COMPARATIVE ANALYSIS OF RF EMISSION BASED FINGERPRINTING TECHNIQUES FOR ZIGBEE DEVICE CLASSIFICATION

THESIS

Cameron W. Coon, Captain, USAF

AFIT-ENG-MS-17-M-017

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-17-M-017

COMPARATIVE ANALYSIS OF RF EMISSION BASED FINGERPRINTING TECHNIQUES FOR ZIGBEE DEVICE CLASSIFICATION

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

Cameron W. Coon, BSEE

Captain, USAF

March 2017

DISTRIBUTION STATEMENT A:

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT-ENG-MS-17-M-017

COMPARATIVE ANALYSIS OF RF EMISSION BASED FINGERPRINTING TECHNIQUES FOR ZIGBEE DEVICE CLASSIFICATION

THESIS

Cameron W. Coon, BSEE
Captain, USAF

Committee Membership:

Kenneth Hopkinson, Ph.D.
Chairman

Maj A. Betances, Ph.D.
Member

Robert Mills, Ph.D.
Member

AFIT-ENG-MS-17-M-017

Abstract

Low-Rate Wireless Personal Area Networks (LR-WPAN) are increasingly being fielded to complete tasks in autonomous sensor networks, industrial control systems, and other critical infrastructure. ZigBee is a versatile LR-WPAN platform that also open to risks of sophisticated bit-level attacks. Physical-Layer (PHY) based security measures have been shown in previous research efforts as effective supplemental security measures that a not susceptible to bit-level attacks. This research effort intends to quantify the differences in various RF fingerprinting techniques via comparative analysis of Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification results. The findings herein demonstrate a methodology for the generation of Constellation Based-Distinct Native Attributes (CB-DNA), Radio Frequency-Distinct Native Attributes (RF-DNA), and Correlation Based-Distinct Native Attributes (COR-DNA) fingerprints. The results show that CB-DNA generated fingerprints had the highest mean correct classification rates followed by COR-DNA and then RF-DNA in most test cases and especially in low E_b/N_0 ranges, where ZigBee is designed to operate.

Acknowledgements

I want to thank my God, whose hand of providence has constantly blessed my life and has surrounded me with people that want me to succeed. Of course, I must thank my wife. Your love, support, and abundance of left-overs have seen me through life at AFIT.

I also want to thank my advisor for giving me the freedom to pursue this research, and Major Betances for always helping me understand his previous research. It was foundational for this work.

Cameron W. Coon

Table of Contents

Page

List of Figures

List of Tables

List of Acronyms

E_b/N_0 energy per bit to noise power spectral density ratio.

E_s/N_0 energy per symbol to noise power spectral density ratio.

$\%C$ Average % Correct Classification.

AWGN Additive White Gaussian Noise.

BPSK Binary Phase Shift Keying.

CB-DNA Constellation Based-Distinct Native Attributes.

CM Confusion Matrix.

COR-DNA Correlation Based-Distinct Native Attributes.

CS constellation symbol(s).

DFT Discrete Fourier Transform.

DRA Dimensional Reduction Analysis.

DS data symbol(s).

DSSS Direct Sequence Spread Spectrum.

FSK Frequency Shift Keying.

GRLVQI Generalized Relevance Learning Vector Quantized Improved.

GUI Graphical User Interface.

IEEE Institute of Electrical and Electronics Engineers.

LPI Lowpass Interpolation.

LR-WPAN Low-Rate Wireless Personal Area Networks.

MDA/ML Multiple Discriminant Analysis/Maximum Likelihood.

MSK Minimum Shift Keying.

O-QPSK Offset-Quadrature Phase Shift Keying.

PHY Physical-Layer.

PN pseudo-random noise.

QPSK Quadrature Phase Shift Keying.

RF-DNA Radio Frequency-Distinct Native Attributes.

ROI Region(s) of Interest.

RSSI Received Signal Strength Indicator.

SD Spectral Domain.

SDR Software-Defined Radio.

SER Symbol Error Rate.

SFD State-of-Frame Delimiter.

SHR Synchronization Header.

SNA Sensor Network Analyzer.

SNR Signal to Noise Ratio.

SOI Signal of Interest.

SPS Samples per Constellation Symbol.

TD Time Domain.

WPANs Wireless Personal Area Networks.

WSN Wireless Sensor Network(s).

COMPARATIVE ANALYSIS OF RF EMISSION BASED FINGERPRINTING TECHNIQUES FOR ZIGBEE DEVICE CLASSIFICATION

I. Introduction

The applications of wireless communication networks continue to grow as does the demand for more autonomous sensor networks. Inexpensive Low-Rate Wireless Personal Area Networks (LR-WPAN) are increasingly being used to meet demand. ZigBee, a LR-WPAN framework, is often chosen for its low-cost, low-power, and versatility in assuming many different topologies[4]. As ZigBee is becoming more common in critical infrastructure, from civilian and military hospitals to industrial control systems [5], its degradation from intentional attacks is increasingly devastating. Many systems employ security efforts based on presenting and verifying device bit-level credentials, however, these securities are at risk with open source tools that are designed to capture and replay ZigBee signals that mimic authorized network devices. Previous research efforts have studied the effectiveness of Physical-Layer (PHY) based security in order to supplement security measures already in place in ZigBee devices. These research efforts have shown positive results but most research has only focused on one technique. The research contained in this document examined many different PHY security techniques on a single platform and provides a comparative analysis of results.

1.1 Research Background

1.1.1 ZigBee Devices.

ZigBee is a low-power communication technology used in low-data rate applications that require long battery life and secure networking[6]. ZigBee networks are currently deployed and tasked for functions in Wireless Sensor Network(s) (WSN) such as monitoring medical devices, electrical usage information in smart grid systems, and home automation[7, 8, 9]. ZigBee networks are vulnerable to attacks from rogue devices that extract and present network key information. Bit-layer keys are susceptible to attacks through mimicry, but PHY security measures are independent of network bit-level attacks. For this reason, PHY security techniques are the focus of this research.

1.1.2 Physical Layer Security.

PHY security is based on the knowledge that every RF device's PHY is unique. The PHY difference in one device to the next can be attributed to differences in manufacturing tolerances and techniques, materials used, component configuration, etc. External factors, such as operating temperature, can affect a device PHY. The differences are manifested in intentional and unintentional RF emissions. Quantifying differences in RF emissions is akin to creating a human biological profile with markers like fingerprints and DNA. Device fingerprints are profiles of statistical measurements from unique distributions of data derived from their RF emissions. The profiles can be used for device classification and verification.

1.1.3 Fingerprinting Techniques.

Constellation Based-Distinct Native Attributes (CB-DNA) is a PHY security method where fingerprints are developed in the symbol constellation space. The

symbol constellation space is defined by the modulation method that the device uses. Previous research shows that CB-DNA provided an average rogue reject rates (RRR) of $85.2\% < RRR < 93.1\%$ at $SNR > 26.0\,dB$ in Ethernet cards using unintentional Ethernet cable emissions[1].

Radio Frequency-Distinct Native Attributes (RF-DNA) is another fingerprinting technique where a unique profile is generated from Spectral Domain (SD) or Time Domain (TD) RF features such as amplitude, frequency, and/or phase. RF-DNA has been researched in microwave devices[10], 802.16e WiMAX mobile subscribers classification[11], and ZigBee networks[12, 13].

The third PHY security technique examined for this research is Correlation Based-Distinct Native Attributes (COR-DNA). COR-DNA is closely related to CB-DNA wherein they both require demodulation and both use correlation operations in the demodulation. The difference is that, when using ZigBee demodulation, COR-DNA uses a 16-ary correlation receiver as opposed to a dual correlation receiver for CB-DNA. The implementation of COR-DNA for ZigBee devices is a new method developed during this research.

1.2 Research Goal

The intent of this thesis is to provide a comparative analysis of different fingerprinting techniques on ZigBee devices. The majority of previously published research is limited in scope to one type of fingerprinting technique. The research of this thesis is necessary because it expands the scope to include multiple fingerprinting techniques so that a comparison of fingerprinting methods can be made. It provides information necessary in determining best methods to use to achieve desired results.

1.3 Research Approach

A comprehensive literature review was done to develop the foundational knowledge needed to execute fingerprinting methods and tests. The review included articles published in Institute of Electrical and Electronics Engineers (IEEE) journals, commonly used academic text books, and previous AFIT students' theses and dissertations.

The research was conducted in a manner to create an equal testing bed for all experiments while only varying the devices and fingerprinting methods. This goal was to eliminate all outside influences that could be attributed to affecting results.

The quantity and devices used in this research were 10 Atmel AVR RZ USBstick, a ZigBee device and network development tool, and 8 HackRF One, a Software-Defined Radio (SDR) programmed to mimic ZigBee devices. The devices all transmitted the same predetermined data packets and all were received with the Ettus USRP X310-USB160 SDR. All post capture digital signal processes were completed with MATLAB. The devices were all individually fingerprinted and tested in varying combinations to represent different real world scenarios.

The three fingerprinting techniques that were tested were CB-DNA, RF-DNA, and COR-DNA. CB-DNA and COR-DNA fingerprinting required two different demodulation implementations. The two implemented receivers were verified with Symbol Error Rate (SER).

1.4 Thesis Organization

The thesis is presented in four main chapters with each chapter divided further into sections and subsections. Chapter II presents some of the relevant background obtained from the literature review. Chapter III describes the methodology and design of experiments along with the necessary verification. Chapter IV displays

the results and analysis of the experiments. Chapter V provides a summary and conclusions based on the results as well as a recommendation for future research.

II. Background

2.1 Overview

This chapter provides background on methods used in this research, as described in Chapter III. It also explains other relevant techniques used in related research. Section 2.2 provides details on ZigBee networks and signal protocol as defined by Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard for Wireless Personal Area Networks (WPANs)[3]. Section 2.3 describes a Python based framework and tool set for exploring and exploiting the security of ZigBee and IEEE 802.15.4 networks called KillerBee. Section 2.4 briefly covers the HackRF One Software-Defined Radio (SDR). Section 2.5 gives the foundation for Offset-Quadrature Phase Shift Keying (O-QPSK) modulation and how, specifically, ZigBee utilizes it. Section 2.6 gives a general background on Physical-Layer (PHY) based fingerprinting. Subsections 2.6.1, 2.6.2, and 2.6.3 explain different techniques of fingerprinting, more specifically. Lastly, Section 2.7 gives details about the Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classifier that was utilized, which allows comparative analysis of the fingerprinting techniques.

2.2 ZigBee Protocol

ZigBee is a low-power communication technology used in low-data rate applications that requires a long battery life and secure networking[6]. ZigBee has many applications in the private and public sector, as well as military applications. ZigBee is used in, but not limited to, home automation, smart grid technology, military hospitals to help track movement of patients, and for temperature monitoring in automated control systems[7, 8, 9, 14].

ZigBee follows IEEE 802.15.4 standard for Low-Rate Wireless Personal Area Networks[3]. According to IEEE 802.15.4, ZigBee has different protocols it must abide by: dependent on is operating frequency range (W_{rng}), specifically either W_{rng} = 779-787 MHz, W_{rng} = 868.0-868.6 MHz, W_{rng} = 902-928 MHz, or W_{rng} = 2400.0-2483.5 MHz. This research only focuses on ZigBee devices operating in W_{rng} = 2400.0-2483.5 MHz[15].

In the frequency range W_{rng} = 2400.0-2483.5 MHz, ZigBee uses a 16-ary O-QPSK modulation, as expounded upon in section 2.5. W_{rng} is divided into 16 channels. Each channel has a bandwidth of W_{RF} = 2.0 MHz, and a channel spacing of Δ_{Ch} = 5.0 MHz[12]. Furthermore, ZigBee has a low-data bit rate of R_b = 250 kb/s.

ZigBee utilizes Direct Sequence Spread Spectrum (DSSS) to encode the bits. First, four bits are mapped to one of sixteen data symbol(s) (DS), where the DS are numbered $DS = [0 - 15]$. Due to the DSSS, the DS rate (R_{DS}) is $R_{DS} = R_b/4 = 62.5kDS/s$. Each DS mapped to a 32-chip pseudo-random noise (PN) nearly orthogonal sequence, Table 1, which results in a chip rate (R_c) of R_c = 4000 kc/s. The 32-chip PN sequences are modulated into communication symbols with O-QPSK, figure 1.

IEEE 802.15.4 defines the protocol of a ZigBee transmission including that all transmissions must start with a Synchronization Header (SHR), which includes a preamble and a State-of-Frame Delimiter (SFD)[3]. The preamble was defined as eight consecutive DS=0 and the SFD was DS = [7,10]. Thus, each ZigBee burst began with DS = [0 0 0 0 0 0 0 0 7 10]. This known sequence of DS was exploited for

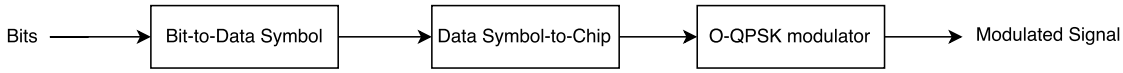


Figure 1. Spreading and Modulation Functions for ZigBee Devices

Table 1. ZigBee data symbol-to-chip mapping for 2450 MHz band.[3]

Data symbol	Chip values (c_0 c_1 ... c_{30} c_{31})
0	1 1 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

Radio Frequency-Distinct Native Attributes (RF-DNA), Section 2.6.3, and for burst detection and alignment, section 3.2.5.

2.3 KillerBee: ZigBee Attack Platform

KillerBee is a framework that was developed to exploit ZigBee networks. It has been used to aid others in many previous ZigBee network security and attack research efforts[16, 17, 18].

The framework includes the following tools [17, 19]:

- *zbassocflood*- Transmit a flood of associate requests to a target network.
- *zbconvert*- Convert Daintree Sensor Network Analyzer (SNA) files to libcap format and vice-versa.
- *zbdump*- Tcpdump-like tool to capture IEEE 802.15.4 frames to a libpcap or a Daintree SNA packet capture file.
- *zbfind*- A Graphical User Interface (GUI) for tracking the location of a ZigBee transmitter by measuring Received Signal Strength Indicator (RSSI).
- *zbgoodfind*- Search a binary file to identify the encryption key for a given SNA
- *zbid*- Identifies available interfaces that can be used by KillerBee and associated tools
- *zbreplay*- Replay ZigBee/802.15.4 network traffic from libpcap or Daintree files.
- *zbdsniff*- Decode plaintext key ZigBee delivery from a capture file. When a key is found, it prints the key to stdout.
- *zbstumbler*- Transmit beacon request frames to the broadcast address.
- *zbwireshark* - Similar to *zbdump* but exposes a named pipe for real-time capture and viewing in Wireshark.

Previous research efforts have had to use the KillerBee platform of tools to obtain control over the transmitted information, to include control of content and timing of transmissions[13]. Killerbee firmware and tools were utilized in this research because it gave necessary control over transmitted data to develop quality fingerprints.

2.4 HackRF One™

HackRF One™ is a SDR manufactured by Great Scott Gadgets™[20]. It is capable of transmission or reception of radio signals for W_{rng} = 1 MHz - 6 GHz. This SDR was designed to enable test and development of current and future radio technologies. It can be programmed for stand-alone operation.

2.5 O-QPSK Modulation

Quadrature Phase Shift Keying (QPSK) can be described as two orthogonal Binary Phase Shift Keying (BPSK) signals. The In-Phase, or I-Channel, consists of the modulation of the even chips and the Quadrature-Phase, or Q-Channel, consists of the odd chips, as follows[3]:

$$\mathbf{C}_I(t) = c_0, c_2, c_4, ... \text{(even chips)} \tag{1}$$

$$\mathbf{C}_Q(t) = c_1, c_3, c_5, ... \text{(odd chips)},$$

where the values of the chips $c_k(t) = \pm 1$, represent binary one and zero[21].

The I-Channel and Q-Channel are modulated onto carrier waves that are orthogonal cosine and sine functions defined as[21]:

$$s(t) = \frac{1}{\sqrt{2}} c_I(t) cos\left(2\pi f_0 t + \frac{\pi}{4}\right) + \frac{1}{\sqrt{2}} c_Q(t) sin\left(2\pi f_0 t + \frac{\pi}{4}\right). \tag{2}$$

Due to orthogonality of QPSK, the two BPSK signals can be detected separately. Because this relationship, both QPSK and O-QPSK can be demodulated as two separate BPSK signals[21, 22].

QPSK can also be expressed in exponential form as:

$$s(t) = A(t)e^{(j2\pi f_o t)}, \quad \text{where } A(t) = \left[e^{j\frac{\pi}{4}}, e^{j\frac{3\pi}{4}}, e^{j\frac{5\pi}{4}}, e^{j\frac{7\pi}{4}}\right]. \tag{3}$$

$A(t)$ is a function of the four possible combinations of $c_I(t)$ and $c_Q(t)$. $A(t)$ determines the orientation of the symbol constellation as illustrated in Figure 2.

O-QPSK and QPSK have the same symbol constellation because O-QPSK is a form of QPSK. Furthermore, O-QPSK is also represented by Equation (3). The main difference between O-QPSK and QPSK is that QPSK can transition from any symbol to any other symbol. O-QPSK has a channel offset which limits transitions only to adjacent symbols. The offset occurs in the timing of the two BPSK channels where the I-Channel and Q-Channel are offset in time by T_c, where

$$T_c = \frac{1}{R_c}. \tag{4}$$

The effect of the offset is that only one channel can change at a time eliminating the possibility of a phase shift (ϕ_s) of $\phi_s = \pi$[21]. The only shifts possible are $\phi_s = 0, \pm\frac{\pi}{2}$. The offset is shown in Figure 3.

The ZigBee PN chip sequences are shaped with a half sine pulse filter as given by:

$$p(t) = \begin{cases} sin\left(\pi\frac{t}{2T_c}\right), & 0 \le t \le 2T_c \\ 0, & otherwise, \end{cases} \tag{5}$$

to minimize inter-symbol interference and bandwidth utilization [3].

