processing in MATLAB, each I/Q pair was converted into its corresponding complex format as:

$$[(I_0 + jQ_0), (I_1 + jQ_1), ..., (I_{N_C} + jQ_{N_C})]. \tag{3.2}$$

The collected bursts were then put through an amplitude-based detection process to extract usable bursts out of the background noise. Bursts that met specific detection criteria were determined as suitable to subsequently turn into fingerprints for later *Device Classification*, while others were discarded. Specific requirements for detected bursts included specific leading ($t_L$) and trailing ($t_T$) edge thresholds, as well as minimum ($T_{Min}$) and maximum ($T_{Max}$) time duration, shown in Table. 3.1.

Table 3.1: Amplitude-based burst detection parameters for ZigBee transmission collections.

| Parameter | Variable | Value |
|---|---|---|
| Leading Threshold | $t_L$ | -6.0 dB |
| Trailing Threshold | $t_T$ | -6.0 dB |
| Min Duration | $T_{Min}$ | 425 $\mu sec$ |
| Max Duration | $T_{Max}$ | 550 $\mu sec$ |

The detection process began with the instantaneous amplitude response ($a_{\lfloor}n]$) being calculated according to (2.1). These values for a specific collection (multiple bursts) were then converted into dBv using:

$$a[n]_{dBv} = 20\log_{10}(\frac{a[n]}{1.0\ v}). \tag{3.3}$$

This provides a direct relation between amplitude and dB so that the largest $a[n]_{dBv}$ for a specific $n$ can be found throughout the entire collection. A normalized peak value is then established such that all other bursts in the collection meeting the required $t_L$ and $t_T$ thresholds from this peak are retained for possible extraction. If a burst has met this requirement, it is then examined for duration requirements. Recalling that $f_s = 20$ Msps, and $\Delta t = 1/f_s = 0.05$ $\mu$sec, a direct relation between $N_C$ samples and time duration can be established. The burst duration is then calculated according to its leading sample ($n_L$) and trailing sample ($n_T$) where

$$N_{Dur} = (n_T - n_L), \tag{3.4}$$

$$T_{Min} < (N_{Dur} * \Delta t) < T_{Max}. \tag{3.5}$$

If threshold and duration requirements are met, a burst is retained and "extracted" for use in classification; if it does not meet the requirements it is discarded.

### *3.2.2 Down Conversion and Filtering.*

After burst extraction was completed, the retained bursts were subsequently placed through a two-stage process where each was down-converted to baseband ($f_c = 0$) and filtered. Each process is outlined below:

1. MATLAB was used to down-convert each extracted burst to baseband using its own center frequency estimate derived from a gradient-based frequency estimation process [9, 30].

2. The down-converted burst was placed through a baseband filter to remove background noise and minimize fluctuations in *Device Classification*. This was done as in [9, 30], using a $8^{th}$-order Butterworth filter having a baseband bandwidth of $W_{BB} = 1$MHz. The result was a single burst, centered at $f_c = 0$, with minimal effect from noise outside of the collected IEEE 802.15.4 channel. This process was repeated for all extracted bursts, with one such burst shown in Fig.3.5 [30].

### *3.2.3 SNR Scaling.*

Finally, to provide a desired analysis range of $SNR \in$[0 24] dB ($SNR_A$) for *Device Classification*, AWGN was created using MATLAB and like-filtered before addition to each burst to form the collective SHR used to generate fingerprints.

The collected $SNR$ ($SNR_C$) is a function of both power in the collected signal (without background noise) ($P_C$), and the power in the background noise during collection ($P_N$). $P_N$

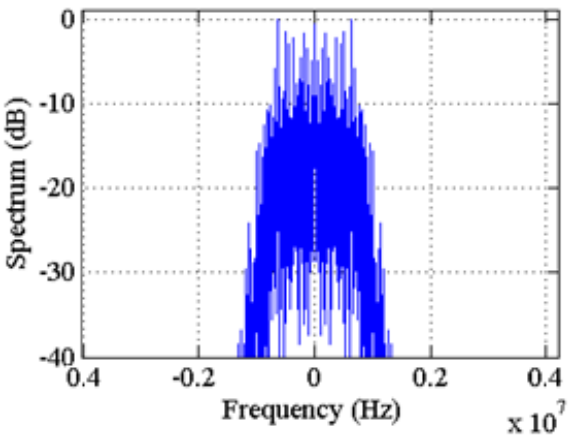


Figure 3.5: Normalized PSD Response for Atmel RZUSBstick after baseband down-conversion and application of $8^{th}$-order Butterworth Filter $W_{BB} = 1MHz$ [30].

was measured when none of the six devices was transmitting so that it represents a true "noise-only" power. The resulting $SNR_C$ in dB is represented as

$$SNR_C = 10 \times \log_{10}\left(\frac{P_C}{P_N}\right)(dB)\,, \tag{3.6}$$

which for typical ZigBee collections here ranged from $SNR_C \approx 24$ dB (USRP) to $SNR_C \approx 30$ dB (PXIe).

The total signal ($s_{Tot}$) used for analysis over $SNR_A$ is the summation of the received signal with no noise ($s_r$), background noise alone ($s_N$), and added AWGN ($s_{GN}$), and is given by

$$s_{Tot} = s_r + s_N + s_{GN}\,. \tag{3.7}$$

The average power in $s_{GN}$ required to achieve $SNR_A$ is noted as $P_{GN}$. The noise samples used to create the desired average AWGN were generated using a random sequence with a

normal distribution that was complex with zero *mean*. With $P_{GN} = 1$, the associated scale factor ($S_F$) required to obtain the desired analysis $SNR_A$ is given by

$$S_F = \sqrt{10^{\frac{-SNR_A}{10}} \times P_C} \, . \tag{3.8}$$

Following the definition of $SNR$ as the ratio of total signal (without noise) to total noise (without signal), (3.6) can be rewritten to incorporate $P_{GN}$, shown as

$$SNR_A = 10 \times \log_{10}\left(\frac{P_C}{P_N + P_{GN}}\right)(dB) \, , \tag{3.9}$$

where it is noted that generally, the scaled AWGN power is far greater than the collected background noise power ($P_{GN}>>P_N$). This allows for (3.9) to be simplified, reducing it to

$$SNR_A = 10 \times \log_{10}\left(\frac{P_C}{P_{GN}}\right)(dB) \, . \tag{3.10}$$

Finally, the total estimated average power for $P_{GN}$ can be calculated following the expression for the total of any given arbitrary complex sequence as shown below

$$P_{GN} = \frac{1}{N_C} \sum_{i=1}^{N_C} S_F \cdot n_{GN}(i) S_F \cdot n^*_{GN}(i) \, . \tag{3.11}$$

where $n_{GN}(i)$ is the real power, and $n^*_{GN}(i)$ is the complex conjugate or reactive power, over $i$=1, 2, . . . , $N_C$ total samples. As described above, this process of generating AWGN and appropriately scaling it such that *Device Classification* could be performed over $SNR_A \in$[0 24] dB, was repeated and subsequently added to each extracted burst before RF-DNA fingerprint generation. Finally, it is noted that $SNR_A$ henceforth is referred to as $SNR \in$[0 24] dB throughout this document.

### 3.3 RF Fingerprint Generation

The overall ZigBee SHR as described in Section 3.2.3 (SHR + AWGN), while similar in structure when defined in terms of transmitted bits, is slightly different for each device

in terms of the physical waveform. The SHR therefore contains each device's unique signature. This unique signature comes from manufacturing tolerances, device aging characteristics, and differences in the manufacturing process. It is this unique, device-dependent signature that is exploited to generate RF-DNA fingerprints and perform *Device Classification*.

IEEE 802.15.4 defines the first 5 octets for all ZigBee signals. The first $T_P = 128$ $\mu$sec of each transmission corresponds to the *preamble*, and the following $T_S yn = 32$ $\mu$sec contains the *synchronization* information [24]. The collective preamble and sync information (128 $\mu$sec +32 $\mu$sec) makes up the total $T_S HR = = 160$ $\mu$sec) SHR, as illustrated in Fig.3.6. Accordingly, the duration of collected emissions, given $\Delta t = 1/f_s = 0.05$ $\mu$sec in each sample, is given by:

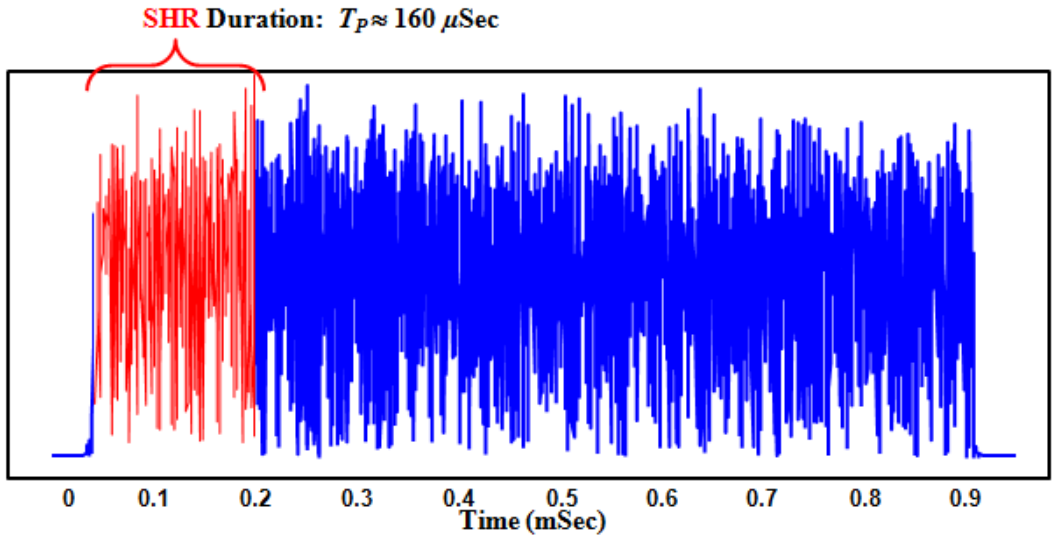


Figure 3.6: ZigBee transmission showing the SHR (highlighted in red) and the payload (highlighted in blue).

$$N_{Pre} = \frac{128\mu sec}{.05\mu sec} = 2560 samples. \tag{3.12}$$

$$N_{Syn} = \frac{32\mu sec}{.05\mu sec} = 640 samples. \tag{3.13}$$

$$N_{SHR} = 2560 + 640 = 3200 samples. \tag{3.14}$$

Recalling the constraint that $N_C/N_R$ must be an integer per Section 2.2.2, the SHR was divided into $N_R = 32$ equal subregions of 100 samples each, beginning at the start of the transmission (burst) and ending after the last sync sample as depicted in Fig. 3.7.