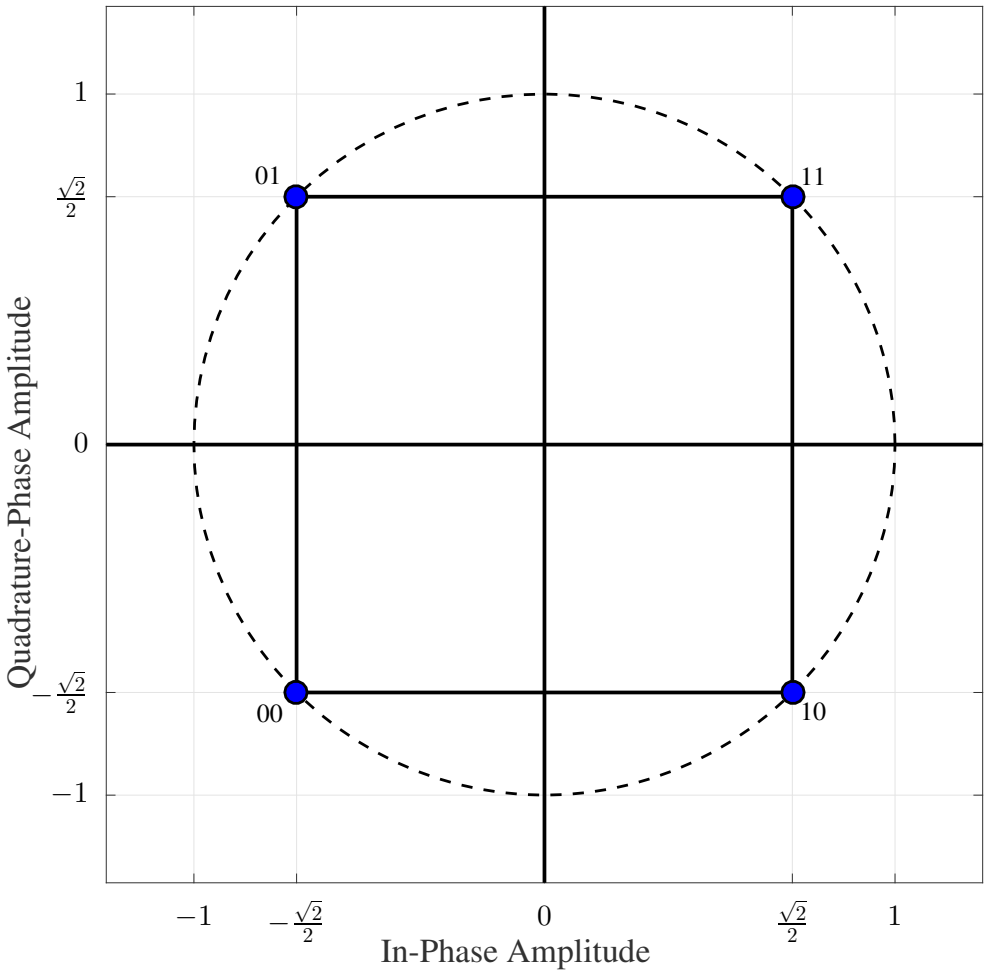


Figure 2. O-QPSK symbol constellation with gray coding. The symbols are located on the unit circle with a phase separation $\phi_s = \frac{\pi}{2}$ and a phase offset $\phi_o = \frac{\pi}{4}$.

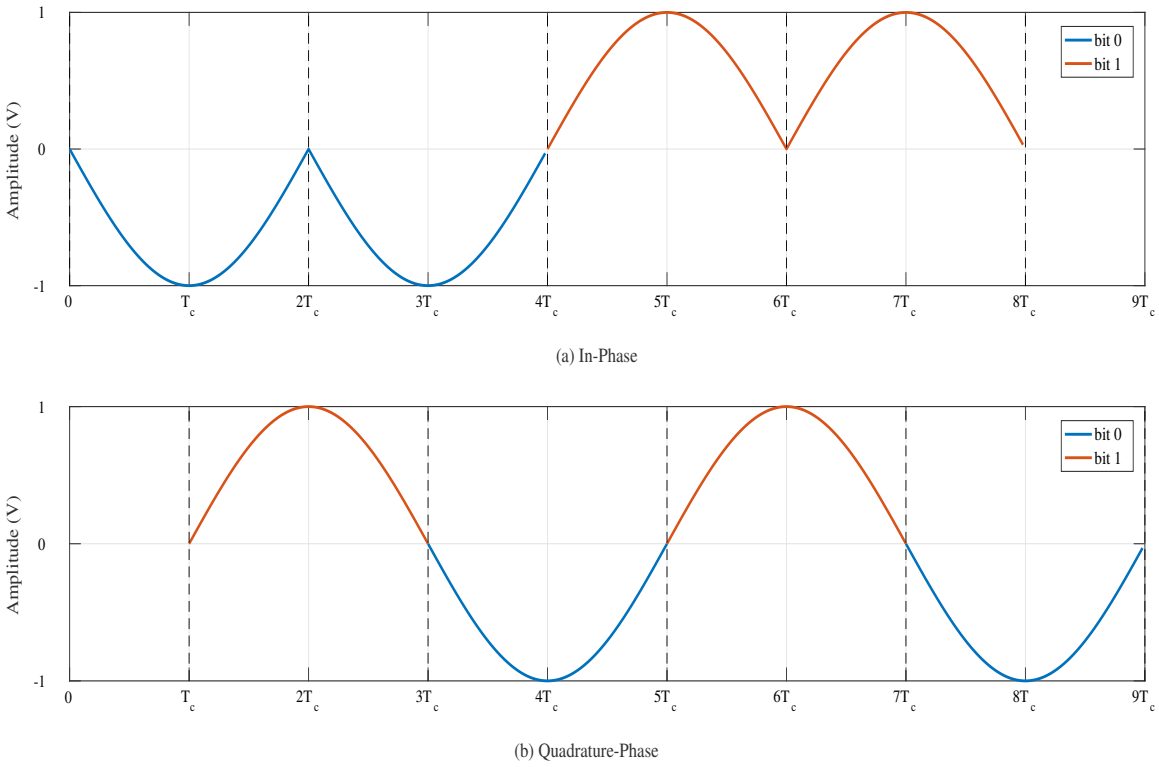


Figure 3. O-QPSK modulated bits in the (a) In-Phase and (b) Quadrature-Phase. The Quadrature-Phase is delayed by the constellation symbol time T_c.

2.6 Fingerprinting

Fingerprinting is a method of creating a mathematical profile of a device based on various statistical measurements of its RF emissions. The fingerprint is unique to the device and is based on the device's PHY. It has been shown in previous research that it is possible to distinguish devices based on their fingerprints[12, 23, 24]. The age of the device, its manufacturing methods and tolerances, and operating temperature can all attribute to a unique fingerprint[25].

The fingerprint is a collection of statistical features such as standard deviation (σ), variance (σ^2), skewness (γ), and kurtosis (κ) whose values are calculated as follows:[26]

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{n=0}^{N-1}(\mathbf{x}[n]-\mu)^2}, \tag{6}$$

$$\sigma^2 = \frac{1}{N-1}\sum_{n=0}^{N-1}(\mathbf{x}[n]-\mu)^2, \tag{7}$$

$$\gamma = \frac{1}{(N-1)\sigma^3}\sum_{n=0}^{N-1}(\mathbf{x}[n]-\mu)^3, \tag{8}$$

$$\kappa = \frac{1}{(N-1)\sigma^4}\sum_{n=0}^{N-1}(\mathbf{x}[n]-\mu)^4, \tag{9}$$

where μ is the mean of $\mathbf{x}[n]$,

$$\mu = \frac{1}{N-1}\sum_{n=0}^{N-1}\mathbf{x}[n]. \tag{10}$$

These statistical moments are calculated for regions R_i in the Signal of Interest (SOI) where $\mathbf{x}[n]$ represents a signal characteristic, such as amplitude or frequency, in a specific R_i. The distinguishable fingerprints are generated by combining the statistical

moments into new vectors for each given R_i as follows:

$$\mathbf{F}_{R_i}^{\alpha} = [\sigma_\alpha, \sigma_\alpha^2, \gamma_\alpha, \kappa_\alpha]_{1\times 4}, \tag{11}$$

where α denotes a specific property of the sampled signal (e.g. amplitude, phase, or frequency). The vectors $\mathbf{F}_{R_i}^{\alpha}$ are concatenated as:

$$\mathbf{F}_{R}^{\alpha} = \left[\mathbf{F}_{R_1}^{\alpha} \quad \vdots \quad \mathbf{F}_{R_2}^{\alpha} \quad \cdots \quad \mathbf{F}_{R_N}^{\alpha}\right]_{1\times N_R \times N_M}, \tag{12}$$

where N_{R_i} is the number of R_i and N_M is the number of statistical metrics. Equation (12) is the devices' fingerprint and the total number of features (N_{feats}) is $N_{feats} = N_{R_i} \times N_M$. The method of fingerprinting will determine the value of α, the SOI, the different R_i, and $\mathbf{x}[n]$, which, in turn, determines the contents of the fingerprint, equation (12). Three different fingerprinting methods were used in this research, namely, Constellation Based-Distinct Native Attributes (CB-DNA), Correlation Based-Distinct Native Attributes (COR-DNA), and RF-DNA.

2.6.1 Constellation-Based Fingerprinting.

CB-DNA fingerprinting performed by generating the devices' statistical profile based on measurements of intentional RF emissions in the symbol constellation space. A received communication symbol is projected as a point, c_{proj}, on the I/Q plane through demodulation. The I/Q plane has decision boundaries and regions that map to a bit assignment dependent on the location of c_{proj}. Each type of modulation has an ideal configuration of its symbol constellation to optimize signal performance[27]. However, c_{proj} is not likely to be projected at the ideal location, but will be offset by some amplitude and/or phase, illustrated in Figure 4. Two reasons for the offset are noise and the device's unique PHY.

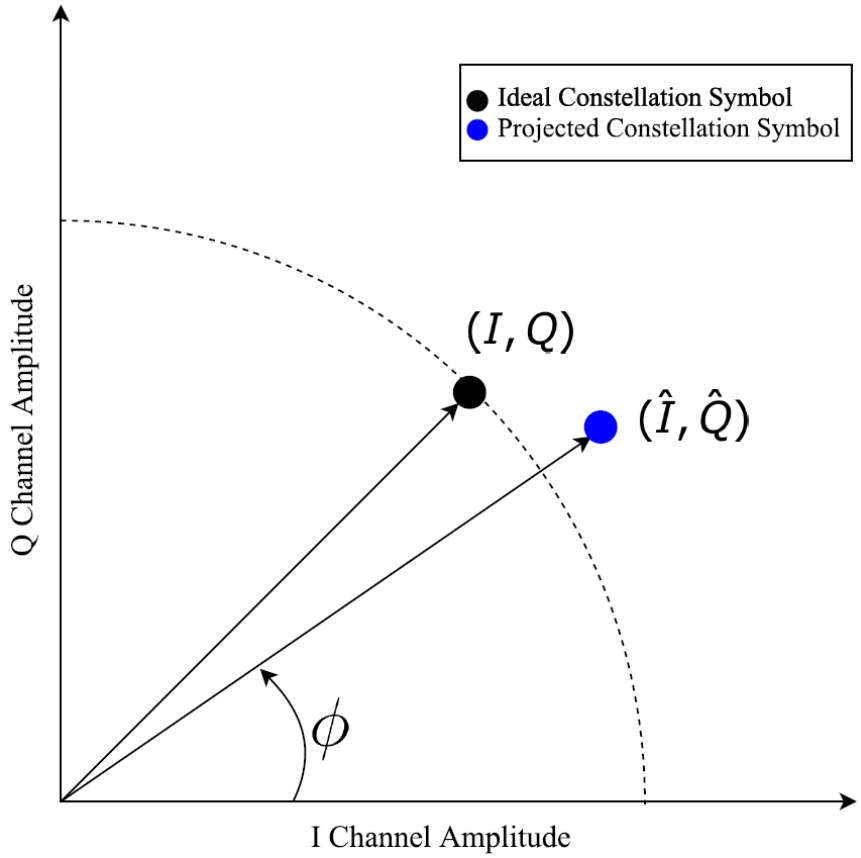


Figure 4. Ideal constellation projection vs notional received constellation projection. The magnitude of $(\hat{I}, \hat{O})$ and subsequent phase (ϕ).

The RF burst provides a complex vector of projections ($\mathbf{c}_{proj}$) where each element ($c_{proj}[n]$) has a real component in the In-Phase and an imaginary component in the Quadrature-Phase as follows:

$$c_{proj}[n] = \hat{I}[n] + j\hat{Q}[n]. \tag{13}$$

The vector $\mathbf{c}_{proj}$ was normalized as follows:

$$c_{proj}[n] = \frac{c_{proj}[n]}{\mu(|\mathbf{c}_{proj}|)}, \tag{14}$$

to account for the difference of energy in each burst.

Previous research in CB-DNA [1, 28], shows that a unique fingerprint can be generated from statistical metrics, Equations(6)-(9), from the magnitude vector $\mathbf{a}[n]$,

$$\mathbf{a}[n] = |c_{proj}[n]| = \sqrt{|\hat{I}[n]|^2 + |\hat{Q}[n]|^2}, \tag{15}$$

and phase vector $\boldsymbol{\phi}[n]$,

$$\boldsymbol{\phi}[n] = tan^{-1}\left(\frac{\hat{I}[n]}{\hat{Q}[n]}\right), \tag{16}$$

for each R_i in the constellation.

In the constellation space, R_i are conditional sub-clusters within the original constellation[1]. The conditions are successive c_{proj}, where $[C_p, C_c, C_n]$ are the previous, current, and next c_{proj}, respectively. Figure 5 shows an example of previous research where different R_i with unique distributions can be seen as they relate to successive c_{proj}[1].

Each conditional transition distribution is a R_i and the statistical measurements of the R_i are features of the devices fingerprint, Equations (11),(12). As a result of using the constellation symbol space, the SOI is the entire burst.

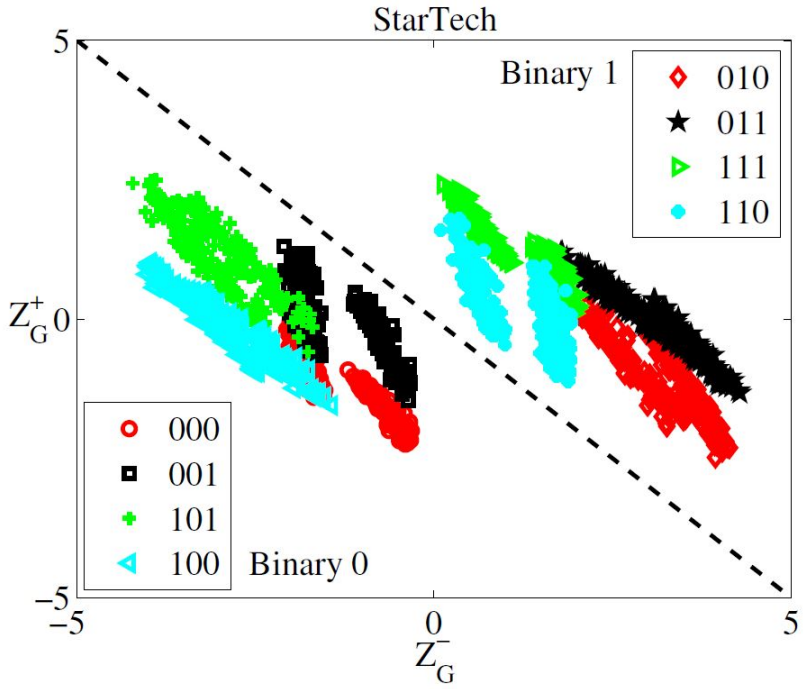


Figure 5. Binary symbol constellation projections showing different conditional transition distributions from unintentional 10BASE-T Ethernet cable emissions.[1]

2.6.2 Correlation-Based Fingerprinting.

COR-DNA is a new fingerprinting method that was tested for this research. ZigBee uses 16 PN near orthogonal chips[3], which allowed demodulation with a 16-ary orthogonal signaling receiver. Previous research shows that orthogonal signal receivers are suited for low-power signals in noisy environments[29]. The design and performance of this receiver is shown in section 3.4.1.

The output of the 16 correlators were put into vector form,

$$\mathbf{z}(T) = [z_0, z_1, \cdots, z_{15}]_{1x16}, \tag{17}$$

which then are ordered into an matrix,

$$\underline{\mathbf{Z}}_{\hat{DS}} = \begin{bmatrix} z_0 & z_1 & \cdots & z_{15} \\ \vdots & \ddots & & \vdots \\ z_0 & z_1 & \cdots & z_{15} \end{bmatrix}_{N_{\hat{DS}} x 16} \tag{18}$$

where the number of rows $N_{\hat{DS}}$ is the number of times that a particular DS was estimated. This will create 16 different $\underline{\mathbf{Z}}_{\hat{DS}}$ The moments vectors, equation (11), are generated by calculating the various ordered moments across the columns of $\underline{\mathbf{Z}}_{\hat{DS}}$ for each matrix. The columns of the matrices are the R_i. As explained in section 2.6, the moments vector from each R_i are concatenated into the device's final fingerprint, equation (12).

2.6.3 Radio Frequency Fingerprinting.

RF-DNA fingerprints are generated from the collection of RF emissions and can be generated from both the Time Domain (TD) and the Spectral Domain (SD) [28]. The fingerprints are derived from the synchronization parameters (preambles, midambles, postambles, etc). For ZigBee transmissions, the SOI for RF-DNA is the SHR because it is the portion of the signal that is constant burst to burst. The SOI can be divided many different ways in the TD to generate multiple R_i. In previous research the SOI was equally partitioned in the TD such that all R_i are equal in time plus one R_i that encompasses the entire SOI [12, 13]. The sampled complex signal is written as $\mathbf{r}[n] = s_I[n] + js_Q[n]$, where s_I and s_Q are the I-Channel and Q-Channel components of the signal, respectively. The common signal characteristics used in RF-DNA fingerprinting are the instantaneous amplitude ($\mathbf{a}$)

$$\mathbf{a}[n] = \sqrt{|s_I[n]|^2 + |s_Q[n]|^2}, \qquad n = \{0, 1, 2, ..., N-1\}, \tag{19}$$

instantaneous phase ($\boldsymbol{\phi}$)

$$\boldsymbol{\phi}[n] = tan^{-1}\left(\frac{s_Q[n]}{s_I[n]}\right), \quad s_I[n] \neq 0, \quad n = \{0, 1, 2, ..., N-1\}, \tag{20}$$

and instantaneous frequency ($\boldsymbol{f}$)

$$\boldsymbol{f}[n] = \frac{1}{2\pi}\left(\frac{d\phi[n]}{dn}\right) \qquad n = \{0, 1, 2, ..., N-1\}. \tag{21}$$

2.7 Multiple Discriminant Analysis/Maximum Likelihood

The intent of fingerprints is to classify a device based on its RF emissions. Classification consists of processes that can effectively detect the differences in the fingerprints in a manner that maximizes device discrimination. MDA/ML is a parametric classification process consisting of a transformation (MDA) followed by a parametric classification decision (ML)[30]. The intent of MDA is to minimize feature dimensionality while also maximizing the separation between input classes. This is done by taking a projection of a full-dimension fingerprint in a lower-dimension space, Figure 6. The MDA model is created with fingerprints from known sources.