Each subregion of 100 samples contained three instantaneous signal responses ($a$, $\phi$, $f$) that uniquely described that subregion. Each instantaneous response was described by three RF-DNA statistics ($\sigma^2$, $\gamma$, $\kappa$). Accordingly, $\sigma^2$, $\gamma$, and $\kappa$ were calculated per (2.9)-(2.11) for each $a$, $\phi$, and $f$ for each of the $N_R = 32$ subregions as well as over the entire SHR for one final region such that the total number of regions was $N_{R+1} = 33$. Each statistic calculation represents a single RF-DNA "feature." It is these specific features that uniquely generated the RF-DNA fingerprints used for MDA/ML and GRLVQI *Device Classification*. In the case that all features were used to describe a unique fingerprint, known as "full-dimensional" (FD), the number of features is shown as

$$N_{FD} = (a, \phi, f) \times (\sigma^2, \gamma, \kappa) \times (N_{R+1}) = N_F = 297. \tag{3.15}$$

### 3.4 Dimensional Reduction Analysis

A process known as DRA was performed to reduce the number of features contained within each RF-DNA fingerprint for a given device. The overall DRA goal is to effectively reduce computational time and complexity, while maintaining a desired comparable

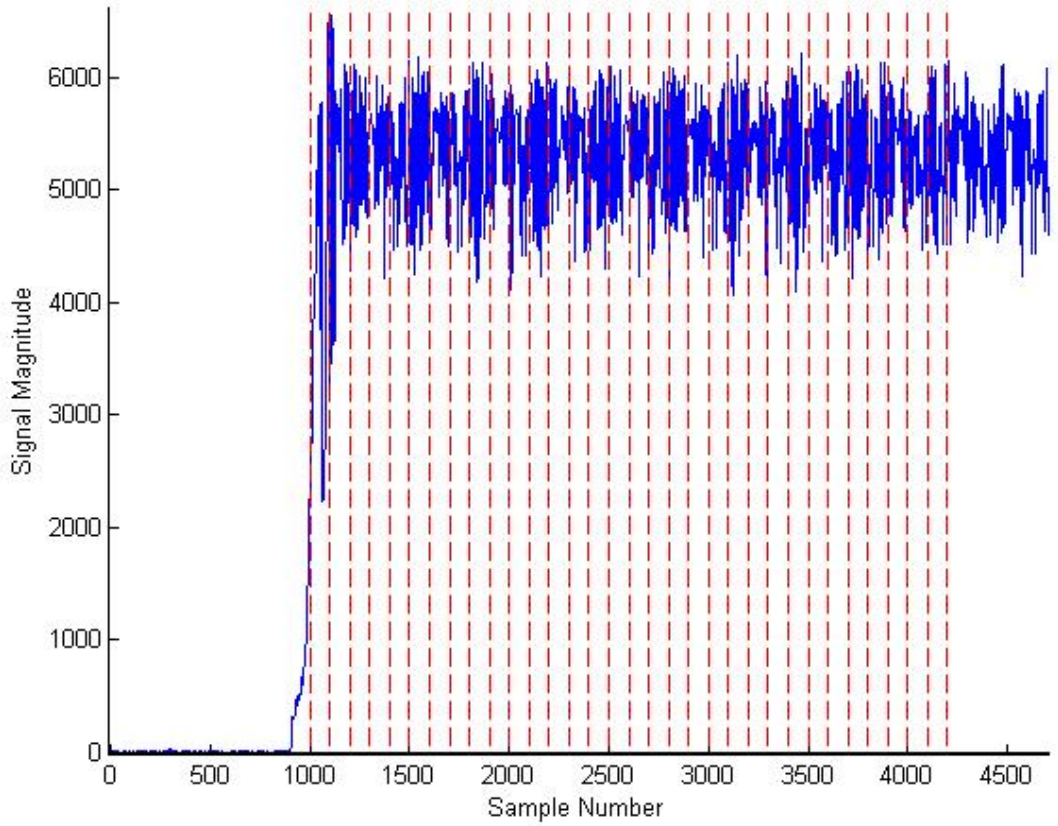


Figure 3.7: Magnitude response of a single burst SHR divided in to $N_R = 32$ subregions for subsequent RF-DNA fingerprinting. 100 samples are represented between each vertical red dashed line.

classification performance regardless of the receiver used. Two types, Quantitative DRA and Qualitative DRA are discussed next.

### *3.4.1 Quantitative DRA.*

The first method of DRA is enabled through GRLVQI and deals with the actual number of features $N_F$. Recall from Section 3.3 that the full-dimensional set of features describing an RF-DNA fingerprint for the Atmel RZUSBstick is $N_{FD} = N_F = 297$

features. This research followed the method in [9, 31] to iteratively reduce $N_F$ to a level that maintains the $\%C$=90% performance benchmark as will be described in Chap. 4. Quantitative DRA takes the GRLVQI relevance vector $\lambda_B$ from Section 2.4 and selects a specified number of salient features such that only the top-ranked $\lambda_i$ values are retained and used to represent the characteristic "space" of a particular class. These values are relevance ranked, meaning that the top-ranked (highest-valued $\lambda_i$) features have the greatest impact on *Device Classification*. Quantitative DRA can be performed using any desired $N_F$ provided the chosen value adheres to

$$N_{FD} \leq N_F > 0. \tag{3.16}$$

Selection of specific values used for $N_F$ here are described in Chap. 4, where results for $N_F = 5, 10, 33, 66$, and 99 features are provided.

### *3.4.2 Qualitative DRA.*

The other method of DRA selects feature-sets as a given instantaneous signal response subset as described in Section 2.2. Again the full-dimensional feature-set for a given RF-DNA fingerprint included $N_{FD} = N_F = 297$ features. These features were composed of statisticas $(\sigma^2, \gamma, \kappa)$ calculated for the instantaneous $(a, \phi, f)$ responses of a given burst. Given three responses for each full-feature RF-DNA fingerprint,

$$N_{F(a)} = N_{F(\phi)} = N_{F(f)} = 99, \tag{3.17}$$

where during RF-DNA fingerprint generation, response features were organized sequentially in RF-DNA fingerprints according to

$$\mathbf{F} = [F(a) \vdots F(\phi) \vdots F(f)]_{1\times 297}, \tag{3.18}$$

where indices in $\mathbf{F}$ are given by:

$$a : i \in [1\ 99]; \phi : i \in [100\ 198]; f : i \in [199\ 297]. \tag{3.19}$$

Each subset was analyzed seperately, meaning that in one case for example, $\phi$-only features were used. In each case, relevance rankings ($1 - 99$ with "1" being noted as the "top feature" and thus having the biggest effect on *Device Classification*) were assigned to the given subset of $\lambda_i$ values. This process was repeated for each instantaneous response $(a, \phi, f)$ to obtain an accurate comparison among the subsets of their effects on *Device Classification*. Additionally, this enabled direct comparison with Quantitative DRA for $N_F = 99$ (where the number of features may be composed of features from any and all of the $a, \phi$, or $f$ subsets).

## 3.5 Device Discrimination

As described in Chap. 2, two methods of *Device Discrimination* were performed using identical sets of RF-DNA fingerprints, MDA/ML and GRLVQI. Fig. 3.8 [41] shows the basic discrimination process (in block diagram form) that all classifiers follow. Additionally, DRA was performed using a model generated from GRLVQI and its associated $\lambda$ values; all methods of *Device Classification* performed will be shown in Section 3.5.3.

### *3.5.1 MDA/ML Model Development and Classification.*

The development here is taken exclusively from [9] and presented here for completeness. MDA/ML as described in Section 2.3 is a two-step discrimination process that involves both MDA model development and ML *Device Classification*. It is an extension of Fisher's Linear Discriminant and used for $N_{Cl} > 2$. This research was conducted for six devices (classes), $N_{Dev} = N_{Cl} = 6$, and it thus follows from Section 2.3.1 that $N_D = (N_{Cl} = 6) - 1 = 5$ dimensions.

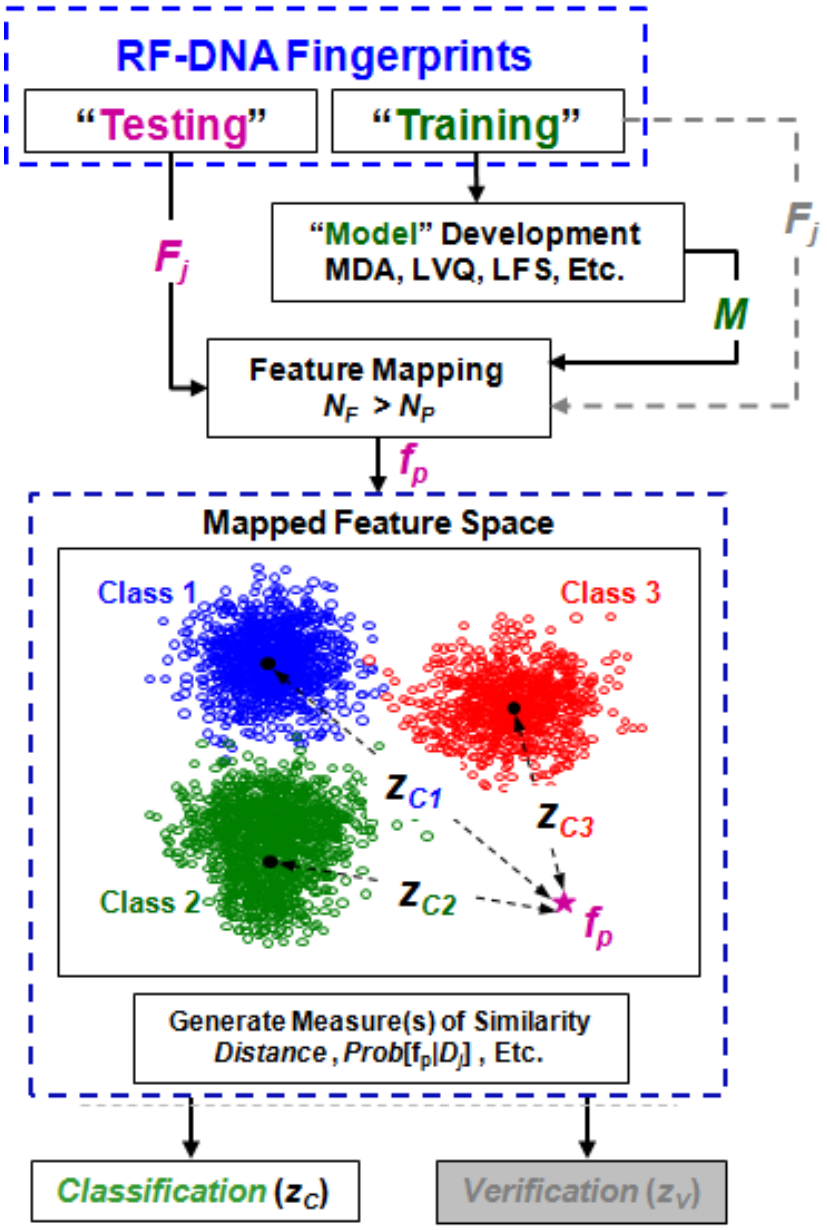


Figure 3.8: Block diagram of device discrimination process showing model development, usage of test statistics, and subesequent classification [41]. It is noted that "verification" is possible after model development as well but not addressed in this research and therefore grayed out.

MDA/ML was performed using RF-DNA fingerprints from both the PXIe and USRP NI receivers for three different models:

1. Single Receiver: PXIe-only *Training* fingerprints

2. Single Receiver: USRP-only *Training* fingerprints

3. Hybrid Cross-Receiver: Combined PXIe and USRP *Training* fingerprints

Each model was developed by MDA through input feature dimensional reduction. The full-dimensional feature-set, $N_F$=297, RF-DNA *Training* fingerprints were projected onto the $N_D$=5-dimensional subspace. This was done using an iterative method known as a $K$-fold process as described in detail in [9]. $K$-fold is a method that uses cross-validation to develop the "best" model for use in *Device Classification* as shown in Fig. 3.9 [9]. The best model, as discussed in Section 2.3.1, refers to the model that leaves the maximum distance between the *mean* of each class and simultaneously minimizes the *variance* within any single class [12]. This research utilized a $K$=5 approach for model development. Once the best model ($W_B$) was selected, that model formed the projection matrix ($\mathbf{W}$) as discussed in Section 2.3.1. The fingerprints ($F_j$) were then projected according to (2.19), with the resulting $\hat{\mathbf{f}}$ representing the lowered-dimensional projected RF-DNA fingerprints. Following projection of all RF-DNA fingerprints, the feature space describing each class was "mapped" accordingly into the Fisher Space (Fig.3.10) such that the "decision boundaries" defining each respective class were formed. ML was then used to perform *Device Classification*.

ML classification, as described in Section 2.3.2, was accomplished using the remaining *Testing* fingerprints that were set aside during MDA model development. Each of the $N_{Dev} = 6$ devices were represented and the process again assumed Multivariate Guassian (MVG) distributions. The distributions were each described by their class-specific *means* ($\hat{\mu}_i$) where $i = 1, 2, ...(N_{Cl} = 6)$, and a collective *covariance* for all devices ($\hat{\Sigma}_P$) as calculated in (2.20). Additionally, all prior probabilities and device likelihoods

were assumed to be equal. Each *Testing* fingerprint was classified one at a time following the iterative process [9]:

1. Input *Testing* fingerprint $\mathbf{F}_j$ from an unknown class $c_j$.
2. Project $\mathbf{F}_j$ into the Fisher space using (2.19) to generate projected fingerprint $\hat{\mathbf{f}}_j$.
3. Associate $\hat{\mathbf{f}}_j$ to one of the known classes (devices) based on its maximum conditional likelihood probability according to

$$c_i \ : \ \arg\max_i \Big[ \ p(c_i|\hat{\mathbf{f}}_j) \ \Big], \tag{3.20}$$

where $i$=1, 2, . . . , ($N_{Cl}$ = 6) and $p(c_i|\hat{\mathbf{f}}_j)$ is the conditional likelihood probability that projected fingerprint $\hat{\mathbf{f}}_j$ belongs to class $c_i$. The overall measure of effectiveness for the classifier ($\%C$) is the percentage of the time the classifier correctly assigns the fingerprint to its true device or class over all trials performed. "Correct" classification notes when $\hat{\mathbf{f}}_j$ is classified as its known $c_i$ for a single trial.

### *3.5.2 GRLVQI Model Development and Classification.*

The development here is taken exclusively from [18, 31] and presented here for completeness. GRLVQI processing follows the same basic process shown in Fig. 3.8 [41]. Unlike MDA/ML though, GRLVQI, as described in Section 2.4, performs model development and *Device Classification* jointly, rather than as two independent processes.

GRLVQI requires no prior assumption of MVG distribution and additionally, requires no knowledge of or assumption of any specific statistical distribution for model development. It uses a specified number of prototype vectors to "shape" the space of each class. This research utilized $N_P$ = 10 prototype vectors to describe each class, with each prototype vector being comprised of $N_F$ = 297 features for full-dimensional analysis. The

collection of all prototype vectors, $\mathbf{p}^n$ as derived in (2.25) [18], was used to iteratively shift intra-class ($\mathbf{p}^n$) and inter-class ($\mathbf{p}^o$) prototype vectors until a "best model" was achieved according to (2.26) [18]. Model development and subsequent classification followed the process as shown below:

1. Randomly choose a *Training* fingerprint ($\hat{\mathbf{f}}^m$) and relevance-ranked feature ($\lambda_i$) and input to (2.26).

2. Shift prototype vectors describing class "space" by distortion factor $d_\lambda^n$

3. Continue to iteratively shift protype vectors by $d_\lambda^n$ and update corresponding relevance-rankings ($\lambda_i$) until "best-fit model" is achieved by defined smallest $d_{Bias}^n$ as described in [31]

4. Define "best-fit" relevance ranking vector ($\lambda_B$) as the vector containing $\lambda_i$ for $i = 1, 2, 3, \ldots, N_F$; higher-valued $\lambda_i$ correspond to most relevant features used in describing a class.

5. Measure euclidian distance from a single *Testing* fingerprint ($\hat{\mathbf{f}}$) to each of the prototype vectors as defined by the best model.

6. Associate the unknown $\hat{\mathbf{f}}$ to one of the known $c_i$ based on the smallest euclidean distance to the prototype vectors of a specified $c_i$ following

$$c_i : \min_{i,j}(d_\lambda^p(\mathbf{p}_{i,j}, \hat{\mathbf{f}})) \tag{3.21}$$

where $i$=1, 2, . . . , ($N_{Cl} = 6$) and $j$=1, 2, . . . , ($N_P = 10$). As with MDA/ML, $\%C$ provides the measurement of classifier effectiveness and "correct" classification occurs when $\hat{\mathbf{f}}_j$ is classified as the true known $c_i$.

### *3.5.3 Comparative Assesment Test Matrix.*

The full spectrum of assesments performed, including full-dimensional and DRA (quantitative and qualitative) using both MDA/ML and GRLVQI is shown in Table. 3.2. The results of these tests, which allow for an accurate comparison of both classification methods, as well both receivers are further discussed in Chap. 4.

Table 3.2: Comparative Assesment Test Matrix: **1** Full-Dimensional Baseline (MDA/ML & GRLVQI), **2** Quantitative DRA (GRLVQI), **3** Quantitative vs. Qualitative DRA (GRLVQI), and **X** denotes Test Not Performed

| **Num Feats** | **MDA/ML** | | **GRLVQI** | |
|---|---|---|---|---|
| | PXIe | USRP | PXIe | USRP |
| Full Dim 297 | 1,2 | 1,2 | 1,2 | 1,2 |
| Qual DRA 99 | **X** | **X** | 3 | 3 |
| Quan DRA 99 | **X** | **X** | 2 | 2 |
| 66 | **X** | **X** | 2 | 2 |
| 33 | **X** | **X** | 2 | 2 |
| 10 | **X** | **X** | 2 | 2 |
| 5 | **X** | **X** | 2 | 2 |

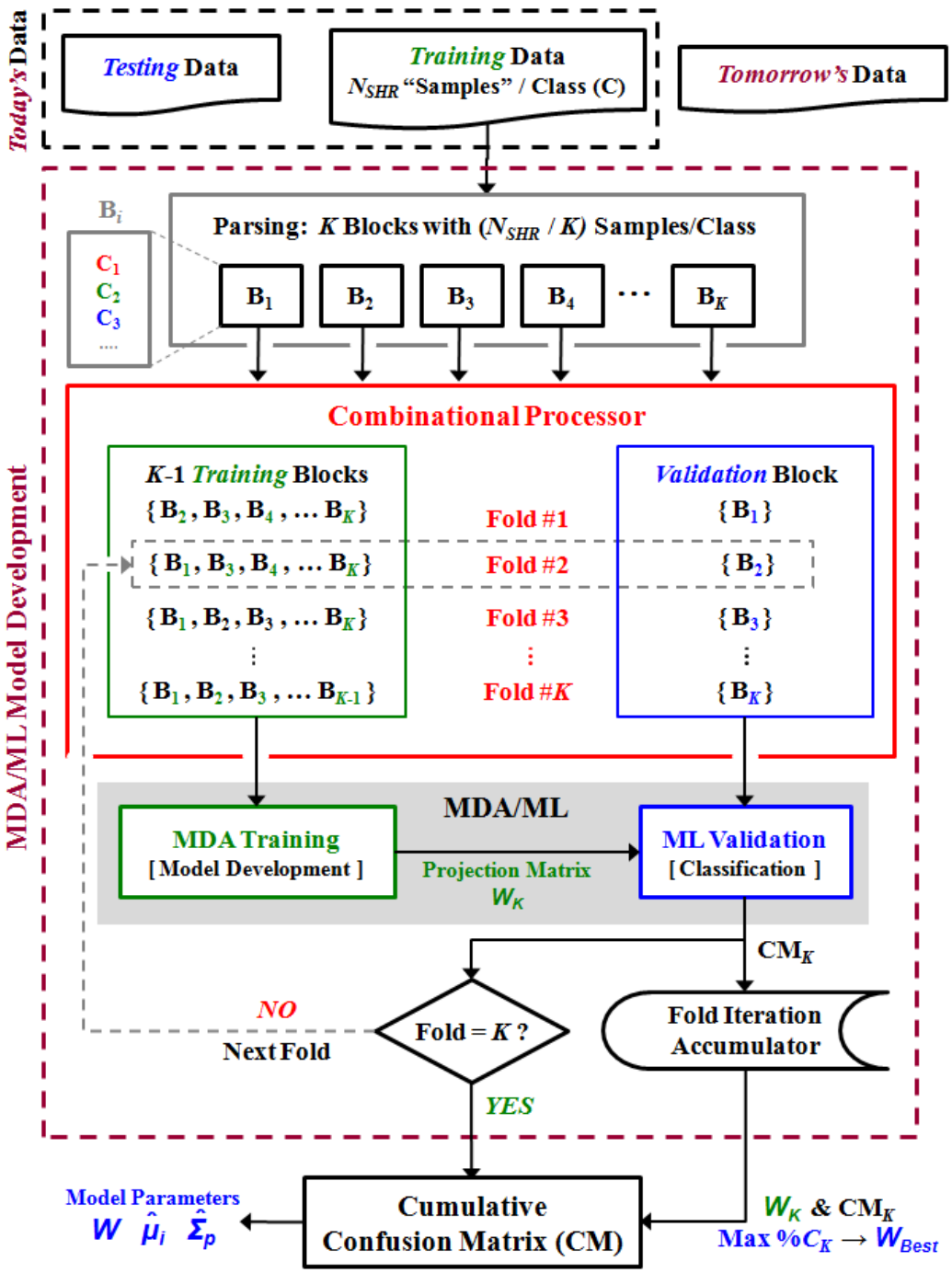


Figure 3.9: An illustration of the $K$-fold training process used for MDA model development. The "best" model $\mathbf{W}_B$ is selected based on the $\mathbf{W}_K$ that yields the highest $\%C_k$. This $\mathbf{W}_B$ then becomes the model projection matrix used for subsequent classification and verification [9].