After the model is created, classification is the next step. Classification is performed by a ML estimation process based on Bayesian posterior probablity with uniform cost and equal prior probability given as[31]:

$$P(H_i|\mathbf{x}) = \frac{p(\mathbf{x}|H_i)P(H_i)}{p(\mathbf{x})}. \tag{22}$$

Classification is made by taking a fingerprint from an unkown source and estimating the device that most likely matches that fingerprint across a range of energy per bit to noise power spectral density ratio (E_b/N_0). The accuracy of the classifier is the metric by which the fingerprinting techniques are compared.

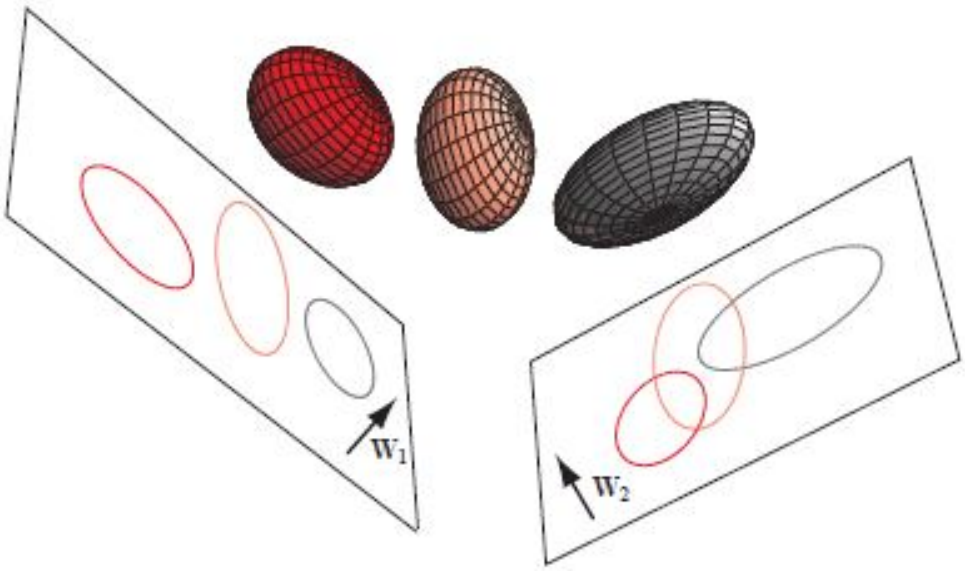


Figure 6. MDA/ML Projection of 3D Space into 2D Space [2]. In this case, the plane W_1 shows the maximum separation between input classes while minimizing feature dimensions.

III. Methodology

Wireless Sensor Network(s) (WSN) are proliferating as we desire more and more autonomous technology. As WSN start to control more of our critical infrastructure and systems the protection of their wireless communications are also critical. Physical-Layer (PHY) based fingerprinting techniques have shown to be effective in adding an additional layer of security for RF emitting devices. As there are multiple fingerprinting methods with varying effectiveness, this research aims to provide a comparative analysis of Constellation Based-Distinct Native Attributes (CB-DNA), Radio Frequency-Distinct Native Attributes (RF-DNA), and Correlation Based-Distinct Native Attributes (COR-DNA) using ZigBee devices, a WSN platform.

This chapter will cover the methodology used in experimentation of fingerprinting techniques. This chapter also provides mathematical and graphical verification for the described methodology. The results of the experiments are presented in Chapter IV.

3.1 Experimentation Equipment and Set Up

Fingerprints were generated for ten *Atmel* AVR RZUSB Sticks and 8 HackRF One SDRs. The MAC addresses for the RZUSB Sticks were used through out the documentation for differentiating purposes, Table 2, and the HackRF One SDRs were simply assigned a number. The only receiver used was an *Ettus Research* USRP with a X310/UBX-160 motherboard/daughterboard configuration. All transmissions with the RZUSB Sticks and collections were done inside a *Ramsey* STE4400 shielded test enclosure, which has a $> 90dB@2GHz$ isolation rating[32]. The HackRF One transmissions and collections were done in the open air with their antennas in close proximity because the HackRF One could not be configured inside the STE4400. The

signal was collected at an Signal to Noise Ratio (SNR) of $E_b/N_0 \geq 30\,dB$ to mitigate adverse affects of open air collections. The sampling frequency of the receiver was constant for all transmissions at $F_{Samp} = 5\,MSamp/s$. This F_{Samp} value was chosen because it exceeds the Nyquist sampling rate for the ZigBee signal bandwidth of $W_{RF} = 2\,MHz$ and it is a closer representation of a real network where oversampling is computationally expensive.

The experiments were designed to minimize any unintentional exterior influences on the fingerprinting processes. As such, a transmission file was created that all the devices transmitted. The file consisted of 1500 data packets. It was empirically determined that the maximum number of data symbol(s) (DS), (N_{DS}) packets was $N_{DS} = 212DS$, including the 10 DS of the Synchronization Header (SHR). The SHR was inherent to the RZUSBstick and could not be altered. The other 202 DS were drawn from a uniform random integer distribution from 0-15 with probability of:

$$p_{DS}[n] = \frac{1}{16}. \tag{23}$$

The RZUSBstick factory installed firmware does not allow for the manipulation of timing nor contents in the data packets. In order to control the data packets

Table 2. MAC Addresses of RZUSBSTICK Devices

Device	MAC
0	A0F69FE0
1	A0F69FE7
2	A0014370
3	A0015D34
4	A0F6A068
5	A0F6A04E
6	A0F69FFF
7	A0F6A00C
8	A0F6A004
9	A0F69FEA

transmission, KillerBee firmware was flashed onto each RZUSBsticks with an *Atmel* AVR One!. The *Atmel* AVR One! is a development tool for all AVR devices with On-Chip coding and debugging capabilities. It provides a high-speed data transfer between a host PC and the target AVR device. The AVR One! allowed for the KillerBee firmware upgrade through the RZUSBstick JTAG interface.

The data packets were converted from a text file to a libpcap file with the KillerBee *zbconvert* function. Next, the *zbreplay* function allowed the RZUSB Sticks to transmitted the data packets. There was a delay of $T_{delay} = 0.05s$ between packet transmissions to avoid any inner-packet overlap.

3.2 Receiver Design

With the intent to analyze multiple fingerprinting techniques, multiple receivers were simulated in MATLAB. A single block diagram with the multiple receivers are shown in Figure 7. Each demodulation and fingerprint generation technique that was used required the signal to go through an initial series of processes that enabled the signal to be demodulated and the device to be fingerprinted. The initial signal processes were, namely, Energy Based Burst Detector 3.2.1, Lowpass Interpolation 3.2.2, Frequency Offset Detector 3.2.3, Phase Correction 3.2.4, and Correlation Alignment 3.2.5.

The end result of the initial signal process were aligned equal-length sampled bursts. The total number of samples in each received burst was calculated as:

$$N_{Samp/burst} = N_{DS/burst} \times N_{CS/DS} \times N_{Samp/CS} = 33,920\, Samp/burst, \qquad (24)$$

where the number of DS per burst was $N_{DS/burst} = 212\,DS/burst$, the number of constellation symbol(s) (CS) per DS was $N_{CS/DS} = 16\,CS/DS$, and the number of samples per CS was $N_{Samp/CS} = 10\,Samp/CS$.

3.2.1 Burst Detection.

The input of the Burst Detector was the ZigBee signal that was captured and sampled at $f_{Samp} = 5\,MSamp/s$ by an X-310/UBX-160 SDR with a UX-160. The output was a single burst with a predetermined length of 36000 samples. The bursts were extracted using an energy detection technique, where a portion of the signal was determined to be a ZigBee data packet if the energy of the signal exceeded a empirically predetermined threshold for more than 250 samples. This method protected against falsely identifying a noise spike that exceeded the threshold for a few samples as a true ZigBee burst.

3.2.2 Lowpass Interpolation.

The sample frequency (f_{Samp}) of the Software-Defined Radio (SDR) receiver was set to $f_{Samp} = 5\,MSamp/s$ to exceed Nyquist sampling rate for a signal bandwidth of $W_{RF} = 2\,MHz$ and to simulate a true receiver's f_{Samp}, where oversampling would

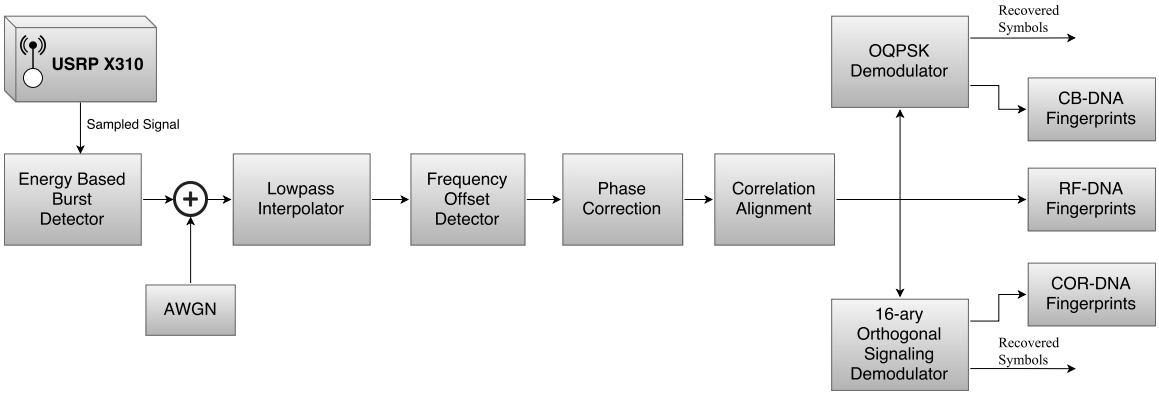


Figure 7. Offset-Quadrature Phase Shift Keying (O-QPSK) and 16-ary Orthogonal Signaling Receiver and Fingerprint Generator.

be cost prohibitive. As explained in section 2.5, O-QPSK delays the Q-channel by T_s, such that at $f_{Samp} = 5\,MSamp/s$. In terms of Samples per Constellation Symbol (SPS), where

$$N_{SPS} = \frac{f_s}{R_s}, \tag{25}$$

$N_{SPS} = 5$, thus the sample delay ($Samp_d$) of the Q-channel was $Samp_d = 2.5\,samples$. Having $Samp_d$ as a non-integer required interpolation of the data as part of the process. Simple linear interpolation is not ideal for a sinusoidal signal as the interpolated data would be a best fit match for a straight line between two sampled data points. For these reasons, Lowpass Interpolation (LPI) was used.

LPI is a defined as a two-step process to interpolate data with a lowpass filter as follows[33]:

1. Up-sample the signal by the interpolation factor of L samples. This introduces a high frequency component to the signal.

2. Apply a lowpass filter that is designed specifically to remove high frequencies and interpolate the data. The frequency response of an ideal LPI filter is defined as:

$$H_{lin}e^{(j\omega)} = \frac{1}{L}\left[\frac{sin(\omega L/2)}{sin(\omega/2)}\right]^2. \tag{26}$$

The LPI that was used had an interpolation factor of $L = 2$ to both, minimize the amount of interpolated data and make the Q-Channel $Samp_d$ an integer, specifically $Samp_d = 5\,samples$. The filter was implemented in MATLAB as a fourth order Butterworth filter with a bandwidth of $W_{RF} = 2.48\,MHz$. W_{RF} is slightly less than the original maximum sampling bandwidth for $F_{Samp} = 5MSamp/s$ for two reasons:

1. It ensures that no upsampled copies of the signal remain.

2. MATLAB filtering can be problematic if $W_{RF} = \frac{F_{Samp}}{2}$ exactly.

The filter was implemented with the *filtfilt* function and had a magnitude response as shown in Figure 8 and a zero-phase response [34].

As a result of the LPI, all subsequent digital signal processes, including fingerprinting, were completed with the parameters of $F_{Samp} = 10\,MSamp/s$, $f_{SPSym} = 10\,SPSym$, and Q-Channel $Samp_d = 5\,samples$. The process and effect of the LPI in the spectral domain is shown in a series of figures in Figure 9.

3.2.3 Frequency Correction.

The purpose of frequency correction is to remove the frequency carrier offset (f_c). The f_c was estimated using the modified rife algorithm which has been shown in previous research as a valid approach to identify f_c in a Minimum Shift Keying (MSK) signal[35]. The algorithm applies also to ZigBee transmissions because MSK is a special case of O-QPSK with sinusoidal symbol weighting[21]. The square of a MSK signal is given as[35]:

$$s^2(t) = A^2 exp\left(j4\pi\left[f_c + \frac{a(t)}{4T_s}\right]t + 2\phi_0\right), \tag{27}$$

where T_s is the symbol interval and ϕ_0 is an equivalent phase. Equation (27) shows the the square of MSK signal is a Frequency Shift Keying (FSK) signal with two carrier frequencies

$$f_1 = 2f_c + \frac{1}{2T_s},\ f_2 = 2f_c - \frac{1}{2T_s}. \tag{28}$$

The summation of f_1 and f_2 gives f_c as:

$$f_c = \frac{1}{4}(f_1 + f_2). \tag{29}$$

The estimation and removal of f_c was accomplished through the following steps:

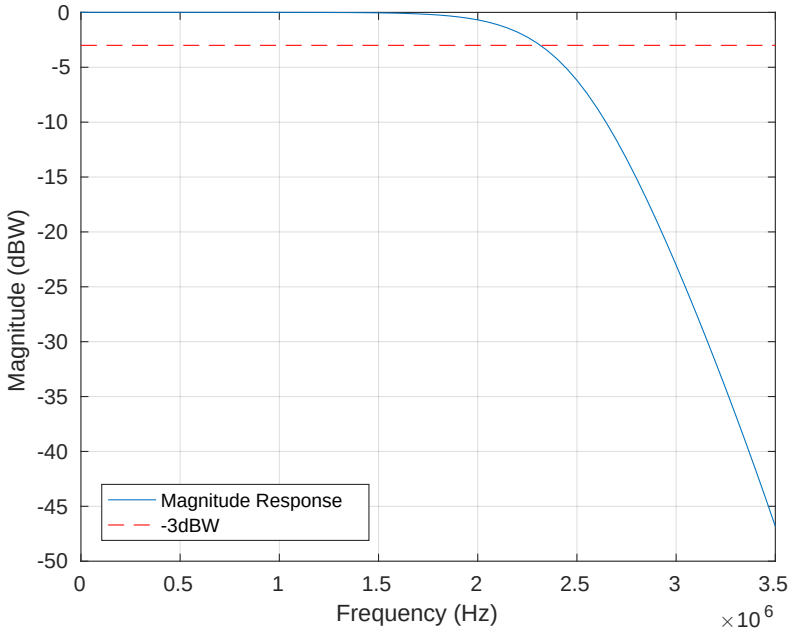


Figure 8. Magnitude Response of implemented Lowpass Interpolation filter.

1. Apply a square operation to the burst $b(t)$.

2. Compute a Discrete Fourier Transform (DFT) of $(b(t))^2$

3. Record the position of the two peaks in the DFT. These are the estimates $\hat{f}_1$ and $\hat{f}_2$ and are displayed in Figure 10.

4. Apply equation 29 to derive the estimate $\hat{f}_c$.

5. Remove $\hat{f}_c$ from $b(t)$,

$$b_{baseband}(t) = b(t) * exp(-j2\pi\hat{f}_c t). \tag{30}$$

The accuracy of $\hat{f}_c$ is dependent on the accuracy of $\hat{f}_1$ and $\hat{f}_2$ which are factors the resolution of the DFT and energy per bit to noise power spectral density ratio (E_b/N_0). Due to these factors, an estimation error $(err_{\hat{f}_c})$ will still exist. It is given

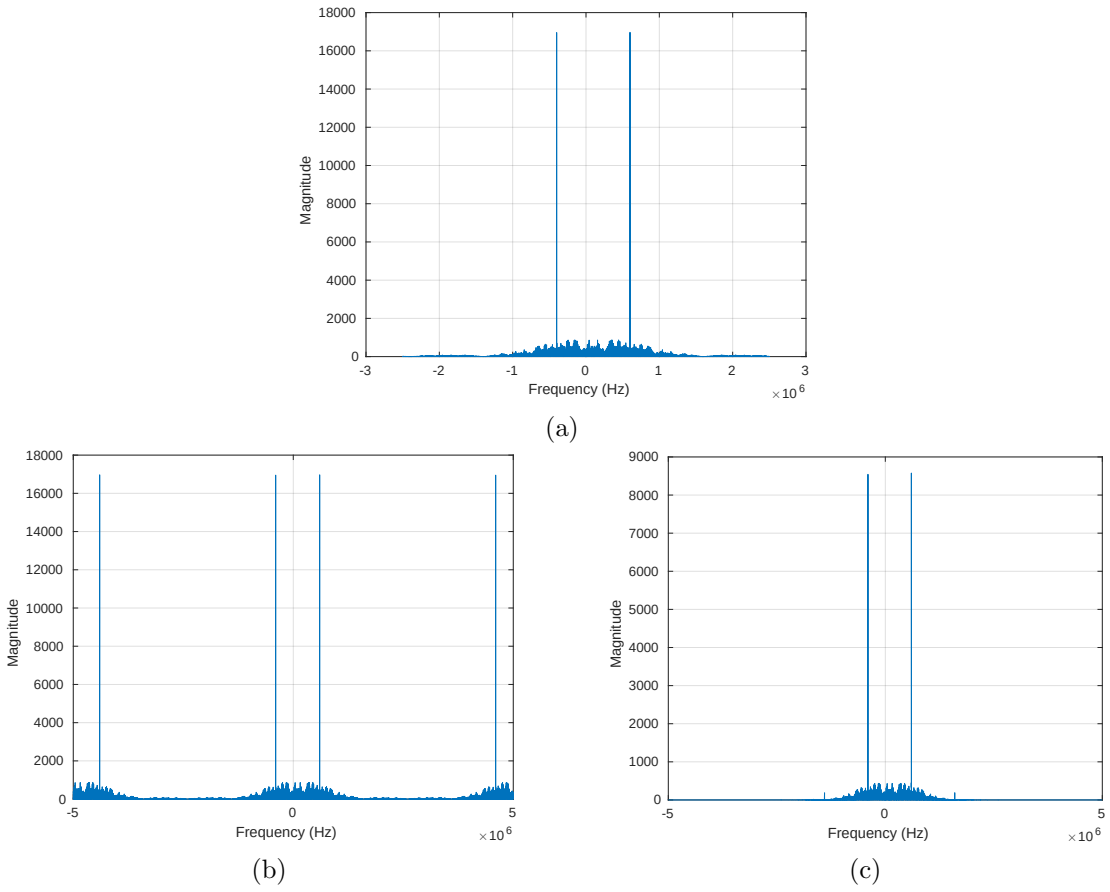


Figure 9. Frequency domain representation of Lowpass Interpolation. (a)Original O-QPSK signal with $F_{Samp} = 5\,MSamp/s$. (b)Post up-sampling by a factor of $L = 2$. The signal has an added high frequency component. (c)After LPI, the filter removed the high frequency component and interpolated the data as if $F_{Samp} = 10\,MSamp/s$.