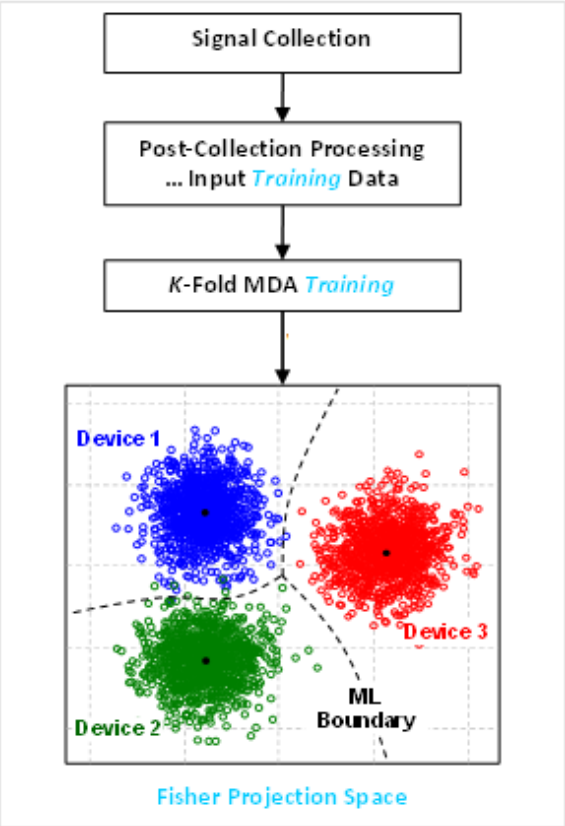


Figure 3.10: Signal collection, post-collection processes and $K$-fold cross-validation training for MDA model development. This depicts a representative $N_{Dev}$=3 ZigBee devices (classes) and the corresponding 2D Fisher Space. Each (o) represents a projected training fingerprint $\hat{\mathbf{f}}$ clustered around the respective class *means* shown as (•) [9].

# IV. Results and Analysis

This chapter contains device discrimination results for six ZigBee devices using emissions collected on National Instruments (NI) PCI Extension for Instrumentation Express (PXIe) and Universal Software Radio Peripheral (USRP) receivers. *Device Classification* was performed on both full-dimensional as well as *qualitative* and *quantitative* Dimensional Reduction Analysis (DRA) feature-sets. DRA was performed using Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) relevance-ranked features. Subsequent classification of fingerprints from both receivers using DRA was only performed using the GRLVQI method previously discussed in Section 3.4. Finally, *Device Classification* was executed on the *Hybrid* fingerprints. Here, the term *Hybrid* is used in different context from [9] and describes Cross-Receiver model development using RF-DNA fingerprints derived from PXIe and USRP collections. As with the single-receiver setup described above, both full-dminesional and *quantitative only* DRA feature-sets were used for *Device Classification*. Section 4.1 describes how the model was developed after dividing the prints into *Training* and *Testing* sets. Section 4.2 discusses full-dimensional fingerprint *Device Classification* using both Multiple Discriminant Analysis, Maximum Likelihood (MDA/ML) and GRLVQI methods and compares performance of PXIe and USRP. Section 4.3 details the DRA process, including specific *quantitative* $N_F$ selection and comparison of *qualitative* versus *quantitative* features for PXIe and USRP receivers. Section 4.4 presents *Hybrid Cross-Receiver* model development and shows MDA/ML and GRLVQI *Device Classification* performance results for full-dimensional fingerprints while Section 4.5 compares *quantitative* DRA *Device Classification* results for MDA/ML and GRLVQI models.

## 4.1 Classification Model Development

The classification model for single-receiver assessment was developed using PXIe and USRP collections seperately. Specifically, a number of Synchronization Header Response (SHR) from ZigBee emissions from each receiver were split into *Training* ($N_{SHR}$ = 300) and *Testing* ($N_{SHR}$ = 300) for $N_{Cl}$ = 6 classes. Further, a given number of noise realizations were like-filtered and used for Monte Carlo simulation. The total of $N_{IR}$ used for Monte Carlo simulation for each device included:

$N_{IR} = (N_{SHR} = 600) \times (N_{Nz} = 15) = 9000$ Independent Realizations.

Of this total, $N_{IR}$ = 4500 independent realizations for each device were used for "*Training*," to develop the model via projection (MDA/ML) and with prototype vectors (GRLVQI) as described in Section 3.5.1 and Section 3.5.2. The remaining $N_{IR}$ = 4500 were set aside for "*Testing*," and assessing *Device Classification*.

## 4.2 Single Receiver Classification: Full-Dimensional (MDA/ML and GRLVQI)

Both classification methods were used for full-dimensional *Device Classification* where in this case, $N_F$ = 297. This was derived from the fact that each SHR was described by three instantaneous responses ($a$ = **amplitude**, $\phi$ = **phase**, $f$ = **frequency**), each of which were in turn described by three statistics ($\sigma^2$ = **variance**, $\gamma$ = **skewness**, $\kappa$ = **kurtosis**). Further, each SHR divided into a fixed $N_R$ = 32 subregions across the entire SHR. The statistics of each response were taken withinin each subregion resulting in a total of:

$$N_{FullFeat} = (a, \phi, f) \times (\sigma^2, \gamma, \kappa) \times (N_{R+1} = 33) = N_F = 297. \tag{4.1}$$

Each RF-DNA fingerprint used for either model development of classification thus contains $N_F$ = 297. Classification was performed on both PXIe and USRP using both

MDA/ML and GRLVQI. Fig. 4.1 shows full-dimensional classification performance for fingerprints used for *Testing*. This was done for $SNR \in$[0 24] dB, keeping in context of [30]. The performance of each device at each $SNR$ is shown as well as the cross-device average performance for all devices noted as "**Average**." A desired benchmark of $\%C$=90% was set for easy comparison of full-dimensional and DRA performance. It can be seen in Fig. 4.1 that while it requires a range of $SNR \in$[8.5 24] dB to do so, each device as well as their average achieves the benchmark for both receivers and both methods.

With the baseline for full-dimensional classification established, the remainder of this paper will drop device-specific comparison and provide analysis only on the "**Cross-Device Average**" performance of all given devices. Fig. 4.2 shows the same classification performance as Fig. 4.1 with the devices removed, leaving only the cross-device average for each receiver and method for comparison. Table. 4.1 provides a quick-reference chart for Fig. 4.2, showing the $SNR$ value at which each cross-device average achieves the arbitrary $\%C$=90% benchmark. When averaging performance for each individual receiver across both methods, it can be seen that the higher end PXIe receiver clearly outperforms the lower end USRP receiver by $SNR \approx 4.9$ dB. Additionally, GRLVQI, when averaged across both receivers, performs consistently poorer, requiring $SNR \approx 2.0$ dB gain to match MDA/ML performance.

### 4.3 Single Receiver Classification: DRA Performance (GRLVQI)

Due to the nature in which it is calculated, MDA/ML does not allow for DRA to be performed as it does not provide relevance-ranking values for specific features as does GRLVQI. Refering back to GRLVQI performance in Table. 4.1, PXIe achieved the $\%C$=90% benchmark at $SNR \approx 12.0$ dB and USRP at $SNR \approx 18.0$ dB. It is from these two $SNR$ values that DRA was performed respectively for each receiver.

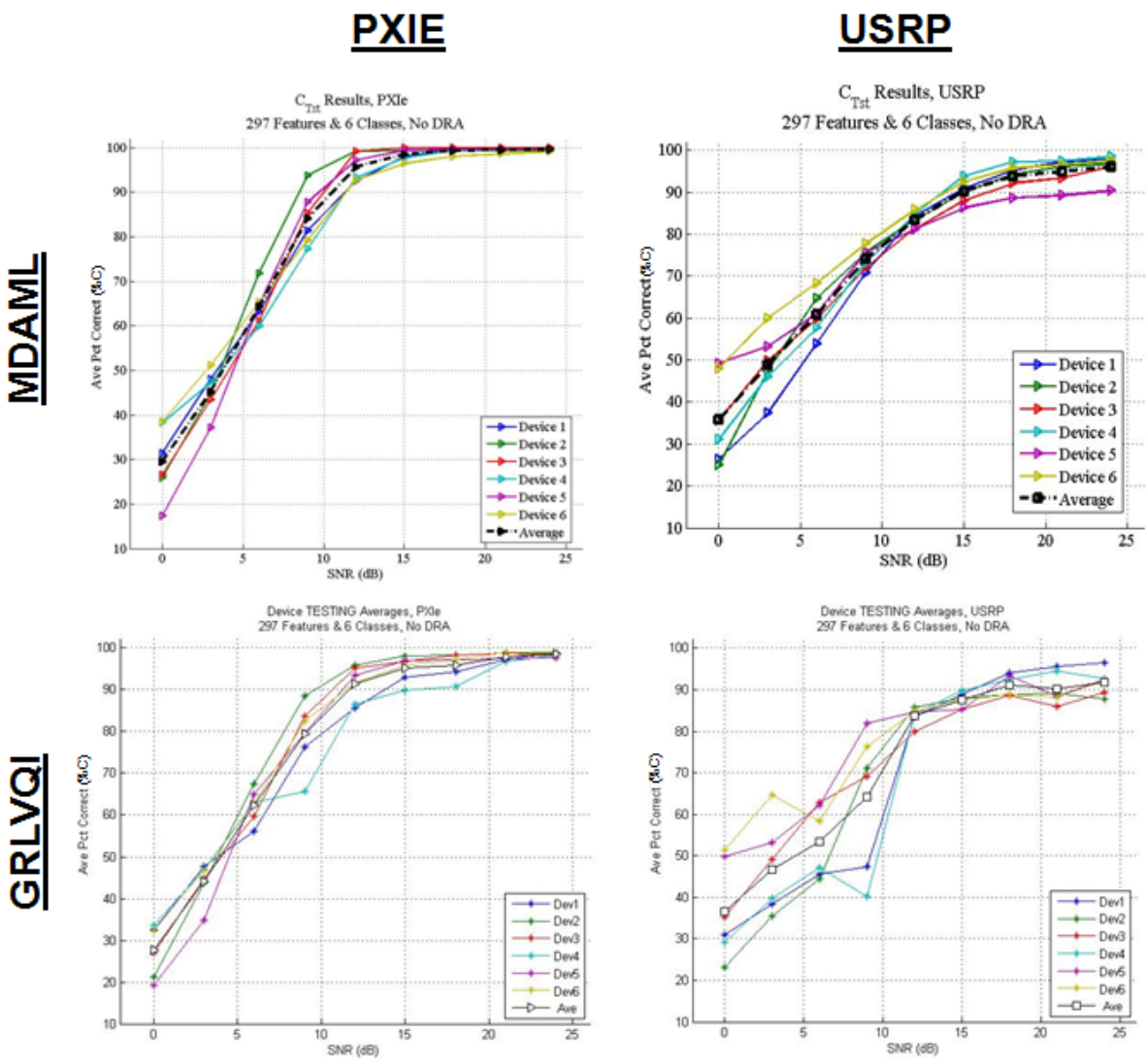


Figure 4.1: Full-dimensional ($N_F = 297$) classification comparing PXIe and USRP using both MDA/ML and GRLVQI processes for $N_{Cl} = 6$. This shows all device averages as well as the aggregated cross-device average

### *4.3.1 Quantitative DRA Performance.*

Quantitative DRA was first performed in order to see how far of a reduction in features the model could be developed with before *Testing* performance suffered signifigantly.

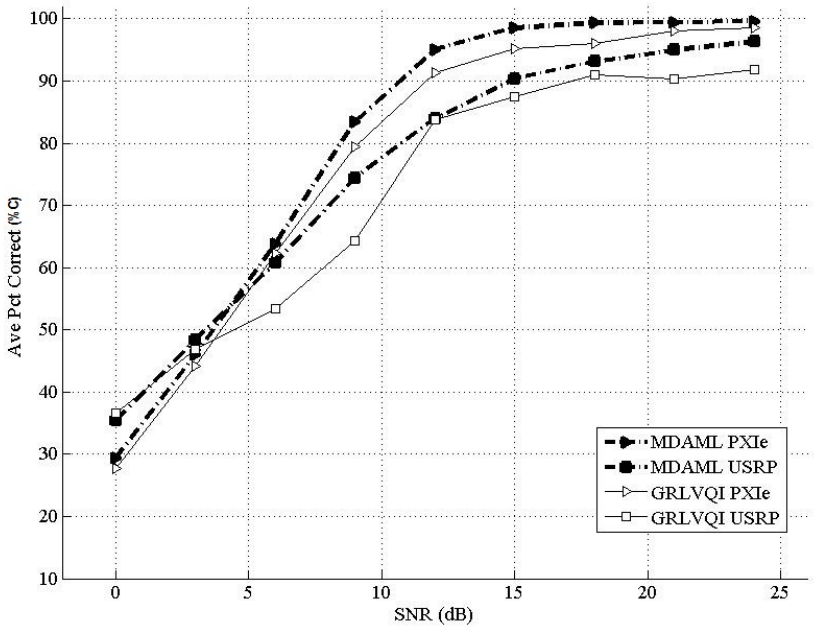


Figure 4.2: Full-dimensional ($N_F = 297$) Cross-Device Averages for both receivers and both classifiers.

Table 4.1: Full-dimensional ($N_F = 297$) Cross-Device Average Benchmark Performance Comparison.

| Method | Receiver | SNR |
|---|---|---|
| MDAML | PXIe | 10.5 dB |
| | USRP | 14.9 dB |
| GRLVQI | PXIe | 11.8 dB |
| | USRP | 17.6 dB |

Signifigant degradaded performance is defined as a shift in $SNR$ at which meeting the $\%C$=90% benchmark either requires more gain (positive dB) from the full-dimensional case, or where the benchmark is never achieved for $SNR\in$[0 24] dB. Refering to Section 4.2 where each fingerprint is made up of three responses ($a$, $\phi$, $f$), each providing $N_F$ = 99 features, quantitative DRA began with $N_F$ = 99. DRA was subsequently repeated over all $SNR$ values as before, reducing by 33% first to ensure performance was not degraded. It was then repeated with increased % reduction each time until performance for either PXIe or PXIe began to suffer. Overall, quantitative DRA was performed for ($N_F = 5, 10, 33, 66$ and 99) features. Fig. 4.3 shows both receivers' cross-device average for the full-dimensional feature-set as well as each $N_F$ DRA. It is observed that as in full-dimensional analysis in Section 4.2, high-value PXIe outperforms low-value USRP as DRA is increased and $N_F$ is decreased. PXIe in fact consistently achieves the $\%C$=90% benchmark at the full-dimensional prescribed $SNR \approx 12.0$ dB for all except $N_F = 5$. PXIe does however, unlike USRP, always achieve the benchmark overall. At $N_F = 10$ features, USRP performance begins to suffer, requiring an additional gain of $SNR \approx 6.0$ dB. It then quickly degrades to where the benchmark isn't even achieved at $N_F = 5$ features.

### *4.3.2 Qualitative DRA Performance.*

Qualitative DRA, describing features by their signal responses ($a$, $\phi$, $f$) was then performed on both receivers using GRLVQI. Previous research [9] has suggested that unique RF-DNA signatures of ZigBee devices tend to be easier distinguished when looking at the phase ($\phi$) features of the SHR. Response-specific DRA was performed such that $N_F$ = 99 each for ($a$, $\phi$, $f$). A model was created for each response feature-set seperately. A comparison of these qualitative features as well as the quantitative DRA for $N_F$ = 99 is seen in Fig. 4.4. Along with the full-dimensional feature set for each receiver from Section 4.2, it is clear that for the Atmel ZigBee devices used, ($\phi$)-only features far outperform $a$ and $f$. Additionally, $\phi$-only feature-set for both receivers performs just as well as full-

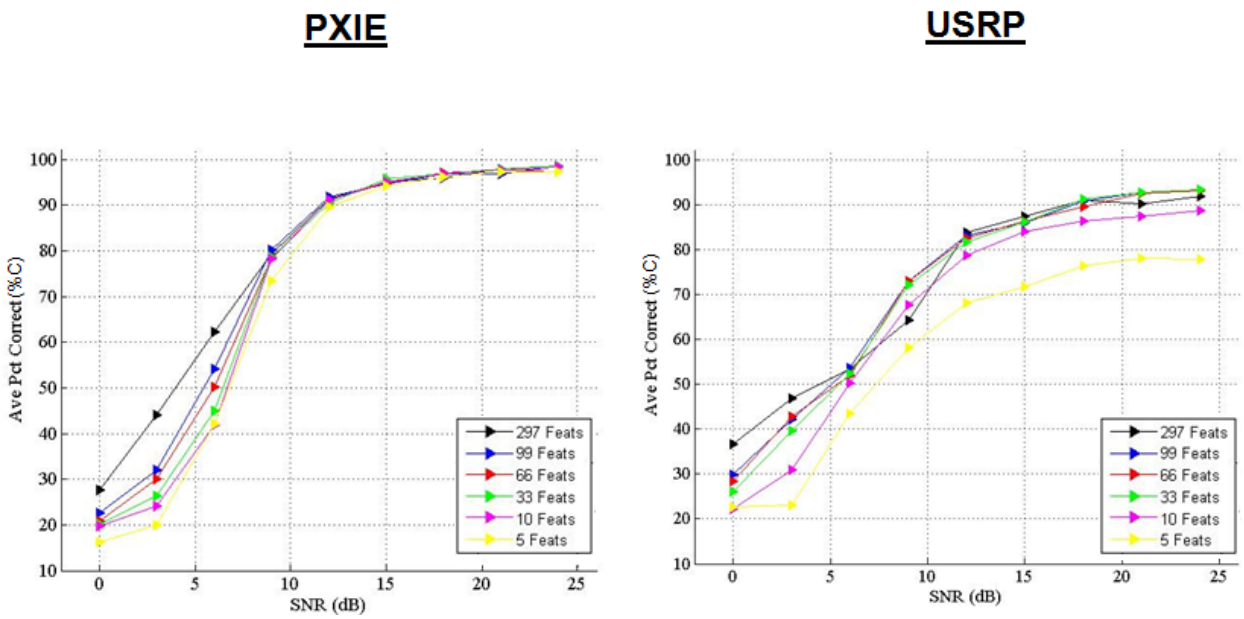


Figure 4.3: Quantitative DRA ($N_F = 5, 10, 33, 66, 99$ and 297) Cross-Device Averages Benchmark Comparison

dimensional and quantitative DRA for $N_F = 99$ features. It is no surprise that PXIe continues to outperform USRP, achieving the $\%C$=90% benchmark with an $SNR \approx 6.2$ dB gain

## 4.4 Hybrid Cross-Receiver Classification: Full-Dimensional and Quantitative DRA

The model for the cross-receiver setup was developed in a similar fashion to the single-receiver model described in Section 4.1. In the *Hybrid Cross-Receiver* setup though, the model was developed by combining PXIe and USRP fingerprints. Again, each receiver provided $N_{SHR} = 600$ ZigBee responses, which were divided into *Training* and *Testing*. The *Hybrid Cross-Receiver* model though, containing fingerprints from both receivers, was split, with *Training* = $N_{SHR} = 600$ and two sets (one for each receiver) of *Testing* = $N_{SHR} = 300$ for each of the $N_{Cl} = 6$ classes. As in the single-receiver model, $N_{Nz} = 15$ like-filtered, independent Monte Carlo Noise realizations were added to each ZigBee response

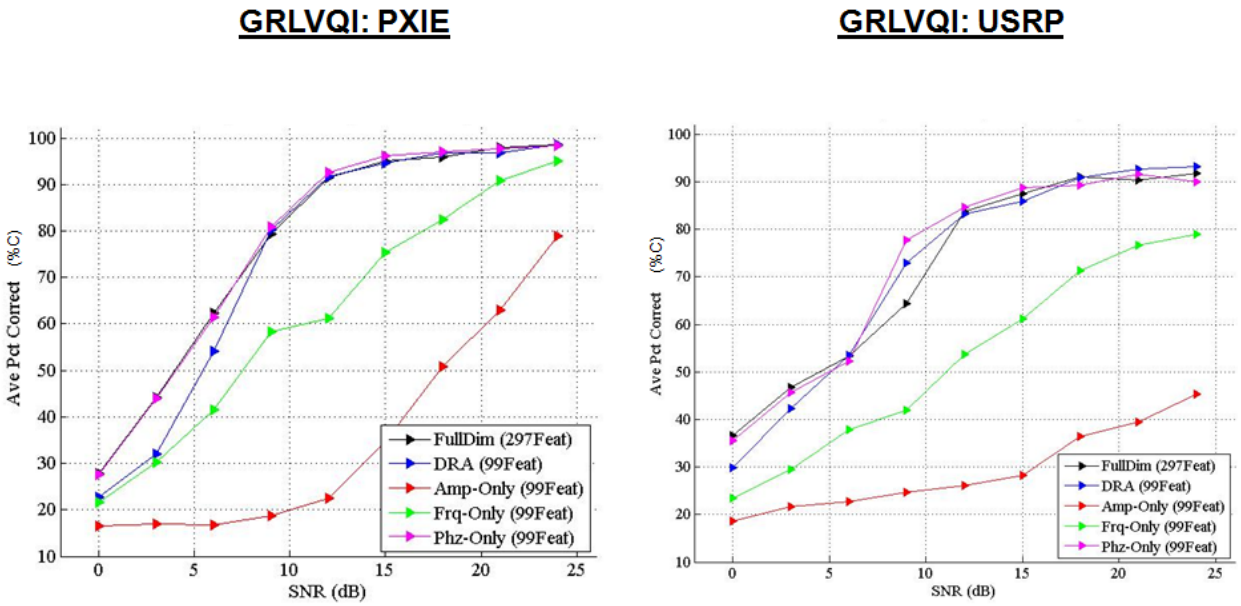


Figure 4.4: Quantitative DRA ($N_F$ = 99 & 297) versus Qualitative DRA ($N_F$ $(a, \phi, f)$ = 99) Cross-Device Averages Benchmark Comparison.

for each device to develop $N_{IR}$ independent realizations given by:

$$N_{IR} = (N_{SHR} = 600) \times (N_{Nz} = 15) \times (2 \text{ Receivers}) = 18000.$$

The *Hybrid Cross-Receiver* was then, in contrast to Section 4.1, developed with $N_{IR}$ = 9000 independent realizations labeled "*Training*." The remaining "*Testing*," fingerprints were split into three cases as summarized in Table. 4.2.