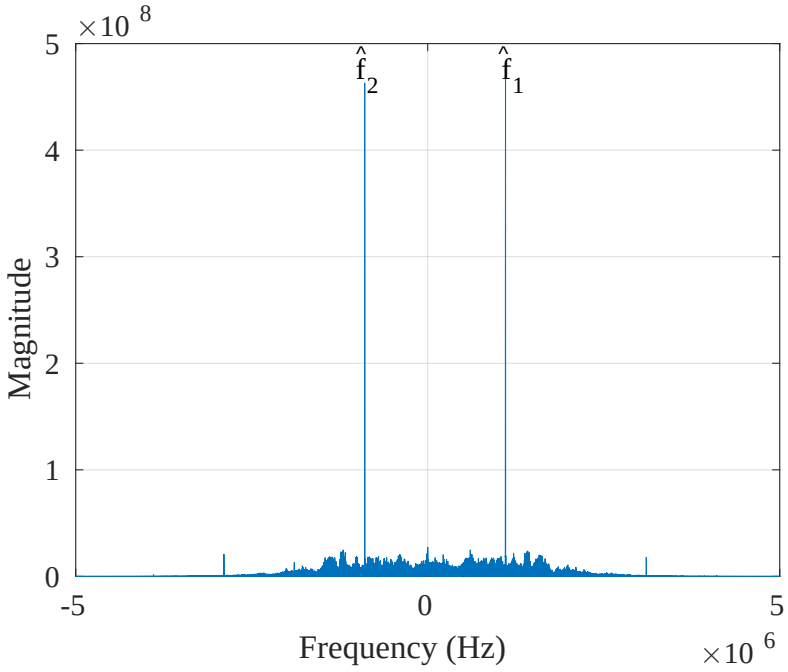


Figure 10. DFT of a squared O-QPSK ZigBee burst. $\hat{f}_1$ and $\hat{f}_2$ are defined in equation (28) and are used in equation (29) to derive $\hat{f}_c$.

as:

$$err_{\hat{f}_c} = \left| f_c - \hat{f}_c \right|. \tag{31}$$

The mean and variance of $err_{\hat{f}_c}$ was calculated as a function of E_b/N_0 via adding a known f_c to an ideal signal and comparing it with the derived $\hat{f}_c$. Figure 11 shows how the mean $err_{\hat{f}_c}$ diminished to the resolution of the implemented DFT given as

$$res_{DFT} = \frac{W_{DFT}}{N_{points}} = 1.19\,Hz, \tag{32}$$

where $W_{DFT} = 10\,MHz$ and $N_{points} = 2^{23}$. Due to the remaining $err_{\hat{f}_c}$, the constellation symbols will rotate during the time of the burst (T_B). If the symbols rotate more than their phase separation of $\phi_s = \frac{\pi}{2}\,radians$ the demodulation will not be correct because the receiver cannot synchronize the symbol constellation and the burst. The

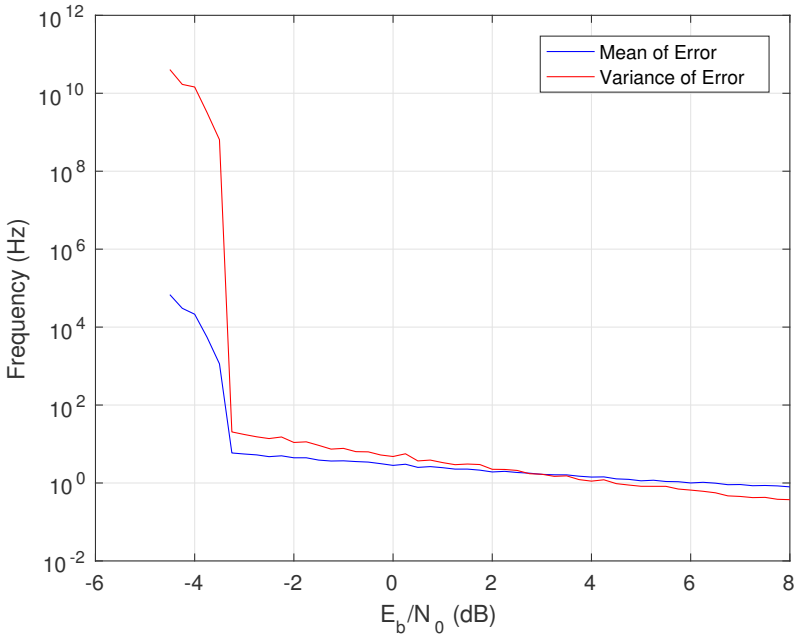


Figure 11. Mean and Variance of $err_{\hat{f}_c}$ Error vs E_b/N_0. For $E_b/N_0 < 3.5\,dB$ the frequency correction exceeds operational bounds.

maximum allowable $err_{\hat{f}_c}$ can be derived from the following equation:

$$sin\left(2\pi(err_{\hat{f}_c})T_B\right) \leq \frac{\pi}{2}. \tag{33}$$

Solving equation (33) for $err_{\hat{f}_c}$ shows that

$$err_{\hat{f}_c} \leq \frac{sin^{-1}(\pi/2)}{2\pi T_B} \approx 47\,Hz, \tag{34}$$

where,

$$T_B = \frac{212\,DS/burst}{R_{DS}} = 3.39 \times 10^{-3}\,s. \tag{35}$$

The maximum $err_{\hat{f}_c}$ was verified by adding a known $err_{\hat{f}_c}$ and examining the normalized symbol projection as a factor of time for an entire burst. If the add $err_{\hat{f}_c}$ caused the projections to rotate beyond constellation symbol boundary. Figure 12 illustrated the effect of $err_{\hat{f}_c}$ on the constellation projections by examining just the In-Phase of

the signal, thus becoming a Binary Phase Shift Keying (BPSK) signal and having one constellation symbol boundary. At $err_{\hat{f}_c} = 0$ there is no rotation in the projections. At $err_{\hat{f}_c} = 48$ the projections cross the symbol boundary before $T_B = 3.39 \times 10^{-3} s$. For $err_{\hat{f}_c} >> 47\,Hz$, synchronization fails and demodulation is meaningless.

3.2.4 Phase Correction.

There was a phase ambiguity in the received burst, the purpose of phase correction is to estimate the phase offset of the burst and correct for it. A previously documented approach has been shown to remove the phase offset by shifting the signal sample by sample and tracking the opening of the eye[36]. A similar approach was used where a phase shift ($\hat{\phi}$) intentionally added to the burst and incremented in small steps for $\hat{\phi} = 0, 0.1, ..., \frac{pi}{2}\, radians$. After each incrementation the constellation projection samples were overlaid, similarly to an eye-diagram. The maximum opening of the eye was tracked and the $\hat{\phi}$ attributed to the maximum opening was added to the burst to correct the phase offset as follows:

$$out(t) = in(t) * exp(j\hat{\phi}). \tag{36}$$

3.2.5 Correlation Alignment.

Determining the beginning sample of a received signal and the correct orientation of the symbol constellation are essential steps in the demodulation and fingerprinting processes. The correlation alignment section of the receiver solved these inherent ambiguities through a series of cross correlation and inner product operations.

The starting position of the received signal was found by calculating the maximum cross correlation (R_{XY}) value between the received signal and a simulated ZigBee

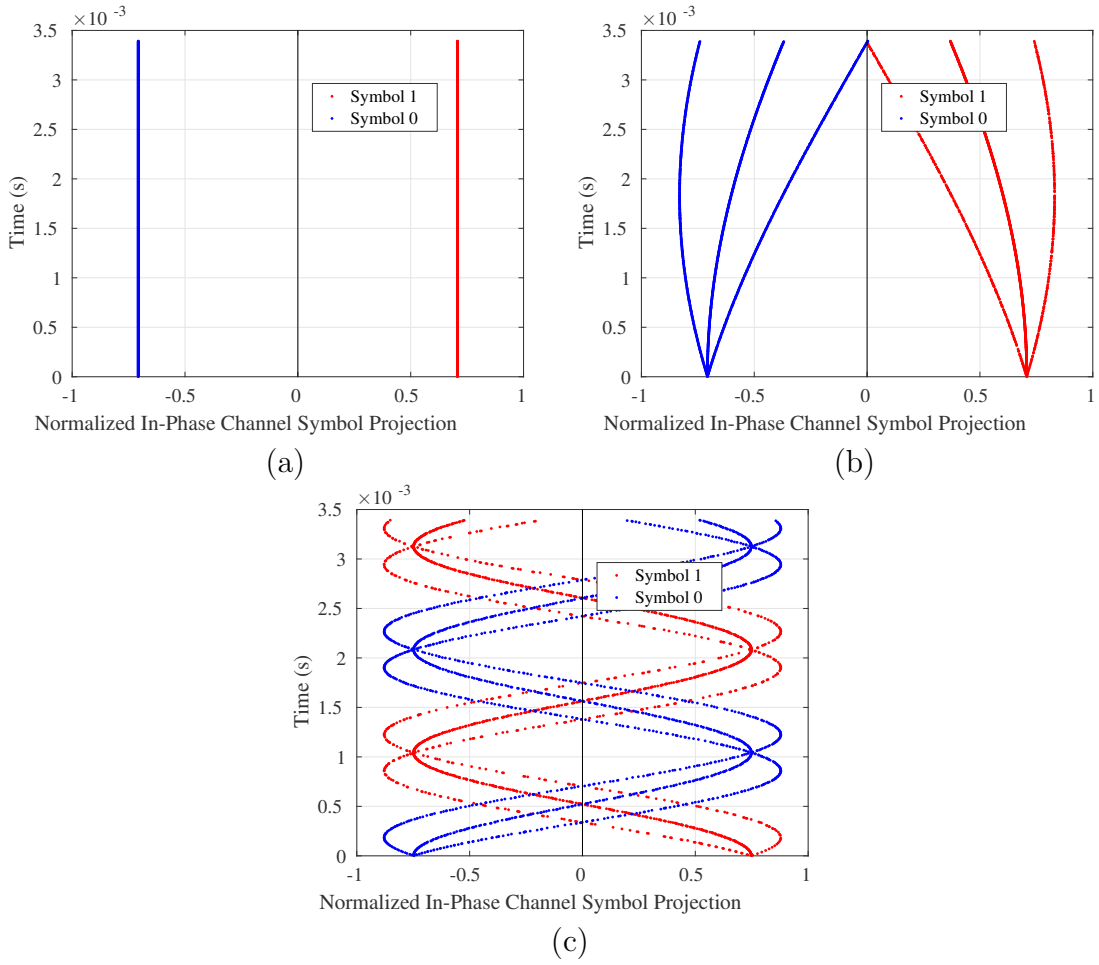


Figure 12. Simulated BPSK symbol projections vs time with: (a) $err_{\hat{f}_c} = 0\,Hz$, (b) $err_{\hat{f}_c} \geq 48\,Hz$, and (c) $err_{\hat{f}_c} = 480\,Hz$. At $err_{\hat{f}_c} = 48\,Hz$ symbol projections will cross the MLE symbol boundary within $T_B = 3.39 \times 10^{-3}$ seconds.

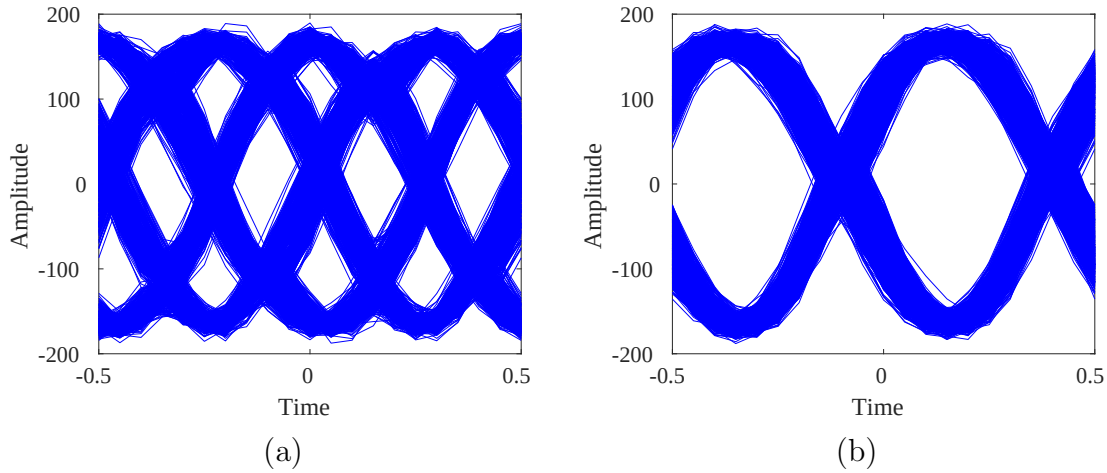


Figure 13. Eye-diagram showing: (a) Burst with no phase correction, (b) Burst after phase offset corrected.

preamble. R_{XY} is given as[26]:

$$R_{XY}[n_1, n_2] = E\left[X[n_1]Y[n_2]\right], \tag{37}$$

where $X[n_1]$ is the sampled received signal and $Y[n_2]$ is the simulated preamble. The exact sample of maximum R_{XY} differed burst-to-burst but all had a very distinguishable maximum value, as shown in Figure 14. Furthermore, to determine the proper orientation of the symbol constellation, the inner product, given as[37]:

$$\mathbf{a} \cdot \mathbf{b} = \sum_{n=1}^{N} a[n] \times b[n], \tag{38}$$

of the In-Phase of the received signal and In-Phase simulated SHR ($\mathbf{I}_{Rx} \cdot \mathbf{I}_{sim}$) was compared to the inner product of the In-Phase of the received signal and Quadrature-Phase of the simulated preamble ($\mathbf{I}_{Rx} \cdot \mathbf{Q}_{sim}$). If $\mathbf{I}_{Rx} \cdot \mathbf{I}_{sim} > \mathbf{I}_{Rx} \cdot \mathbf{Q}_{sim}$, then the phase were determined to be correct as received. Otherwise, they were switched. Likewise, if $\mathbf{I}_{Rx} \cdot \mathbf{I}_{sim} > 0$ and $\mathbf{Q}_{Rx} \cdot \mathbf{Q}_{sim} > 0$, then the received symbol constellation axes were not inverted. The proper configuration of the symbol constellation is shown in figure 2.

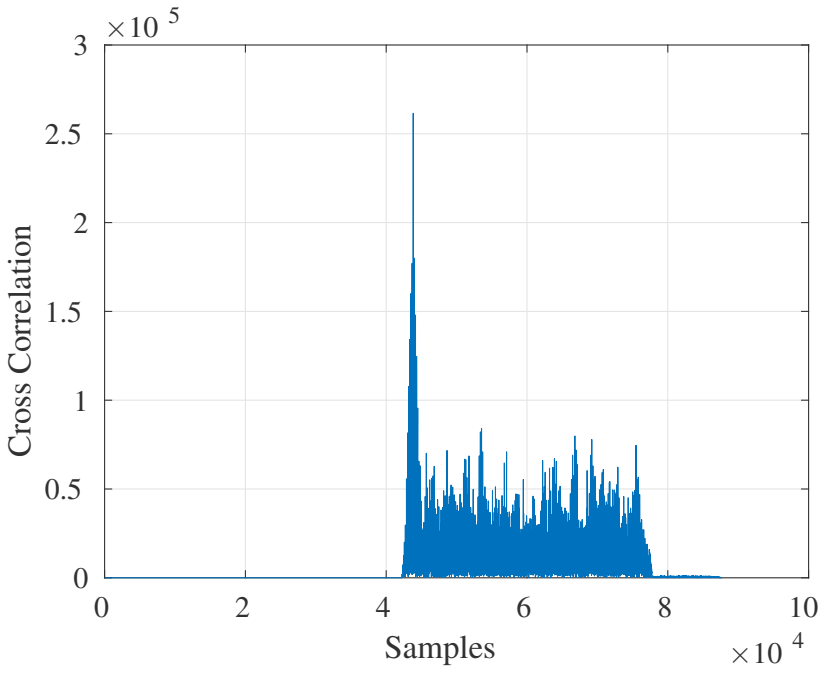


Figure 14. Cross Correlation of received sampled signal with simulated SHR. The peak signifies maximum correlation and the starting sample of the burst.

3.3 CB-DNA

CB-DNA fingerprinting was a two-step process. The first step was demodulation of the signal to acquire constellation projections, discussed in section 3.3.1. The second step was a create meaningful statistical profile of the projections, as described in section 3.3.2.

3.3.1 O-QPSK Demodulation.

The O-QPSK receiver operated as two separate BPSK receivers. The quadrature-phase offset was removed in the sample space as:

$$Q[n] = Q\left[n + \frac{N_{SPS}}{2}\right], \tag{39}$$

where $N_{SPS} = 10$. The decision stage projected the output of the I-Channel and Q-Channel correlation receivers into the O-QPSK symbol constellation space. The

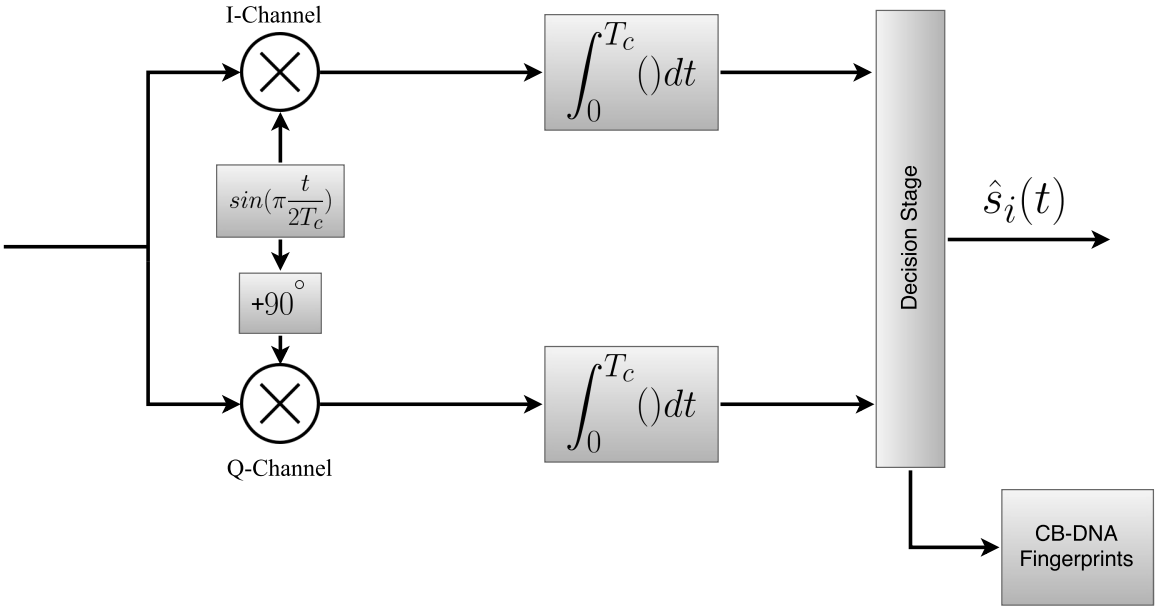


Figure 15. Block Diagram of Simulated O-QPSK Demodulator.

projection was estimated, rightly or wrongly, to be 1 of 4 constellation symbols. Any error attributed to the receiver's Symbol Error Rate (SER).