In Case 1, the "*Testing*" fingerprints were a combination of the reserved fingerprints for both receivers, thus $N_{IR}$ = 4500 for each device. Case 2 and Case 3 tested the same *Hybrid Cross-Receiver* model on only one receiver at a time. The reserved $N_{IR}$ = 2250 per device for PXIe and $N_{IR}$ = 2250 for USRP were used as "*Testing*" fingerprints for *Device*

Table 4.2: Case Descriptions for *Hybrid Cross-Receiver* Training (Model Development) and *Device Classification* Testing

| Scenario | Training (Model) | Testing |
|---|---|---|
| Case 1 | PXIe & USRP | PXIe & USRP |
| Case 2 | PXIe & USRP | PXIe |
| Case 3 | PXIe & USRP | USRP |

*Classification* in Case 2 and Case 3 respectively.

Both Full-Dimensional and Quantitative DRA *Device Classification* were performed using both MDA/ML and GRLVQI. It is important to note though, that while DRA was performed using MDA/ML, the relevance-ranked features used to allow this, were actually taken from the models developed using GRLVQI. Additionally, DRA for both MDA/ML and GRLVQI for all three cases shown in Table. 4.2, was performed at $SNR = 18.0$ dB. This value was determined by recalling from Section 4.3 that the $\%C$=90% benchmark was achieved in the worst case, for both receivers, at $SNR \approx 18.0$ dB.

### *4.4.1 Case 1: Hybrid Cross-Receiver Testing.*

The *Hybrid Cross-Receiver* fingerprints used for *Testing* were again a combination of reserved, interleaved PXIe and USRP fingerprints. Fig. 4.5 shows a Full-Dimensional ($N_F = 297$) and Quantitative DRA ($N_F = 5, 10, 33, 66, 99$) *Device Classification* comparison of MDA/ML and GRLVQI. Table. 4.3 shows clearly that for a Full-Dimensional feature-set, MDA/ML is superior to GRLVQI, requiring nearly $SNR \approx 2.0$ dB less gain to achieve $\%C$=90%. GRLVQI immediately surpasses MDA/ML for Quantitative DRA, providing a $SNR \approx 3.5$ dB gain for $N_F = 99$. Subsequent MDA/ML DRA performance fails to even

meet the $\%C$=90% benchmark as GRLVQI DRA remains mostly consistent even as $N_F$ decreases.

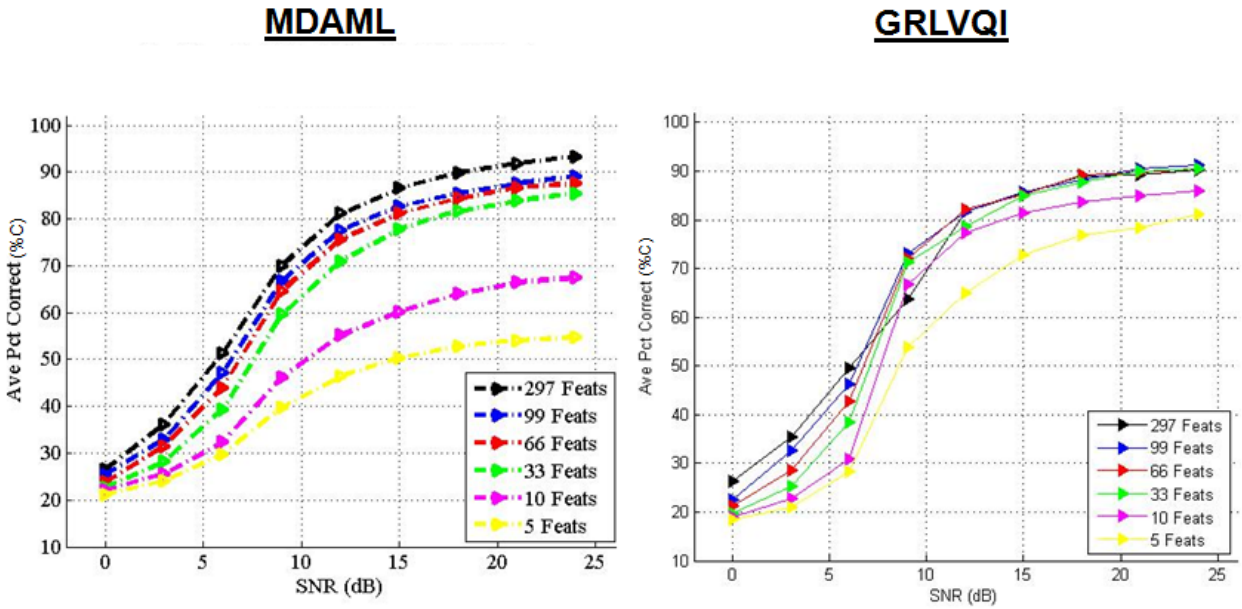


Figure 4.5: **Case 1**: Full-Dimensional ($N_F$ = 297) and Quantitative DRA ($N_F$ = 5, 10, 33, 66, 99) *Device Classification* using *Hybrid Cross-Receiver* model and *Hybrid Cross-Receiver* testing.

Table 4.3: Case 1: GRLVQI "Gain" relative to MDA/ML. "**X**" indicates an incalculable value given the $\%C$=90% benchmark is never achieved within $SNR\in$[0 24] dB.

| $N_F$ | 297 | 99 | 66 | 33 | 10 | 5 |
|---|---|---|---|---|---|---|
| GRLVQI "Gain" (dB) | -2.3 | 3.5 | X | X | X | X |

### *4.4.2 Case 2: PXIe Only Testing.*

Fingerprints used for **Case 2** *Testing* were entirely from PXIe fingerprints held out of model development. Fig. 4.6 compares Full-Dimensional ($N_F$ = 297) and Quantitative DRA ($N_F$ = 5, 10, 33, 66, 99) *Device Classification*, again for MDA/ML and GRLVQI. Table. 4.4 show that while MDA/ML initially is marginally better when running Full-Dimensional features, GRLVQI performance remains consistent as $N_F$ decreases and far outperforms MDA/ML. It is noted also, that unlike in **Case 1**, MDA/ML performance on its own is much better, meeting the $\%C$=90% benchmark for all but $N_F$ = 5.

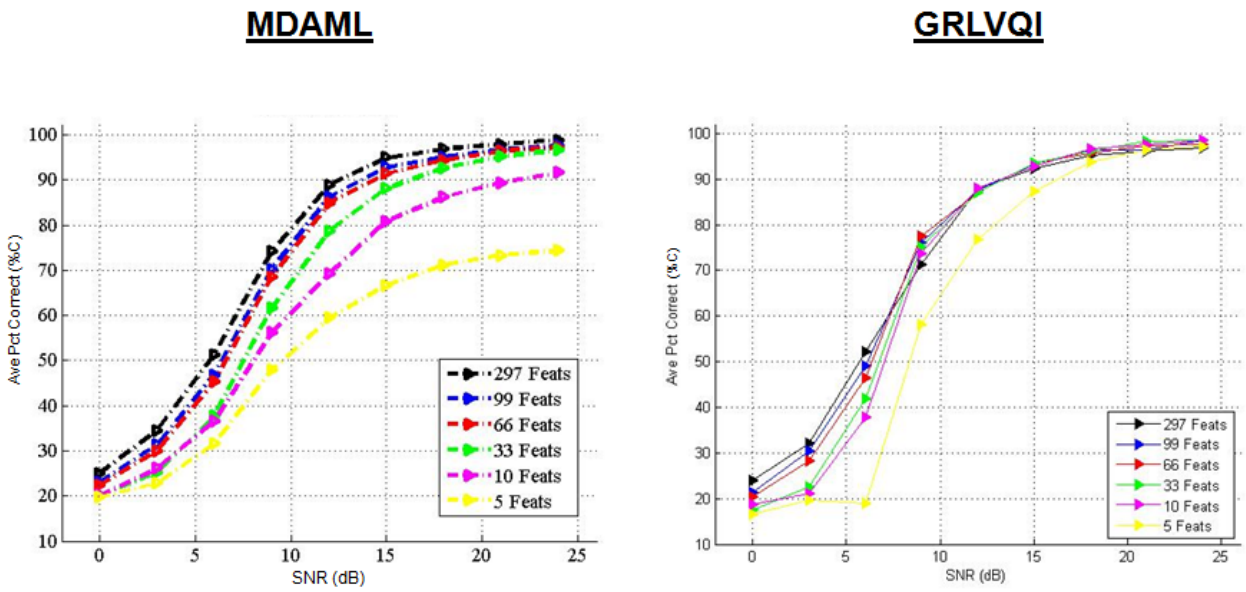


Figure 4.6: Case 2: Full-Dimensional ($N_F$ = 297) and Quantitative DRA ($N_F$ = 5, 10, 33, 66, 99) *Device Classification* using *Hybrid Cross-Receiver* model and PXIe only testing.

### *4.4.3 Case 3: USRP Only Testing.*

**Case 3** *Testing* fingerprints are comprised of only USRP fingerprints held out of model development. Fig. 4.7 compares Full-Dimensional ($N_F$ = 297) and Quantitative DRA ($N_F$

Table 4.4: Case 2: GRLVQI "Gain" relative to MDA/ML. "**X**" indicates an incalculable value given the $\%C$=90% benchmark is never achieved within $SNR\in$[0 24] dB.

| $N_F$ | 297 | 99 | 66 | 33 | 10 | 5 |
|---|---|---|---|---|---|---|
| GRLVQI "Gain" (dB) | -0.9 | 0.5 | 1.1 | 2.8 | 8.7 | X |

= 5, 10, 33, 66, 99) *Device Classification*, using both classification methods. It can be seen from Table. 4.5 that the *Hybrid Cross-Receiver* model is unsuitable for performing *Device Classification* with fingerprints only from the lower end USRP receiver. Both MDA/ML and GRLVQI fail to achieve the $\%C$=90% benchmark even with the Full-Dimensional feature-set. While both methods perform poorly, GRLVQI performance is still measurably better as it stays relatively consistent as $N_F$ decreases.