The performance of the receiver was verified by comparing simulated SER with the theoretical probability of SER ($P_E(M)$) for O-QPSK given as[21]:

$$P_E(4) = 2Q\left(\sqrt{\frac{2E_b}{N_0}}\right), \tag{40}$$

where M is the number of constellation symbols. Equation 40 is valid for both Quadrature Phase Shift Keying (QPSK) and O-QPSK. Figure 16 denotes that the simulated curve is consistent with the theoretical P_E within a normal operational energy per symbol to noise power spectral density ratio (E_s/N_0) range. The receiver could not match the theoretical for $E_S/N_0 < -1\,dB$ because below that symbol energy the frequency offset could not be removed with enough precision, or in other words, when $err_{f_o} > 47\,Hz$ the symbol constellation rotated beyond its maximum limit for

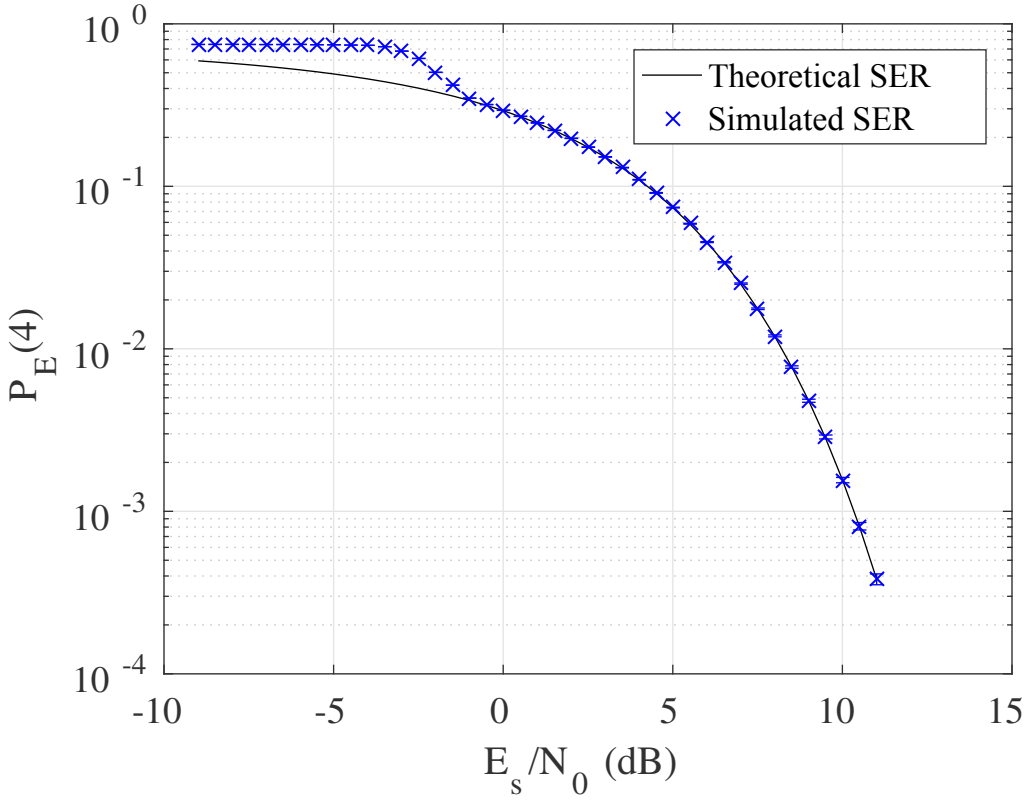


Figure 16. Simulated SER with 95% Confidence Intervals and theoretical $P_E(M)$, where $M = 4$ the number constellation symbols, for O-QSPK vs E_s/N_0.

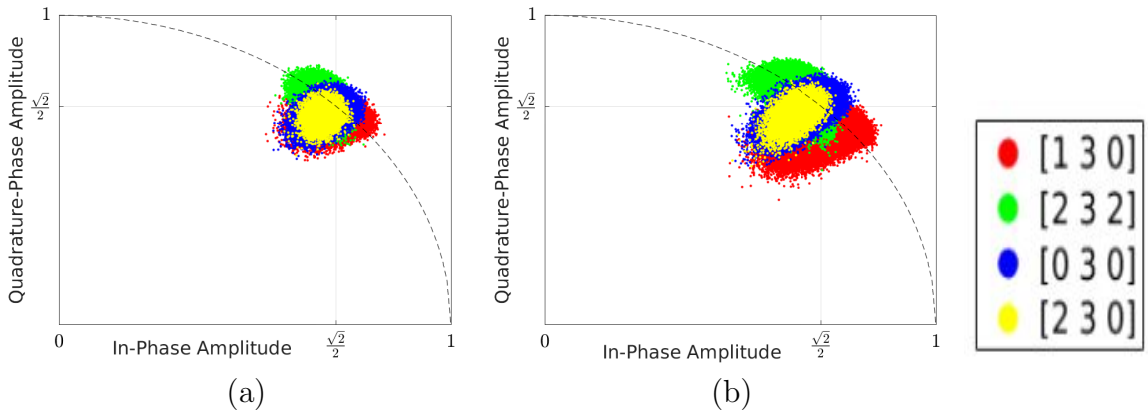
the receiver to work as explained in section 3.2.3. Figure 16 verified the performance of the receiver and that the constellation projections could be used for fingerprinting.

3.3.2 Fingerprinting: CB-DNA.

CB-DNA fingerprints were derived from features in the symbol constellation space for the entire burst. Thus, the Signal of Interest (SOI) was the entire data packet. The constellation projections were partitioned to create unique regions (R_i) within the entire burst. The R_i were all current projections (C_c) that had the same conditional transitions in the constellation symbol space. In other words, the R_i were defined as all projections with equal symbol estimation and equal previous and next symbol estimation, denoted in section 2.6.1 as $[C_p, C_c, C_n]$. The offset in O-QPSK eliminates diagonal transitions, i.e. a transition phase shift of $\phi_s > \frac{\pi}{2}$. For fingerprinting purposes, the offset was removed, thus allowed any transition and more possible R_i. Figure 17 is a visual example of how projections with different previous and next symbol estimations, and also how the same R_i from two different devices can have different distributions. The maximum number of regions is $N_R = 64$ using $R_i = [C_p, C_c, C_n]$ and 4 constellation symbols. However, it was discovered through experimentation that the spreading codes do not allow for all transitions. The PDF of the a transitions for uniform random data symbols was calculated by aligning the spreading codes in all possible orientations and numbering all occurrences of the same transition ($N_{[C_p,C_c,C_n]}$) divided by the total number of transitions (N_{trans}) as follows,

$$P_{[C_p,C_c,C_n]}([c_p, c_c c_n]) = \frac{N_{[C_p,C_c,C_n]}}{N_{trans}}. \tag{41}$$

In order to have a large enough sample for sufficient statistics in each Region(s) of Interest (ROI), the only transitions that were used had an $E[N_{[C_p,C_c,C_n]}] \geq 50$, where



(a) (b)

Figure 17. QPSK Symbol Constellation projections with equal symbol estimation ($\hat{DS}(C_c) = 3$) and unequal Single constellation symbol showing conditional transition distributions for RZ USBstick with MAC addresses: (a) A0F69FFF and (b) A0F69FEA.

the expected value for a discrete random variables is [26]

$$E[X] = \sum_k x_k P_X(x_k). \tag{42}$$

As explained in section 3.1, each burst had 212 total data symbols with 202 that were uniform random from 0 to 15, and 1 data symbol = 16 constellation symbols. Equation 42, can be solved for the minimum $P_X(x_k)$ where $\sum_x x_k = N_{trans} = 16 * 212 = 3392$ and $E[N_{C-p,C_c,C_n}] = 50$ as

$$P_X(x_k) \geq \frac{50}{3392} = 0.015. \tag{43}$$

The PDF shown in figure 18 indicated that only 30 R_i satisfied $P_X(x_k) \geq 0.015$.

The following features for each R_i were extracted:

- Variance of projected magnitude and projected phase angle
- Skewness of projected magnitude and projected phase angle
- Kurtosis of projected magnitude and projected phase angle

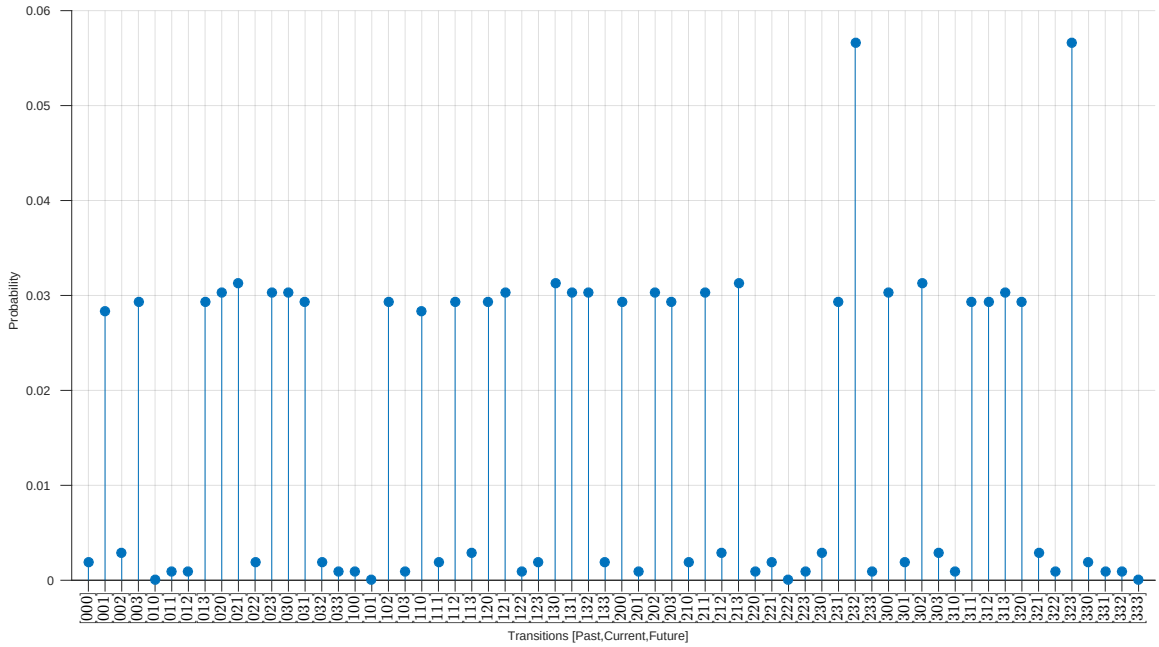


Figure 18. PDF of symbol transition for [Past,Current,Next] estimated symbols in the QPSK symbol constellation space for ZigBee transmissions with uniform random data symbols.

- All unique features of the covariance (auto covariance of In-Phase and Quadrature-Phase and their cross-covariance)

The total number of features was $N_{feats} = 9\frac{feats}{R_i} \times 30R_i = 270\, features$.

3.4 COR-DNA

COR-DNA was similar to CB-DNA in that both use a correlation receiver in a two-step process to generate fingerprints. The difference is that COR-DNA uses a 16-ary quasi-orthogonal signaling receiver, section 3.4.1. Subsequently, the fingerprinting method differed as well, section 3.4.2.

3.4.1 16-ary Quasi-Orthogonal Signaling Receiver.

ZigBee data symbols map to a 32-PN chip sequence, section 2.2. The chips are quasi-orthogonal and are related to each other through cyclical shifts and/or

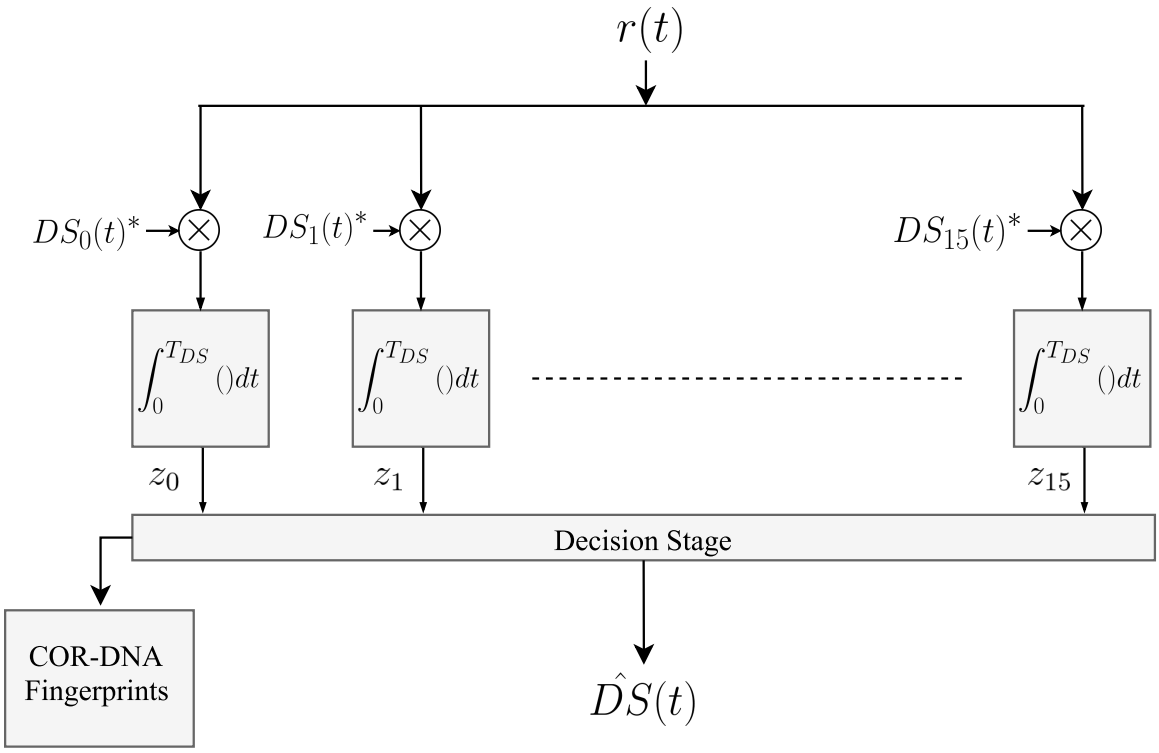


Figure 19. Block Diagram of 16-ary Quasi-Orthogonal Receiver.

conjugation[3]. The chips are modulated onto the carrier using O-QPSK but, the unique chip sequences allowed for 16-ary orthogonal signaling demodulation.

The receiver, figure 19, had 16 correlation functions where, $DS_i(t)^*$ were the conjugates of the ideal modulated complex chips, and T_{DS} is the inverse of the data symbol rate $R_{DS} = 62.5\,kDS/s$. The decision stage compared the outputs of the correlation z_i and estimated a data symbol based on the largest z_i. The performance of the receiver was verified with its symbol error rate as a function of E_s/N_0, as shown in Figure 20.

The comparison of the simulated SER to the 16-ary orthogonal signaling probability of symbol error ($P_E(16)$), given as[21]:

$$P_E(M) \leq (M-1)Q\left(\sqrt{\frac{E_s}{N_0}}\right), \tag{44}$$

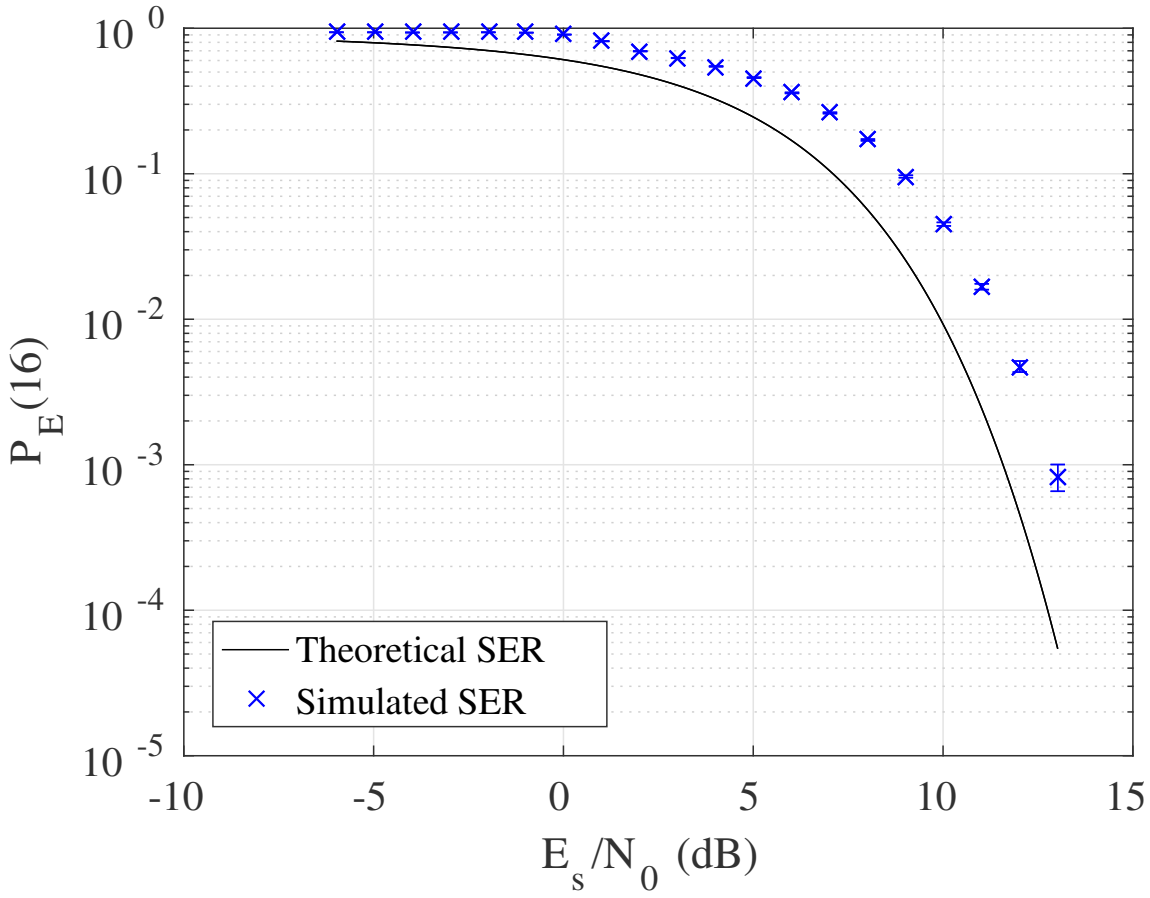


Figure 20. Simulated SER with 95% Confidence Intervals and theoretical $P_E(16)$ for 16-ary Othogonal Signaling, where $M = 16$ the number of data symbols, vs E_s/N_0.

indicates that the receiver performs similarly to a true orthogonal receiver with an offset ($\Delta E_s/N_0$). The offset for $P_E(16) = 10^{-3}$ is $\Delta E_s/N_0 \approx 1\,dB$. The offset is attributed to the usage of quasi-orthogonal codes.