Table 4.5: Case 3: GRLVQI "Gain" relative to MDA/ML. "**X**" indicates an incalculable value given the $\%C$=90% benchmark is never achieved within $SNR\in$[0 24] dB.

| $N_F$ | 297 | 99 | 66 | 33 | 10 | 5 |
|---|---|---|---|---|---|---|
| GRLVQI "Gain" (dB) | X | X | X | X | X | X |

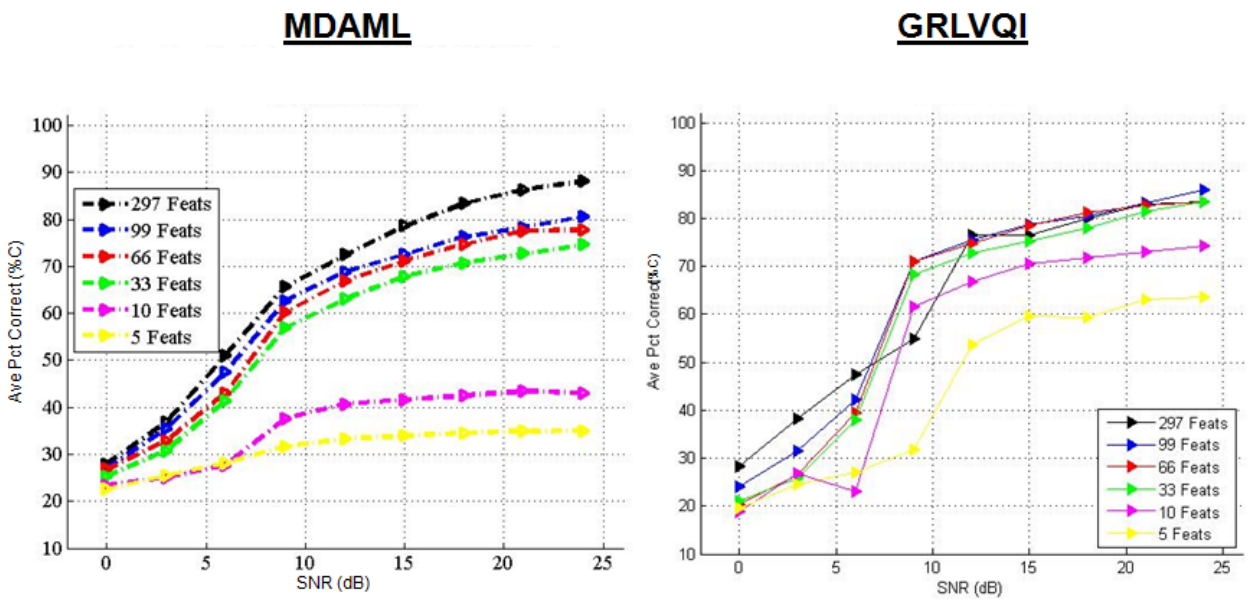


Figure 4.7: Case 3: Full-Dimensional ($N_F = 297$) and Quantitative DRA ($N_F = 5, 10, 33, 66, 99$) *Device Classification* using *Hybrid Cross-Receiver* model and USRP only testing.

# V. Conclusion

This chapter provides a summary of reseach performed, findings and contributions to the Radio Frequency Distinct Native Attribute (RF-DNA) fingeprinting process, and recommendations for follow-on research.

## 5.1 Summary

ZigBee-based networks are an affordable, widely-used option for accomplishing a multitide of tasks within Wireless Personal Area Network (WPAN) applications. Due to their low energy requirements, commercial availability, and low implementation complexity, ZigBee WPANs are found in many buisnesses, hospitals, and homes. They are also used in very important applications for Industrial Control System (ICS) automation, energy management, and by the military for location and positioning [10]. These sensors are becoming increasingly exploited and the systems they are designed to protect remain vulnerable to malicous attacks such as spoofing, denial of service, and key sniffing. These attacks aim to gain unauthorized access by spoofing the bit level credentials required to enter a secure network.

The security of ZigBee systems must be increased to prevent unauthorized persons from entering networks and gaining access to critical information or control of critical systems or infrastructure. One method for doing this is by exploiting known behavior and RF fingerprint signature for known network devices. From this collection, an *Authorized* and *Unauthorized* list can be created that upon request to enter a network, a device must submit its bit-level credentials and be verified prior to being granted access. One method considered here is RF-DNA fingerprinting, which provides an added level of security by examining the actual physical waveform features emitted by a device. This provides a way

to single out a device and prevent something as simple as changing bit level credentials, or spoofing a Media Access Control (MAC) address and entering a network.

## 5.2 Findings and Contributions

This research expanded the capabilities of AFIT's RF-DNA fingerprinting process. Specifically, earlier work in [9] was expanded with and knowledge of ZigBee device behavior increased by introducting and investigating RF-DNA fingerprinting performance using two new receivers and a new set of devices. Accurate comparisons between two different classification methods, Multiple Discriminant Analysis, Maximum Likelihood (MDA/ML) and Generalized Relevance Learning Vector Quantization-Improved (GRLVQI), were made for both full-dimensional and Dimensional Reduction Analysis (DRA) (quantitative and qualitative) feature-sets. Finally, a *Hybrid Cross-Receiver* model for *Device Classification* was introduced and a first-ever comparison made using a model developed with RF-DNA fingerprints from both a high-value PCI Extension for Instrumentation Express (PXIe) receiver and low-value Universal Software Radio Peripheral (USRP) receiver; both receivers are commercial products manufactured by National Instruments (NI).

### *5.2.1 Single Receiver Assessment.*

Full-dimensional *Device Classification* was performed with both receivers using MDA/ML and GRLVQI methods. Regardless of the receiver, MDA/ML consistently dominated GRLVQI, with the latter requiring an average $SNR \approx 2.0$ dB increase in gain to match performance. When averaging across classification methods however, the high-end PXIe receiver outperformed the low-end USRP receiver, requiring $SNR \approx 5.1$ dB less to reach the arbitrary $\%C$=90% benchmark.

Quantitative DRA *Device Classification*, again only performed using GRLVQI, exhibited a notable difference in performance between PXIe and USRP. While PXIe achieved $\%C$=90% at $SNR \approx 12.0$ dB consistently, for $N_F \in$[10 297], USRP performance suffered

and failed to meet the benchmark for $N_F \leq 10$. Qualitative DRA using $N_F = 99$ features proved that regardless of the receiver used, the *Phz*-only feature set far outperformed the *Frq*-only and *Amp*-only feature sets. In fact, when compared to quantitative DRA performance using the top-ranked $N_F = 99$ features (combination of *Amp*, *Phz*, and *Frq* features) for both receivers,

$$\%C_{FD} \approx \%C_{99Qnt} \approx \%C_{99Phz} > \%C_{99Frq} >> \%C_{99Amp},$$

where $\%C_{FD}$ is the average correct classification using the full-dimensional (FD) feature set. Finally, on a comparison of receiver-only performance, regardless of classification method or feature-set, high-value PXIe outpaced performance of low-value USRP by $SNR \approx 6.0$ dB.

### *5.2.2 Hybrid Receiver Assessment.*

For "hybrid" receiver assessment, the MDA/ML and GRLVQI models were developed using fingerprints from both receivers for both full-dimensional and Quantitative DRA *Device Classification*. Three specific cases were examined where the *Testing* fingerprint set included: 1) a hybrid combination of both PXIe and USRP fingerprints, 2) PXIe-only fingerprints, and 3) USRP-only fingerprints.

**Case 1: "*Hybrid Cross-Receiver*" (PXIe and USRP)**

When *Testing* fingerprints were comprised of both receivers (*Hybrid Cross-Receiver*), $\%C$ performance was mixed. While both classification methods met the $\%C$=90% benchmark for full-dimensional features, MDA/ML $\%C$ performance immediately dropped off for $N_F < 99$. Although MDA/ML was the clear winner for full-dimensional classification, edging out GRLVQI by $SNR \approx 2.3$ dB less required gain, subsequent reduction of $N_F$ favored GRLVQI by $SNR \approx 3.5$ dB less required gain than that of MDA/ML to meet $\%C$=90%. In fact, when $N_F \leq 66$, MDA/ML failed to achieve the $\%C$=90% benchmark over the specified $SNR \in$[0 24] dB range.

**Case 2: PXIe Only Testing**

Utilizing only PXIe fingerprints for *Testing* greatly increased $\%C$ performance for both full-dimensional and DRA feature sets using MDA/ML and GRLVQI. While MDA/ML performed better for full-dimensional classification, when averaged across calcuable values ($N_F = 10, 33, 66, 99$), GRLVQI required $SNR \approx 3.27$ dB less gain to match MDA/ML $\%C$=90% benchmark performance. The *Hybrid Cross-Receiver* model is well-suited for use soley with the PXIe receiver.

**Case 3: USRP Only Testing**

Utilizing only USRP fingerprints for *Testing* with full-dimensional and DRA feature sets, regardless of classification method, failed to meet the $\%C$=90% benchmark over the $SNR\in$[0 24] dB range. The *Hybrid Cross-Receiver* model is deemed unsuitable for use soley with the USRP receiver.

Overall when comparing classification methods, as in the single-receiver assessment, MDA/ML outperformed GRLVQI for a full-dimensional feature-set. Averaged among Case 1 and Case 2 (Case 3 full-dimensional analysis failed to achieve $\%C$=90% benchmark over the $SNR\in$[0 24] dB range), GRLVQI required an additional $SNR \approx 1.6$ dB to match MDA/ML $\%C$ performance. Quantitative DRA performance favored GRLVQI though, providing relatively consistent $\%C$ over $SNR\in$[0 24] dB for $N_F > 10$. Again, when averaged across calcuable values for Case 1 and Case 2, MDA/ML required $SNR \approx 3.32$ dB additional gain to match GRLVQI $\%C$=90% benchmark performance.

## 5.3 Recommendations for Future Research

This research has shown that a high-value receiver (PXIe) generally provides better classification performance than a lower-valued receiver (USRP). Further, it was shown that by combining RF-DNA fingerprints from high and low value receivers, a *Hybrid Cross-Receiver* model can be developed and when utilized properly, provide classification per-

formance results consistent with models developed solely from fingerprints for a single receiver. This work is not complete and further benefit could be realized by investigating:

1. Alternative Classifiers - There are numerous other classifiers already in existence. *Device Classification* should be investigated further by developing models and performing classification with these alternative classifiers. Results varied in this research, based mostly off of the classification method used and the $N_F$ chosen to perform classification with. Choosing a different classifier other than MDA/ML or GRLVQI may provide a single method that is the clear winner, outperforming all other classifiers regardless of whether Full-Dimensional or DRA is used.

2. Different RF-DNA Features - There are endless possiblities of how to define the features that are used to describe each RF-DNA fingerprint. Further work should be performed to change the feature sets that are used for classification. Specifically alternatives can include changing the size and number of subregions, developing models that perform quantitative DRA within a specified time domain instantaneous signal response ($\phi$-only for example), and performing fingerprint generation using different statistical metrics or combinations thereof. All these alternatives may provide a different set of features that can more consistently meet or exceed $\%C$=90% at a lower dB value.

3. Alternative (non-ZigBee) Signals - The ZigBee protocol is a very small portion of the mass of existing RF signals capable of performing device classification on. The comparison of high versus low value receivers as well as creation of a *Hybrid Cross-Receiver* may be found to be more suitable if performing *Device Classification* on any of these other non-ZigBee signals.

4. Different devices within the ZigBee protocol - The Atmel AT86RF230 is but one ZigBee device capable of being researched in terms of its signal responses. As the ZigBee protocol is relatively inexpensive and widely used in a myriad of applications, new devices will come to the forefront, and spoofing will remain a concern. Investigating alternative devices with the same receivers will help to further create a known pool of the behavior of all devices running the ZigBee protocol. This information could be used to heighten security within critical networks that rely on ZigBee every day.

## Bibliography


[1] "OSI Reference Model", May 2009. URL http://www.ccnaguru.com/osi-reference-model.html.

[2] Buckner M.A. *Learning From Data with Localized Regression and Differential Evolution*. Ph.D. thesis, University of Tennessee, Knoxville, May 2003.

[3] Buckner M.A., 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.

[4] Buckner M.A., M. Bobrek, E.E. Farquahar, Harmer P.K. and M.A. Temple. "Enhancing Network Security Using 'Learning-From-Signals' and Fractioinal Fourier Transform Based RF-DNA Fingerprints". *SDR'11- Wireless Innovation Conference*. Dec 2011.