Equal energy signal are orthogonal if and only if the cross-correlation coefficient of the spreading codes (z_{ij}) satisfies[21]

$$\begin{aligned} z_{ij} =& \frac{\text{number of chip agreements-number of chip disagreement}}{\text{total number of chips in the sequence}} \\ =& \begin{cases} 1, & for\, i = j \\ 0, & otherwise. \end{cases} \end{aligned} \tag{45}$$

The O-QPSK spreading codes are a combination of orthogonal and non-orthogonal codes. The values of z_{ij} are in Table 3. For the purpose of this research, it was assumed that the receiver is valid based on it's symbol error performance, where the $\Delta E_S/N_0$ is reasonably attributed to the z_{ij} values.

3.4.2 Fingerprinting: COR-DNA.

The features in the fingerprints were derived from the outputs of the correlation receivers, $[z_0, z_1, \cdots, z_{15}]$. As was the case with CB-DNA, the SOI was the entirety of the burst. The outputs were grouped together based on equal estimated data symbols . A matrix representation of $[z_0, z_1, \cdots, z_{15}]$ for $\hat{DS} = 0$ is shown in Table 4. The R_i for a burst were the columns of the matrix and the number of R_i was $N_{R_i} = 16\hat{DS} \times 16 outputs/\hat{DS} = 256$. The R_i were normalized to account for different energy fluctuations burst to burst. Each R_i had a unique distribution, which was seen by comparing an equal set of bursts transmitted by two RZ USBsticks, Figure 21. The following features for each R_i were extracted:

- Variance of projected magnitude and projected phase angle

Table 3. Cross Correlation Coefficient Values (z_{ij}) of the 32-PN Chip Sequences

Data Symbols	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	0	-0.125	-0.25	-0.25	-0.25	-0.125	0	0	0.25	0.125	-0.25	-0.25	-0.25	0.125	0.25
2	0	1	0	-0.125	-0.25	-0.25	-0.25	-0.125	0.25	0	0.25	0.125	-0.25	-0.25	-0.25	0.125
3	-0.125	0	1	0	-0.125	-0.25	-0.25	-0.25	0.125	0.25	0	0.25	0.125	-0.25	-0.25	-0.25
4	-0.25	-0.125	0	1	0	-0.125	-0.25	-0.25	-0.25	0.125	0.25	0	0.25	0.125	-0.25	-0.25
5	-0.25	-0.25	-0.125	0	1	0	-0.125	-0.25	-0.25	-0.25	0.125	0.25	0	0.25	0.125	-0.25
6	-0.25	-0.25	-0.25	-0.125	0	1	0	-0.125	-0.25	-0.25	-0.25	0.125	0.25	0	0.25	0.125
7	-0.125	-0.25	-0.25	-0.25	-0.125	0	1	0	0.125	-0.25	-0.25	-0.25	0.125	0.25	0	0.25
8	0	-0.125	-0.25	-0.25	-0.25	-0.125	0	1	0.25	0.125	-0.25	-0.25	-0.25	0.125	0.25	0
9	0	0.25	0.125	-0.25	-0.25	-0.25	0.125	0.25	1	0	-0.125	-0.25	-0.25	-0.25	-0.125	0
10	0.25	0	0.25	0.125	-0.25	-0.25	-0.25	0.125	0	1	0	-0.125	-0.25	-0.25	-0.25	-0.125
11	0.125	0.25	0	0.25	0.125	-0.25	-0.25	-0.25	-0.125	0	1	0	-0.125	-0.25	-0.25	-0.25
12	-0.25	0.125	0.25	0	0.25	0.125	-0.25	-0.25	-0.25	-0.125	0	1	0	-0.125	-0.25	-0.25
13	-0.25	-0.25	0.125	0.25	0	0.25	0.125	-0.25	-0.25	-0.25	-0.125	0	1	0	-0.125	-0.25
14	-0.25	-0.25	-0.25	0.125	0.25	0	0.25	0.125	-0.25	-0.25	-0.25	-0.125	0	1	0	-0.125
15	0.125	-0.25	-0.25	-0.25	0.125	0.25	0	0.25	-0.125	-0.25	-0.25	-0.25	-0.125	0	1	0
16	0.25	0.125	-0.25	-0.25	-0.25	0.125	0.25	0	0	-0.125	-0.25	-0.25	-0.25	-0.125	0	1

Table 4. 16-ary Quasi-Orthogonal Correlation Normalized Outputs for $\hat{DS} = 0$.

Number of Times DS=0 was Estimated	z0	z1	z2	z3	z4	z5	z6	z7	z8	z9	z10	z11	z12	z13	z14	z15
1	1.00 + j0.02	-0.00 + j0.13	-0.13 + j0.07	-0.25 - j0.05	-0.25 - j0.02	-0.24 + j0.03	-0.13 - j0.05	0.00 - j0.12	-0.01 - j0.08	0.25 - j0.04	0.12 - j0.03	-0.25 + j0.11	-0.25 - j0.09	-0.24 + j0.13	0.12 + j0.03	0.26 - j0.03
2	1.01 - j0.01	-0.00 + j0.12	-0.12 + j0.10	-0.26 - j0.04	-0.26 - j0.00	-0.25 + j0.04	-0.12 - j0.07	0.00 - j0.14	0.01 - j0.08	0.25 - j0.06	0.12 - j0.04	-0.25 + j0.14	-0.25 - j0.07	-0.24 + j0.14	0.12 + j0.01	0.25 - j0.04
3	0.99 - j0.00	0.00 + j0.11	-0.11 + j0.11	-0.25 - j0.04	-0.26 - j0.01	-0.26 + j0.04	-0.12 - j0.07	0.01 - j0.14	0.02 - j0.08	0.26 - j0.07	0.12 - j0.03	-0.25 + j0.12	-0.25 - j0.06	-0.25 + j0.13	0.12 + j0.04	0.24 - j0.04
4	1.01 + j0.03	0.00 + j0.13	-0.13 + j0.10	-0.25 - j0.06	-0.25 - j0.02	-0.25 + j0.03	-0.13 - j0.06	0.00 - j0.14	0.01 - j0.06	0.26 - j0.05	0.13 - j0.03	-0.25 + j0.10	-0.25 - j0.09	-0.26 + j0.12	0.12 + j0.02	0.24 - j0.02
5	1.00 + j0.02	-0.00 + j0.12	-0.13 + j0.10	-0.26 - j0.06	-0.25 - j0.02	-0.24 + j0.02	-0.11 - j0.06	0.01 - j0.12	0.01 - j0.06	0.25 - j0.04	0.12 - j0.03	-0.26 + j0.11	-0.26 - j0.09	-0.24 + j0.12	0.13 + j0.03	0.25 - j0.04
6	1.00 - j0.00	-0.00 + j0.12	-0.13 + j0.09	-0.26 - j0.04	-0.26 - j0.02	-0.24 + j0.03	-0.13 - j0.07	0.00 - j0.11	-0.01 - j0.06	0.26 - j0.05	0.13 - j0.02	-0.25 + j0.11	-0.25 - j0.08	-0.25 + j0.12	0.13 + j0.02	0.24 - j0.04
7	0.99 + j0.00	-0.00 + j0.13	-0.13 + j0.09	-0.25 - j0.06	-0.25 - j0.01	-0.25 + j0.03	-0.12 - j0.07	0.00 - j0.11	-0.01 - j0.07	0.24 - j0.04	0.13 - j0.02	-0.25 + j0.12	-0.26 - j0.09	-0.24 + j0.11	0.13 + j0.02	0.25 - j0.04
8	1.00 + j0.02	0.00 + j0.12	-0.13 + j0.09	-0.26 - j0.03	-0.25 - j0.02	-0.24 + j0.03	-0.13 - j0.07	-0.00 - j0.13	-0.01 - j0.09	0.25 - j0.04	0.13 - j0.02	-0.24 + j0.11	-0.25 - j0.08	-0.25 + j0.13	0.13 + j0.02	0.25 - j0.04
9	1.00 + j0.01	-0.01 + j0.15	-0.12 + j0.08	-0.25 - j0.06	-0.26 - j0.03	-0.24 + j0.01	-0.11 - j0.06	-0.00 - j0.10	0.01 - j0.05	0.25 - j0.04	0.12 - j0.03	-0.25 + j0.10	-0.25 - j0.10	-0.25 + j0.11	0.13 + j0.03	0.24 - j0.02
10	1.00 - j0.04	0.00 + j0.10	-0.13 + j0.07	-0.25 - j0.02	-0.24 + j0.01	-0.26 + j0.02	-0.12 - j0.04	-0.00 - j0.10	0.00 - j0.04	0.26 - j0.03	0.13 - j0.01	-0.26 + j0.09	-0.26 - j0.10	-0.24 + j0.15	0.12 - j0.00	0.25 - j0.06
11	1.00 + j0.00	-0.01 + j0.12	-0.12 + j0.10	-0.25 - j0.05	-0.25 - j0.02	-0.24 + j0.04	-0.13 - j0.06	-0.00 - j0.13	-0.01 - j0.07	0.24 - j0.05	0.12 - j0.03	-0.24 + j0.10	-0.25 - j0.08	-0.24 + j0.13	0.13 + j0.02	0.25 - j0.03
12	1.00 - j0.02	-0.00 + j0.10	-0.12 + j0.07	-0.25 - j0.03	-0.25 + j0.00	-0.25 + j0.02	-0.13 - j0.04	-0.01 - j0.10	-0.02 - j0.05	0.25 - j0.02	0.12 - j0.01	-0.24 + j0.09	-0.25 - j0.11	-0.24 + j0.15	0.13 - j0.00	0.25 - j0.07

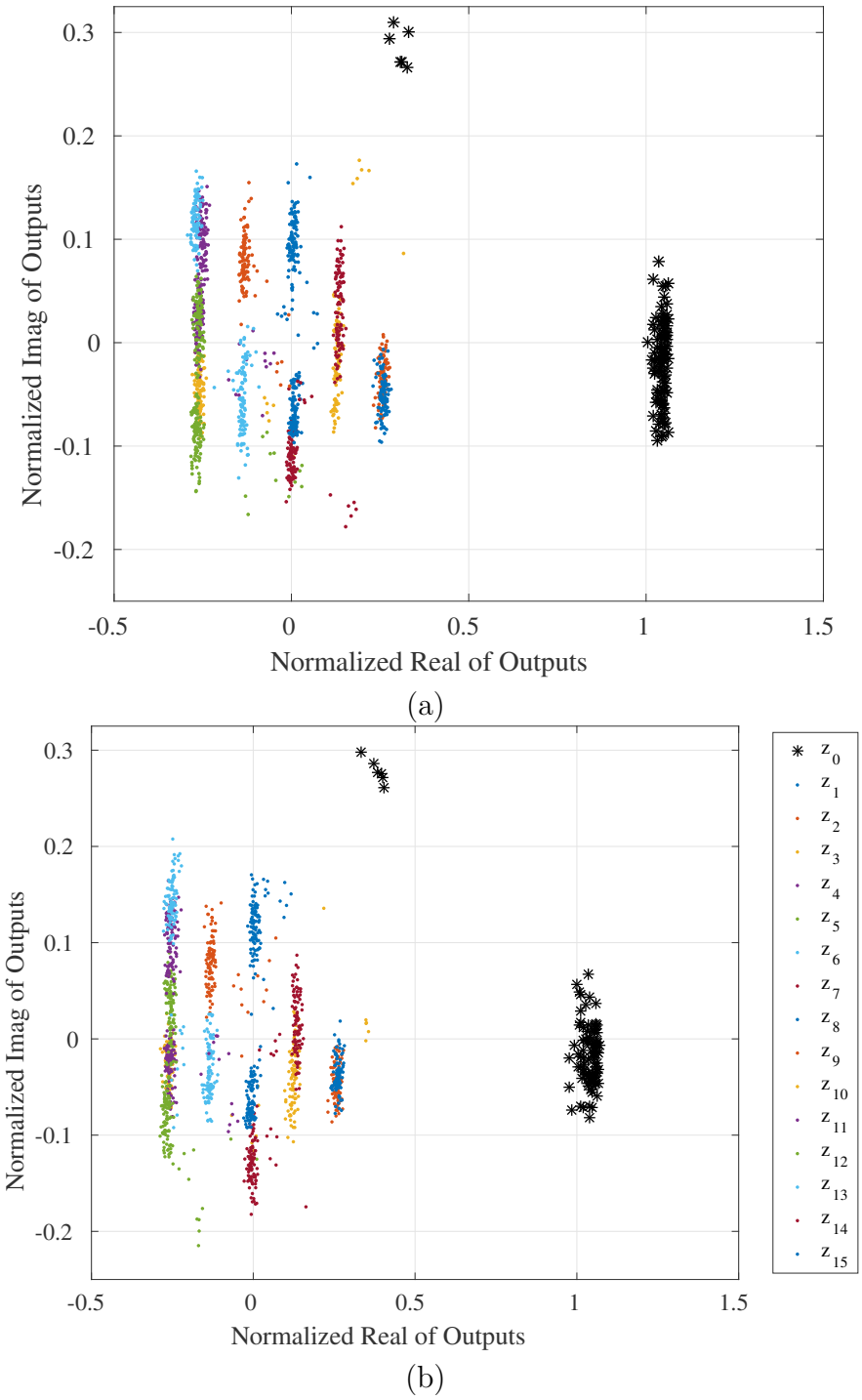


Figure 21. Normalized Outputs of 16-ary Quasi-Orthogonal Receiver where $\hat{DS} = 0$ for RZ USBsticks with MAC addresses: (a) A0F69FE0 and (b) A0015D34.

- Skewness of projected magnitude and projected phase angle
- Kurtosis of projected magnitude and projected phase angle
- All unique features of the covariance (auto covariance of In-Phase and Quadrature-Phase and their cross-covariance)

The total number of features was $N_{feats} = 9\frac{feats}{R_i} \times 256 R_i = 2304\, features$

3.5 RF-DNA

RF-DNA fingerprints were generated from baseband, lowpass filtered, Figure 23, Time Domain (TD) features of the SHR for each burst. As explained in section 2.2, the SHR consisted of 8 consecutive DS=0, the preamble, followed by the State-of-Frame Delimiter (SFD), where DS = [7, 10]. The SHR was the SOI, unlike CB-DNA and COR-DNA where the SOI was the entire burst. The SOI was partitioned into $N_{R_i} = 11\, regions$, where the boundaries of R_{0-10} were the data symbol boundaries and R_{11} is the SOI boundary. Figure 22 show the R_i boundaries for a RZ USBstick and a HackRF One burst, where at a sample rate of $f_{Samp} = 10\, MSamp/s$, $R_{11} = 1600\, Samp$ and $R_{0-10} = 160\, Samp$. The alignment of the bursts was accomplished previously as described in section 3.2.5.

The following features for each R_i were extracted:

- Standard Deviation
- Variance
- Skewness
- Kurtosis

of the instantaneous amplitude, phase, and frequency as defined in equations 19-21. The total number of features was $N_{feats} = 12\frac{feats}{R_i} \times 11 R_i = 132\, features$.

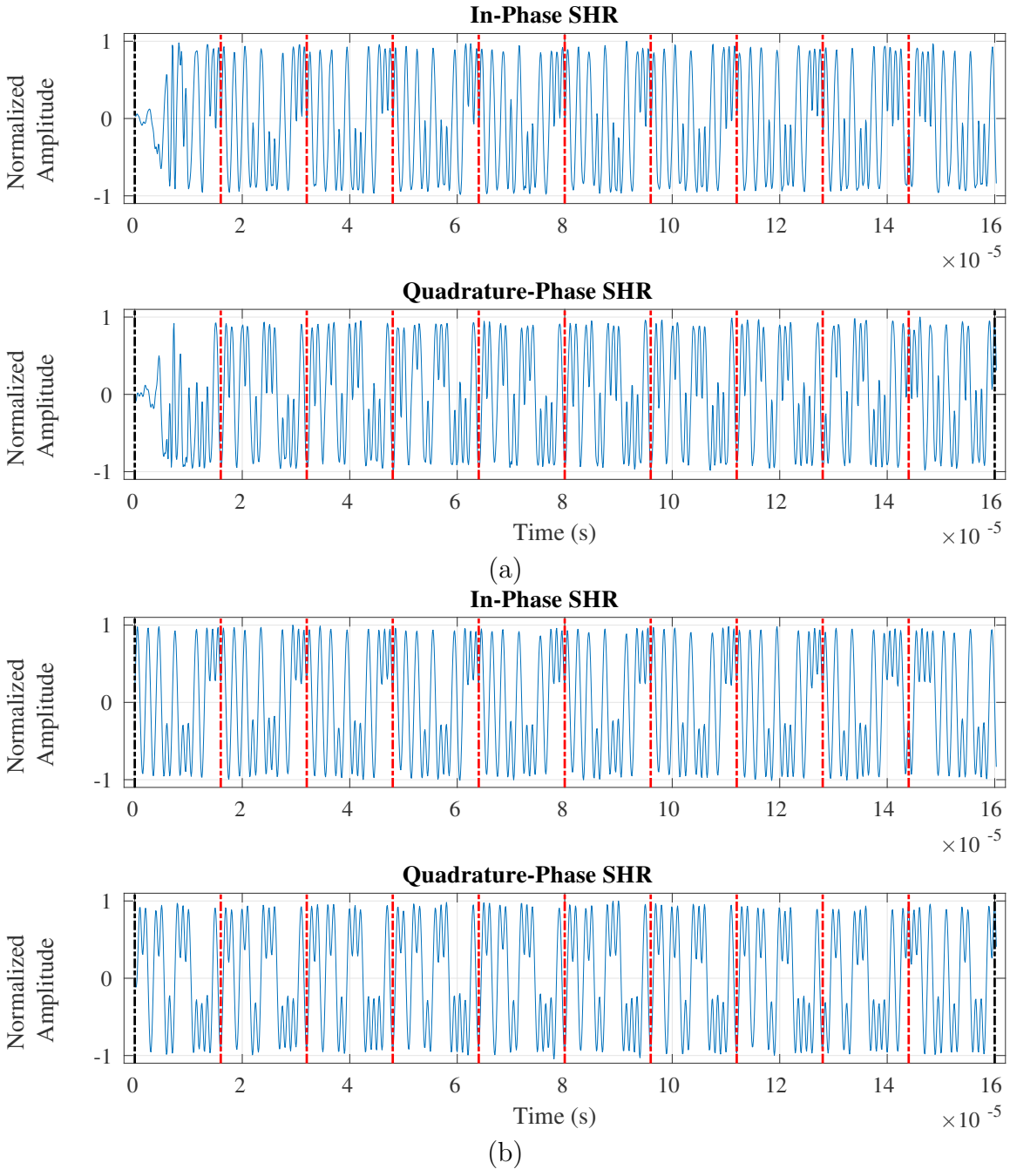


Figure 22. Collected In-Phase and Quadrature-Phase Normalized Amplitude of ZigBee Synchronization Header (SHR) with $N_{R_i} = 11$ for devices: (a) RZ USBstick A0F69FE7 and (b) HackRF01.