[5] Chen, S.K., T. Kao, C.T. Chan, C.N. Huang, C.Y. Chiang, C.Y. Lai, T.H. Tung, and P.C. Wang. "A Reliable Transmission Protocol for ZigBee-Based Wireless Patient Monitoring". *IEEE Trans on Information technology in Biomedicine*, 16(1):6–16, Jan 2012.

[6] Danev B. and S. Kapkun. "Transient-Based Identification of Wireless Sensor Nodes". *Proc of the 8th ACM/IEEE Int'l Conf on Information Processing in Sensor Networks (IPSN09)*. Apr 2009.

[7] Danev B., H. Luecken, S. Capkun, and K. El Defrawy. "Attacks on Physical-layer Identification". *Proc of the 3rd ACM Int'l Conf on Wireless Network Security (WiSec10)*. Mar 2010.

[8] Danev B., Heydt-Benjamin, S. Thomas and S. Capkun. "Physical-layer Identification of RFID Devices". *Proc of the 18th conference on USENIX security symposium*, SSYM'09, 199–214. 2009.

[9] Dubendorfer C.K. *Using RF-DNA Fingerprints To Discriminate ZigBee Devices in an Operational Environment*. Master's thesis, Air Force Institute of Technology, March 2013.

[10] Dubendorfer C.K., B.W. Ramsey and M.A. Temple. "An RF-DNA Verification Process for ZigBee Networks". *Proc of Military Communications Conference (MILCOM12)*. Oct 2012.

[11] Dubendorfer C.K., B.W. Ramsey and M.A. Temple. "ZigBee PHY-Based Device ID Verification: Security Enhancement for Industrial Control and Building Automation Systems". *Proc of IFIP Working Group 11.10 Int'l Conf on Critical Infrastructure Protection (IFIP13)*. Mar 2013.

[12] Duda R., P. Hart and D. Stork. *Pattern Classification*. John Wiley & Sons, Inc., New York, second edition, 2001.

[13] Egan D. "The Emergence of ZigBee in Building Automation and Industrial Control". *Computing & Control Engineering Journal*, 16(2):14–19, April-May 2005.

[14] Hall J., et. al. "Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase". IASTED Int'l Conf on Wireless and Optical Communications, May 2003.

[15] Hall J., et. al. "Using Transceiverprints for Anomaly Based Intrusion Detection". 3rd IASTED Int'l Conf on Communications, Internet and Information Technology (CIIT), November 2004.

[16] Hall J., M. Barbeau and E. Kranakis. "Radio Frequency Fingerprinting for Intrusion Detection in Wireless Networks", Jul 2005. DRAFT.

[17] Hall J., M. Barbeau and E. Kranakis. "Detecting Rogue Devices In Bluetooth Networks Using Radio Frequency Fingerprinting". *Communications and Computer Networks*, 108–113. 2006.

[18] Hammer B. and T. Villmann. "Generalized Relevance Learning Vector Quantization". *Neural Networks*, 15:1059–1068, 2002.

[19] Harmer P.K. *Development of Learning from Signals Classifier for Cognitive Software Defined Radio Applications*. Ph.D. thesis, Air Force Institute of Technology, March 2013.

[20] Harmer P.K., D.R. Reising and M.A. Temple. "Classifier Selection for Physical Layer Security Augmentation in Cognitive Radio Networks". Proc of IEEE Int'l Conf on Communications (ICC13), Jun 2013.

[21] Harmer P.K., M.A. Temple, M.A. Buckner and E.E. Farquahar. "4G Security Using Physical Layer RF-DNA with DE-Optimized LFS Classificatioin". *Jour of Communications, Special Issue: Advances in Communications and Networking*, 9(6):671–681, Dec 2011.

[22] Harmer P.K., M.A. Temple, M.A. Buckner and E.E. Farquahar. "Using Differential Evolution to Optimize 'Learning from Signals' and Enhance Network Security". *Submitted to: Genetic and Evolutionary Computation Conference (GECCO)*. July Jul 2011.

[23] Harmer P.K., M.D. Williams and M.A. Temple. "Using DE-Optimized LFS Processing to Enhance 4G Communication Security". *20th International Conference on Computer Communication and Networks (ICCCN)*. Aug 2011.

[24] Institute of Electrical and Electronics Engineers. *IEEE 802.15.4, Standard, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate WPANS*, 2006.

[25] Klein R.W. *Application of Dual-Tree Complex Wavelet Transforms to Burst Detection and RF Fingerprint Classification*. Ph.D. thesis, Air Force Institute of Technology, September 2009.

[26] Klein R.W., M.A. Temple and M.J. Mendenhall. "Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security". *Jour of Communications and Networks*, Vol. 11, No. 6, Dec 2009.

[27] Klein R.W., M.A. Temple, M.J. Mendenhall and D.R. Reising. "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance". *Proc of IEEE Int'l Conf on Communications (ICC09)*. Jun 2009.

[28] National Instruments. *National Instruments Record and Playback Demo With NI USRP*, 2012.

[29] Ramsey B.W., M.A. Temple and B.E. Mullins. "PHY Foundation for Multi-Factor ZigBee Node Authentication". *Proc of IEEE Global Communications Conf (GLOBECOM12)*. Dec 2012.

[30] Ramsey B.W., T.D. Stubbs, B.E. Mullins, M.A. Temple, M.A. Buckner. "Wireless Critical Infrastructure Protection Using Low-Cost RF Fingerprinting Receivers". *Journal of Computers and Electrical Engineering*. Submitted Feb 2013, Under Review.

[31] Reising, D.R. *Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing*. Ph.D. thesis, Air Force Institute of Technology, December 2012.

[32] Reising, D.R., and M.A. Temple. "Verification of Localized OFDM-Based Devices Using Dimensionally Efficient GRLVQI Processing". *Systems Journal, IEEE*, 2012.

[33] Reising D.R. and M.A. Temple. "WiMAX Mobile Subscriber Verification Using Gabor-Based RF-DNA Fingerprints". *2012 IEEE International Communications Conference (ICC12)*. Jun 2012.

[34] Reising D.R., M.A. Temple, and J.A. Jackson. "Detecting Rogue Devices at Cloud Wireless Access Points Using RF Air Monitors". *Information Forensics and Security, IEEE Transactions on*, 2012.

[35] Reising D.R., M.A. Temple and M.E. Oxley. "Gabor-Based RF-DNA Fingerprinting for Classifying 802.16e WiMAX Mobile Subscribers". 2012 IEEE Int'l Conf on Computing, Networking & Communications (ICNC), Jan 2012.

[36] 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*, Vol. 3, No. 1, pp. 41-59,2010.

[37] Reising D.R., M.A. Temple and M.J. Mendenhall. "Improving Intra-Cellular Security Using Air Monitoring with RF Fingerprints". *Proc of 2010 IEEE Wireless Communications & Networking Conf (WCNC10)*. Apr 2010.

[38] Speers R., J. Wright and R. Melgares. "Api-do: Tools for ZigBee and 802.15.4 Security Auditing". URL http://code.google.com/p/zigbeesecurity/.

[39] Suski W.M. II, M.A. Temple, M.J. Mendenhall and R.F. Mills. "RF Fingerprinting Commercial Communication Devices to Enhance Electronic Security". *Int. J. Electronic Security and Digital Forensics*, Vol. 1, No. 3, pp. 301-322, 2008.

[40] Suski W.M. II, M.A. Temple, M.J. Mendenhall and R.F. Mills. "Using Spectral Fingerprints to Improve Wireless Network Security". *Proc of IEEE Global Communications Conf (GLOBECOM08)*. Mar 2008.

[41] Temple M.A. "RF-DNA Fingerprinting: Distinct Native Attributes", Lecture Notes, EENG 699, Jan 2013.

[42] Theodoridis S. and K. Koutoumbas. *Pattern Recognition*. Academic Press, fourth edition, 2009.

[43] Tihon I. and V. Croitoru. "ZigBee Sensor Networks Telesurveillance". 1–4. 10th International Symposium on Signals, Circuits and Systems (ISSCS'11), Jun 2011.

[44] Whittaker T. "Final Word". 18(3):48, Jun-July 2007.

[45] Williams M.D., M.A. Temple and D.R. Reising. "Augmenting Bit-Level network Security Using Physical Layer RF DNA Fingerprinting". *Proc of IEEE Global Communications Conf (GLOBECOM10)*. Dec 2010.

[46] Williams M.D., S.A. Munns, M.A. Temple and M.J. Mendenhall. "RF-DNA Fingerprinting for Airport WiMax Communications Security". *Proc of 4th Int'l Conf on Net and Sys Security (NSS10)*. Sep 2010.

[47] Wright J. "KillerBee: Framework and Tools for Exploiting ZigBee and IEEE 802.15.4 Networks", Version 1.0, 2010. URL http://code.google.com/p/killerbee/.

[48] ZigBee Alliance. *ZigBee Specification*, 2008.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704–0188*



| 1. REPORT DATE *(DD–MM–YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From — To)* |
|---|---|---|
| 27–03–2014 | Master's Thesis | Oct 2013–Mar 2014 |

**4. TITLE AND SUBTITLE**

A Comparison of RF-DNA Fingerprinting Using High/Low Value Receivers with ZigBee Devices

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

Stubbs, Tyler D., Captain, USAF

**5d. PROJECT NUMBER**

**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-ENG-14-M-74

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

Intentionally Left Blank

**10. SPONSOR/MONITOR'S ACRONYM(S)**

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

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

**13. SUPPLEMENTARY NOTES**



**14. ABSTRACT**

The ZigBee specification provides a niche capability, extending the IEEE 802.15.4 standard to provide a wireless mesh network solution. ZigBee-based devices require minimal power and provide a relatively long-distance, inexpensive, and secure means of networking. The technology is heavily utilized, providing energy management, ICS automation, and remote monitoring of Critical Infrastructure (CI) operations; it also supports application in military and civilian health care sectors. ZigBee networks lack security below the "Network" layer of the OSI model, leaving them vulnerable to open-source hacking tools that allow malicous attacks such as MAC spoofing or Denial of Service (DOS). A method known as RF-DNA Fingerprinting provides an additional level of security at the Physical (PHY) level, where the transmitted waveform of a device is examined, rather than its bit-level credentials which can be easily manipulated. RF-DNA fingerprinting allows a unique human-like signature for a device to be obtained and a subsequent decision made whether to grant access or deny entry to a secure network. Two NI receivers were used here to simultaneously collect RF emissions from six Atmel AT86RF230 transceivers. The time-domain response of each device was used to extract features and generate unique RF-DNA fingerprints. These fingeprints were used to perform Device Classification using two discrimination processes known as MDA/ML and GRLVQI. Each process (classifier) was used to examine both the Full-Dimensional (FD) and reduced dimensional feature-sets for the high-value PXIe and low-value USRP receivers. The reduced feature-sets were determined using DRA for both quantitative and qualitative subsets. Additionally, each classifier performed Device Classification using a "hybrid" interleaved set of fingerprints from both receivers.

**15. SUBJECT TERMS**

RF-DNA Fingerprinting, ZigBee, Classification, Hybrid Receiver

| 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 (ENG) |
| U | U | U | UU | 79 | 19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636 x4279 Michael.Temple@afit.edu |