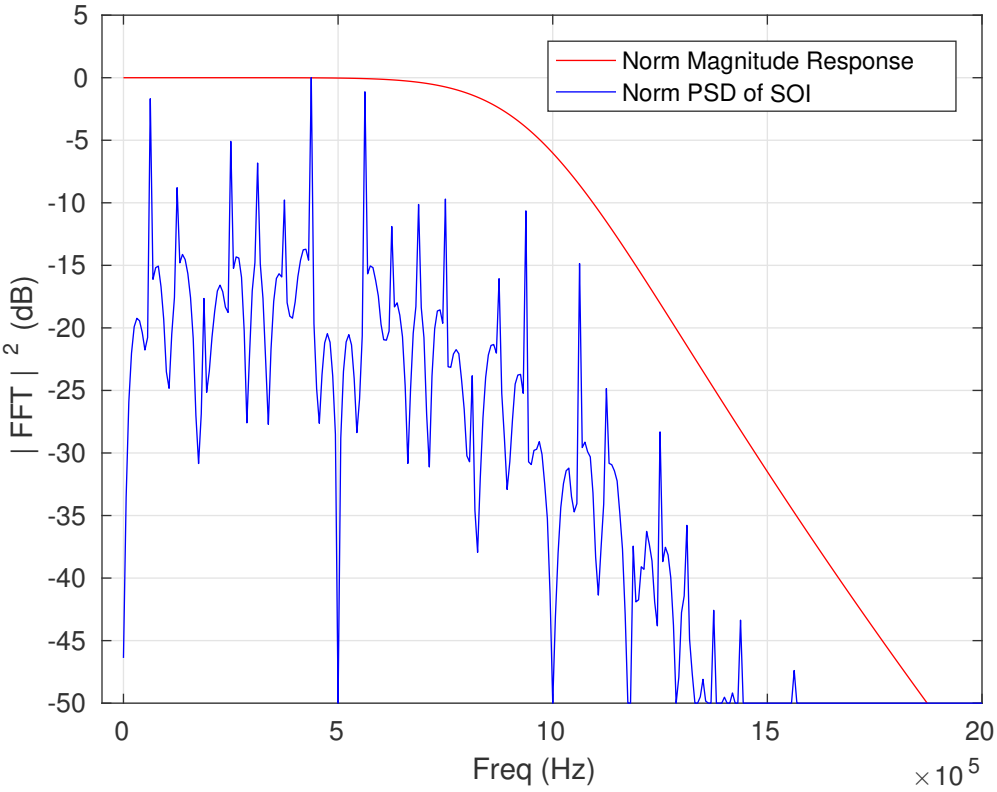


Figure 23. Normalized Magnitude Response for Lowpass filter with $W_{RF} = 1\,MHz$ and the Resultant Normalized Power Spectral Density of the SOI.

3.6 MDA/ML

The fingerprints were classified using Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classifier. The effectiveness of different classification techniques was beyond the scope of this research. However, many previous research efforts have examined different classifiers and have shown the capabilities of MDA/ML. This research assumes that the MDA/ML classifier is an adequate platform to measure differences in fingerprinting techniques.

The classification experiments were conducted with $N_{bursts} = 1000$ independent bursts. Half of the burst are used for MDA/ML training and the other half for testing. Each burst had $N_{NZr} = 4$ Monte Carlo noise realizations for each realization of E_b/N_0. E_b/N_0 realizations were do to varying the power of simulated Additive White Gaussian Noise (AWGN).

IV. Results

4.1 Introduction

This section presents the results from the Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classifier for three different fingerprinting techniques. Constellation Based-Distinct Native Attributes (CB-DNA) fingerprints were derived from projections in the Offset-Quadrature Phase Shift Keying (O-QPSK) constellation symbol space. Radio Frequency-Distinct Native Attributes (RF-DNA) fingerprints were generated from the Time Domain (TD) features in the signals' Synchronization Header (SHR). Correlation Based-Distinct Native Attributes (COR-DNA) fingerprints were a product of 16 quasi-orthogonal correlation receivers' results in the real and imaginary $(\Re, \Im)$ plane.

The results are presented with two different methods. A graphical method compares Average % Correct Classification ($\%C$) for $-4 \leq E_b/N_0 \leq 28\,(dB)$. This range was chosen because at $E_b/N_0 \leq -4\,db$ the receiver could not synchronize with the signal and typically $E_b/N_0 \geq 28\,dB$ is only achievable in a lab setting. The $\%C$ is the percent of times that the classifier correctly classified a device. The second method is a tabular comparison via a Confusion Matrix (CM). The CM diagonal entries also contain the $\%C$ data. The non-diagonal entries show the percentage of times device A was incorrectly classified as device B, C, D, etc. The rows of the CM sum to 100%.

Classification was done for two different classes of devices. One class was the AVR RZ USBStick, a ZigBee development platform, for the number of devices $N_d = 10$. Another class was the HackRF One, a Software-Defined Radio (SDR) configured to transmit ZigBee codes, for $N_d = 8$.

Results are presented for various class configurations. Section 4.2 has intra-classe classification results for both device classes. Section 4.3 shows inter-device classifi-

cation for $N_d = 1$ HackRF class and $N_d = 10$ for RZ USBstick. Section 4.4 are the results for all devices and all classes. Section 4.5 provides a comparison of results from the different tests that were done for this research effort.

4.2 Intra-Class Classification

CB-DNA, RF-DNA, and COR-DNA fingerprinting classification performance was independently measured using $N_d = 10$ RZ USBstick and $N_d = 8$ HackRF One SDRs. The objectives of the tests were to quantify differences in fingerprinting techniques through comparison of $\%C$ in MDA/ML classification for like devices. The tests were conducted by passing all of one type of fingerprints for all devices of a single class to the MDA/ML classifier, and then repeating with each fingerprinting method.

The classification results for $N_d = 10$ RZ USBsticks, displayed in Figure 24, shows the mean $\%C \geq 80\%$ at energy per bit to noise power spectral density ratio (E_b/N_0) = 17, 28, 15 dB for CB-DNA, RF-DNA, and COR-DNA, respectively. CB-DNA had the highest mean $\%C$ for $E_b/N_0 \leq 10\,dB$ including an mean $\%C = 18\%$ at the minimum $E_b/N_0 = -4\,dB$.

The results for $N_d = 8$ HackRF One, displayed in Figure 25, shows that CB-DNA achieved a mean $\%C \geq 80\%$ at $E_b/N_0 = 16\,dB$. RF-DNA and COR-DNA achieved a maximum mean $\%C \approx 18\%, 55\%$, respectively. CB-DNA was the only one to achieve mean $\%C \geq 95\%$ at the maximum E_b/N_0.

The data in Table 5 shows that device A0F69FFF had the lowest mean $\%C$ = $[76.9\%, 12.0\%, 82.8\%]$ for CB-DNA, RF-DNA, and COR-DNA, respectively. That same device also had the highest confusion percentage with device A0F6104E. Table 6 shows that the lowest mean $\%C$ occurs at $\%C = [87.0\%, 9.5\%, 1.6\%]$, however, they are not all for the same HackRF One.

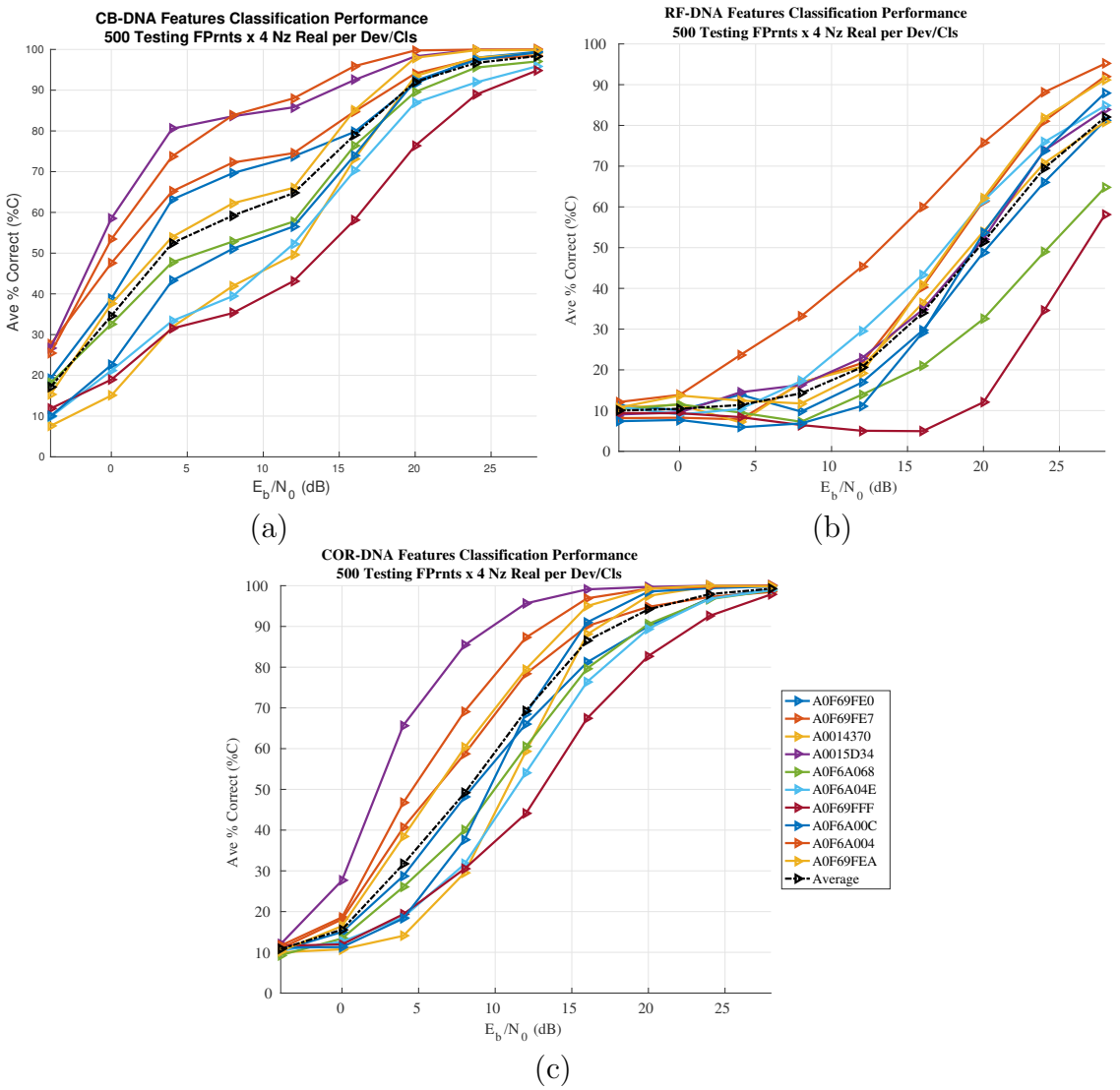


Figure 24. Intra-Class MDA/ML Classification performance for $N_d = 10$ RZ USBsticks using:(a) CB-DNA, (b) RF-DNA, and (c) COR-DNA.

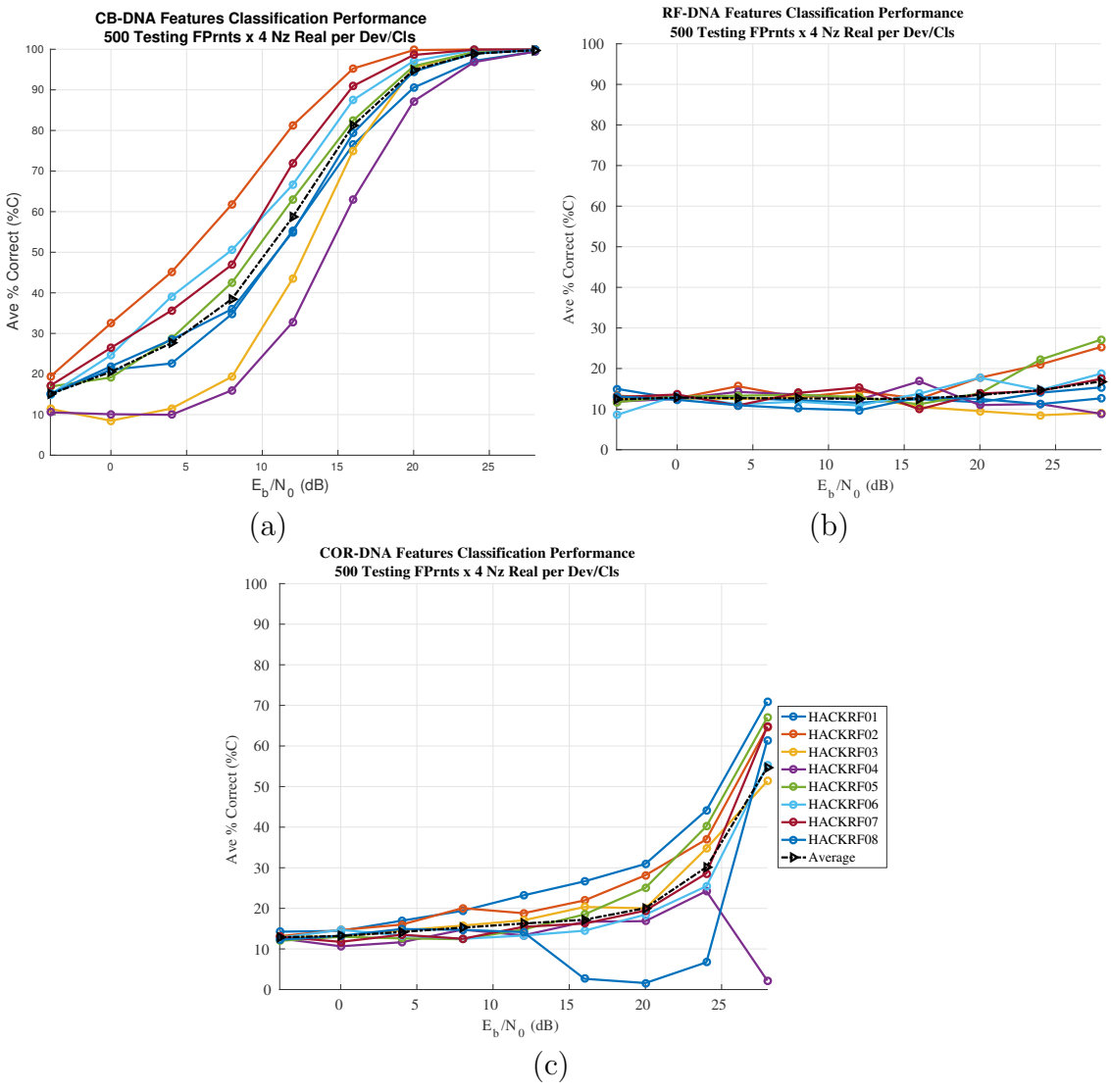


Figure 25. Intra-Class MDA/ML Classification performance for $N_d = 8$ HackRF One using:(a) CB-DNA, (b) RF-DNA, and (c) COR-DNA.

Table 5. Confusion Matrix for RZ USBstick $N_d = 10$ at $E_b/N_0 = 20\,dB$. The table formated as CB-DNA/RF-DNA/COR-DNA (%)

Classified Devices (%)

Input Device (%) CB/RF/COR	A0F69FE0	A0F69FE7	A0014370	A0015D34	A0F61068	A0F6104E	AOF69FFF	A0F6A00C	A0F6A004	A0F69FEA
A0F69FE0	91.8/48.9/90.0	0.6/4.5/0.9	0.4/10.9/0.7	0.1/11.2/0.0	1.8/8.6/4.5	2.4/3.6/1.0	2.7/5.9/2.7	0.1/2.8/0.1	0.0/0.0/0.0	0.1/3.8/0.1
A0F69FE7	2.0/7.4/3.2	94.0/61.4/94.8	0.5/1.1/0.0	0.0/2.3/0.0	0.9/0.8/0.9	0.8/13.2/0.7	1.3/2.5/0.4	0.5/4.3/0.0	0.1/5.1/0.0	0.0/1.9/0.0
A0014370	0.8/11.1/0.6	0.9/0.4/0.0	93.5/53.9/97.5	0.0/4.3/0.0	1.6/12.8/0.5	0.2/0.2/0.1	0.4/3.2/1.2	2.4/4.4/0.0	0.1/0.3/0.0	0.2/9.3/0.0
A0015D34	0.1/10.2/0.0	0.1/2.1/0.0	0.0/8.3/0.0	98.2/52.1/99.7	0.5/5.1/0.1	0.4/15.8/0.1	0.6/6.0/0.0	0.0/0.2/0.0	0.0/0.0/0.0	0.0/0.1/0.0
A0F61068	1.7/10.2/3.8	0.8/1.4/0.2	0.9/25.7/0.5	1.0/4.0/0.2	89.8/32.5/90.6	0.5/4.5/0.8	4.3/2.5/3.4	1.1/10.1/0.4	0.0/1.7/0.0	0.0/7.4/0.0
A0F6104E	2.5/5.4/1.7	0.4/13.2/0.9	0.2/0.3/0.1	0.5/9.7/0.2	1.1/1.8/0.6	86.7/61.5/89.5	8.6/5.2/7.0	0.1/1.1/0.0	0.0/0.5/0.0	0.0/1.1/0.0
AOF69FFF	1.2/15.3/1.4	2.8/5.6/2.0	0.5/15.0/1.2	0.7/14.8/0.0	4.2/6.2/3.2	13.5/26.4/9.4	76.9/12.0/82.8	0.1/1.4/0.0	0.0/0.2/0.0	0.1/3.0/0.0
A0F6A00C	0.2/2.2/0.1	0.4/5.5/0.0	3.2/4.9/0.0	0.0/0.4/0.0	1.1/7.3/0.1	0.1/1.4/0.0	0.1/0.5/0.1	92.6/53.5/98.6	0.8/11.3/0.7	1.5/13.0/0.5
A0F6A004	0.0/0.1/0.0	0.0/6.5/0.0	0.1/0.8/0.0	0.0/0.0/0.0	0.0/0.8/0.0	0.0/0.4/0.0	0.0/0.1/0.0	0.1/9.4/0.6	99.8/75.8/99.2	0.1/6.3/0.1
A0F69FEA	0.4/2.5/0.1	0.1/3.0/0.0	0.3/10.4/0.0	0.0/0.0/0.0	0.1/3.7/0.0	0.0/2.2/0.0	0.0/0.8/0.0	1.1/9.2/0.5	0.4/6.0/0.1	97.7/62.2/99.3

Table 6. Confusion Matrix for HackRF $N_d = 8$ at $E_b/N_O = 20\,dB$. The table formated as CB-DNA/RF-DNA/COR-DNA (%)

Classified Devices (%)

Input Device (%) CB/RF/COR	HackRF01	HackRF02	HackRF03	HackRF04	HackRF05	HackRF06	HackRF07	HackRF08
HackRF01	90.3/11.7/30.9	0.0/15.2/3.8	0.0/10.0/5.9	9.2/11.1/17.2	0.1/13.8/16.2	0.0/14.3/7.8	0.0/13.0/17.5	0.4/11.0/0.6
HackRF02	0.0/12.1/4.2	99.8/17.8/28.1	0.1/10.8/22.8	0.1/9.3/8.0	0.0/10.9/10.0	0.0/15.8/19.5	0.0/14.3/7.3	0.0/9.0/0.1
HackRF03	0.0/12.8/6.5	0.4/16.0/24.0	95.4/9.5/20.0	1.0/10.6/10.1	0.9/12.1/11.3	2.1/16.2/18.1	0.1/11.8/9.8	0.1/11.0/0.4
HackRF04	8.3/12.8/19.6	0.0/16.2/9.5	2.0/10.4/9.5	87.0/11.0/16.9	0.2/13.1/13.9	0.0/14.6/11.9	0.2/11.5/18.1	2.2/10.2/0.7
HackRF05	0.0/13.2/17.0	0.0/14.8/9.2	0.8/10.8/10.6	0.1/10.2/14.3	96.0/13.9/25.1	0.0/14.5/11.4	0.0/12.0/11.6	3.1/10.5/0.9
HackRF06	0.0/13.0/9.1	0.0/15.9/18.8	1.8/9.0/15.8	0.0/9.8/11.6	0.0/11.2/13.7	97.4/17.8/18.4	0.8/13.2/12.4	0.0/10.2/0.3
HackRF07	0.0/13.0/20.1	0.0/16.7/7.4	0.2/9.5/8.1	0.1/9.8/17.0	0.0/11.9/15.6	1.2/16.4/11.9	98.5/13.9/19.4	0.0/8.8/0.4
HackRF08	0.1/14.0/21.6	0.1/15.4/6.4	0.1/10.1/6.2	1.4/10.5/15.4	3.6/12.8/22.2	0.0/14.0/10.4	0.0/10.6/16.0	94.7/12.5/1.6

4.3 Inter-Class Classification with Only 1 SDR

The objective of this test was to quantify differences in fingerprinting techniques when there are several same class devices and only one different class device. CB-DNA, RF-DNA, and COR-DNA fingerprinting classification performance was independently measured using $N_d = 10$ RZ USBstick and $N_d = 1$ HackRF One. The classification results in Figure 26 indicate that MDA/ML was able to reach $\%C = 100\%$ for the HackRF One for all fingerprints , however, for CB-DNA it reached $\%C = 100\%$ at $E_b/N_0 = 0\,dB$. Table 7 also shows very minimal cross class confusion, where both CB-DNA and COR-DNA have 0% confusion of the HackRF One with the RZ USBstick and RF-DNA has a maximum of 0.2% confusion with devices A0F6104E and A0F69FFF at $E_b/N_0 = 20\,dB$.

Table 7. Confusion Matrix for RZ USBstick $N_d = 10$ and HackRF $N_d = 1$ at E_b/N_0= 20 dB

Classified Devices (%)

Input Device (%) CB/RF/COR	HackRF08	A0F69FE0	A0F69FE7	A0014370	A0015D34	A0F61068	A0F6104E	A0F69FFF	A0F6A00C	A0F6A004	A0F69FEA
HackRF08	100.0/100.0/99.5	0.0/0.0/0.1	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.2	0.0/0.0/0.2	0.0/0.0/0.0	0.0/0.0/0.1	0.0/0.0/0.0
A0F69FE0	0.0/0.1/0.0	91.5/50.3/90.4	0.4/4.3/0.8	0.4/10.5/0.6	0.1/10.2/0.0	2.1/8.0/4.0	2.6/3.8/1.1	2.5/6.0/2.7	0.1/3.0/0.1	0.0/0.1/0.0	0.2/3.8/0.2
A0F69FE7	0.0/0.0/0.0	1.9/7.0/3.3	94.2/60.7/94.7	0.5/1.0/0.0	0.1/1.9/0.0	0.8/0.9/0.7	0.9/13.0/0.7	1.1/2.9/0.7	0.4/5.2/0.1	0.1/5.3/0.0	0.0/2.1/0.0
A0014370	0.0/0.1/0.0	0.7/11.4/0.5	0.7/0.4/0.1	93.4/55.1/97.9	0.0/3.5/0.0	1.6/12.0/0.4	0.3/0.3/0.1	0.4/3.2/1.1	2.5/4.5/0.0	0.1/0.2/0.0	0.3/9.2/0.0
A0015D34	0.0/0.2/0.0	0.0/9.2/0.0	0.1/2.1/0.0	0.0/8.8/0.0	98.9/52.1/99.8	0.4/5.3/0.2	0.3/15.7/0.0	0.4/6.1/0.1	0.0/0.2/0.0	0.0/0.0/0.0	0.0/0.1/0.0
A0F61068	0.0/0.0/0.0	1.8/9.8/4.2	1.1/1.2/0.2	1.0/27.1/0.4	0.8/4.1/0.3	89.3/32.0/90.1	0.9/4.4/0.9	3.9/2.9/3.4	1.2/9.3/0.5	0.0/1.8/0.0	0.1/7.3/0.0
A0F6104E	0.0/0.1/0.0	2.5/5.3/2.0	0.4/13.2/1.1	0.1/0.1/0.1	0.4/9.6/0.1	1.3/1.7/0.4	86.5/61.1/89.8	8.8/5.8/6.3	0.0/1.2/0.1	0.0/0.4/0.0	0.1/1.4/0.0
A0F69FFF	0.0/0.5/0.0	1.5/16.0/1.5	2.8/4.9/1.9	0.5/14.8/0.8	0.4/14.3/0.0	4.6/5.7/3.7	13.5/25.6/9.2	76.6/14.0/83.0	0.1/1.4/0.1	0.0/0.2/0.0	0.1/2.8/0.0
A0F6A00C	0.0/0.0/0.0	0.2/2.5/0.1	0.4/5.5/0.1	3.5/5.0/0.1	0.0/0.4/0.0	1.1/7.0/0.1	0.1/1.4/0.0	0.1/0.4/0.1	92.2/54.6/98.6	0.8/10.5/0.6	1.7/12.8/0.5
A0F6A004	0.0/0.0/0.0	0.0/0.1/0.0	0.0/7.5/0.0	0.1/0.9/0.0	0.0/0.0/0.0	0.0/1.1/0.0	0.0/0.1/0.0	0.0/0.1/0.0	0.1/9.2/0.4	99.8/74.4/99.4	0.0/6.6/0.1
A0F69FEA	0.0/0.0/0.0	0.2/2.8/0.1	0.1/2.6/0.0	0.4/9.2/0.0	0.0/0.1/0.0	0.1/3.4/0.0	0.0/2.7/0.0	0.0/0.9/0.0	1.4/9.2/0.5	0.4/6.1/0.1	97.6/63.0/99.2

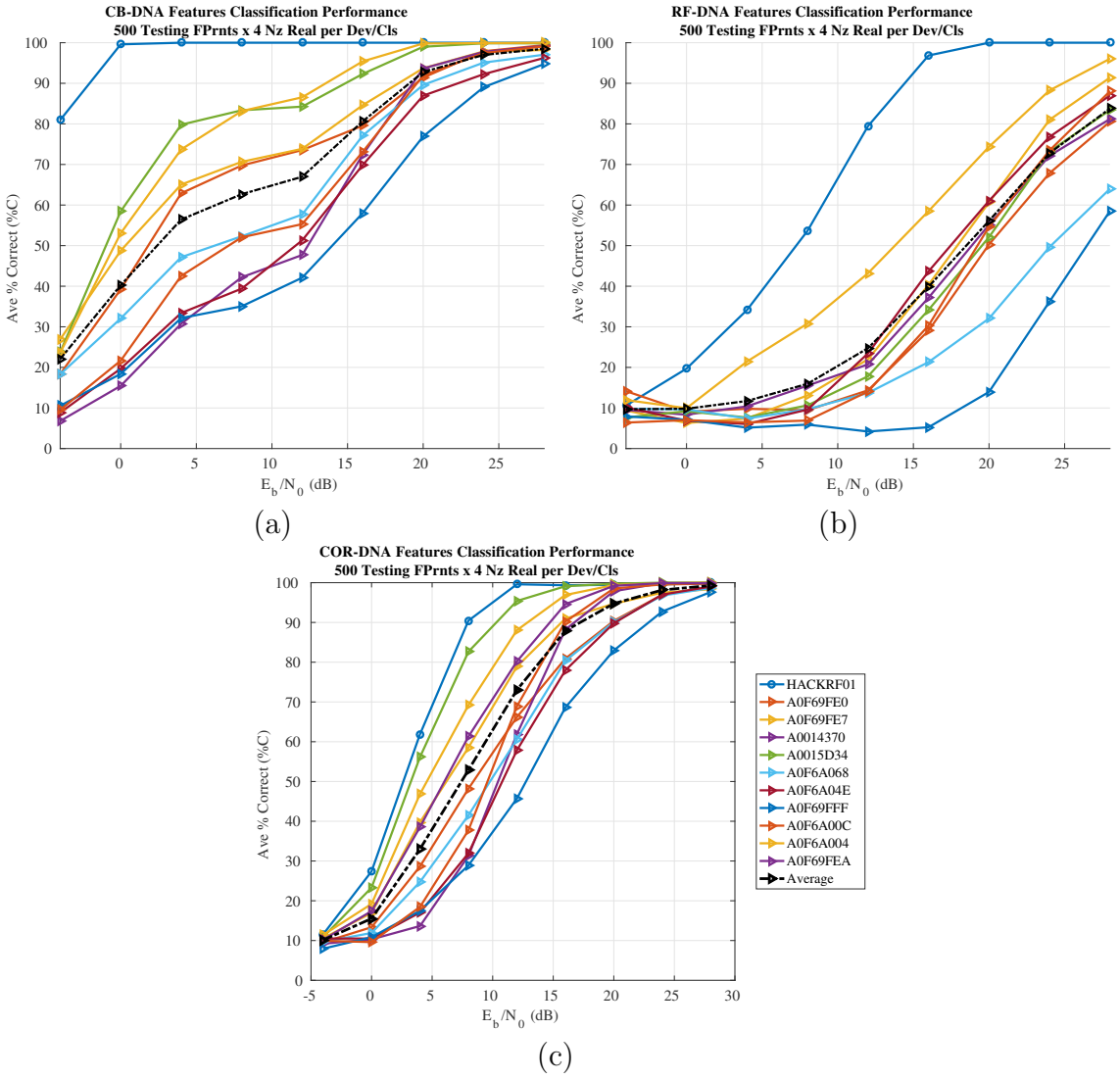


Figure 26. Intra-Class MDA/ML Classification performance for $N_d = 10$RZ USBstick and $N_d = 1$ HackRF One using:(a) CB-DNA, (b) RF-DNA, and (c) COR-DNA.

4.4 Multiple Inter-Class Classification

This test objective was to examine classification results for many devices for both classes. It was conducted with all fingerprints for $N_d = 10$ RZ USBstick and $N_d = 8$ HackRF One combined. Each type of fingerprint was independently tested and the results are in Figure 27 and Tables 8, 9.

The comparison of the different results in Figure 27 shows that only CB-DNA fingerprints achieved a mean $\%C \geq 80\%$. The multiple inter-class mean $\%C$ differed with RF-DNA and COR-DNA compared to the intra-class results but the individual devices' $\%C$ performed similarly. Also for those two cases, a class separation can be seen for RF-DNA at $E_b/N_0 \geq 24\,dB$ and for COR-DNA at $E_b/N_0 \geq 8\,dB$. The maximum class separation (Δ%C), defined as the difference of the minimum $\%C$ for one class and the maximum $\%C$ for the other class, was $\Delta\%\text{C} \approx 27\%$ at $E_b/N_0 = 28\,dB$ and $\Delta\%\text{C} \approx 55\%$ at $E_b/N_0 = 24\,dB$ for RF-DNA and COR-DNA, respectively.

The separations in classes, Figure 27 (b) and (c), could be attributed to minimal cross-class confusion in the classifier. To effectively determine any cross-class confusion, two confusion matrices, Tables 8 and 9 were constructed for $E_b/N_0 = 20$ and $0\,dB$. At $E_b/N_0 = 20\,dB$ there is negligible cross-class confusion for all fingerprints, however, for $E_b/N_0 = 0\,dB$ the maximum cross-class confusion was $[0.1\%, 9.8\%, 7.1\%]$.

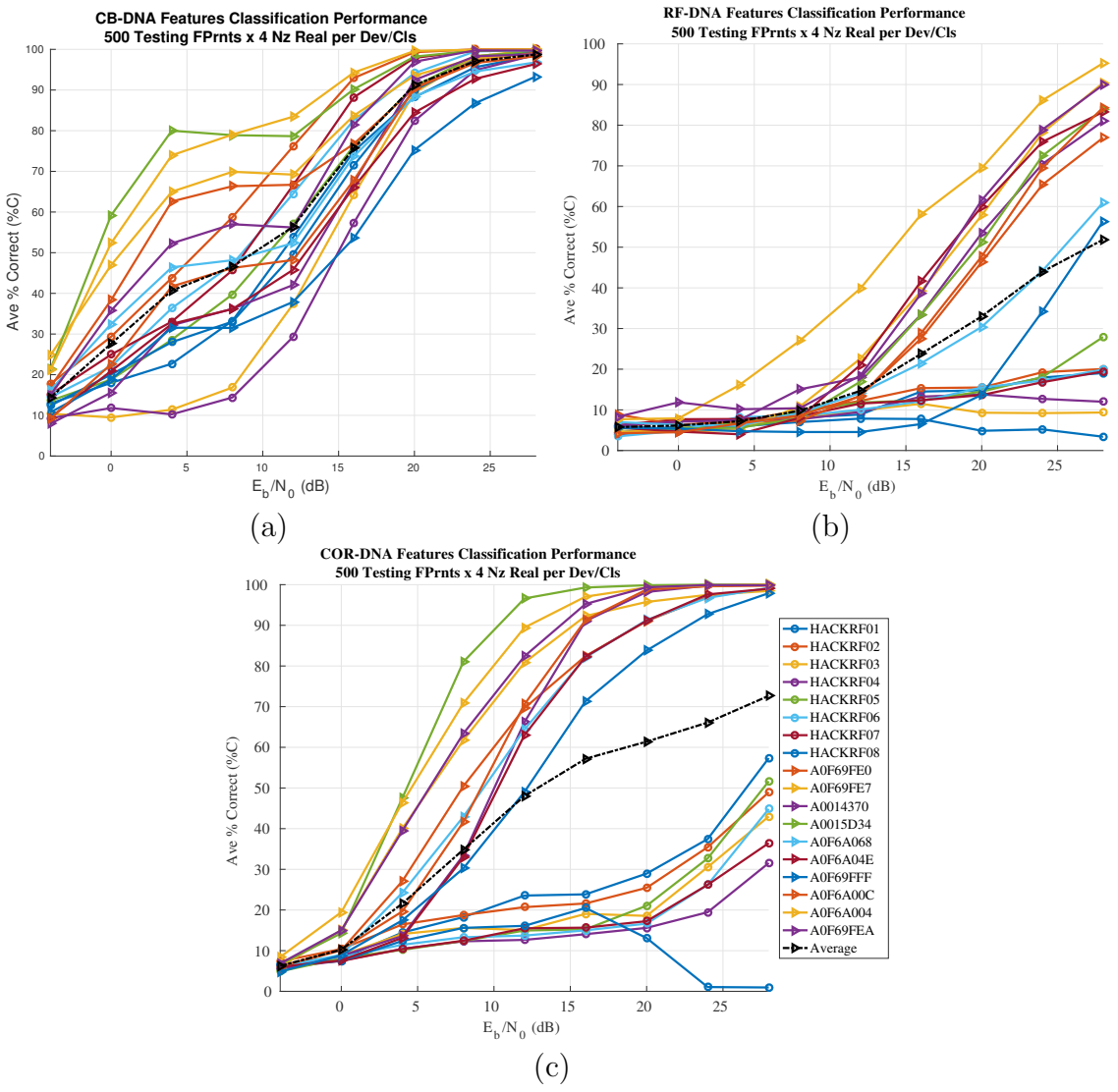


Figure 27. Intra-Class MDA/ML Classification performance for $N_d = 10$RZ USBstick and $N_d = 8$ HackRF One using:(a) CB-DNA, (b) RF-DNA, and (c) COR-DNA

Table 8. Confusion Matrix for RZ USBstick $N_d = 10$ and HackRF $N_d = 8$ at E_b/N_0= 20 dB. *Yellow*: Cross-Class Confusion

Classified Devices (%)

Input Device (%)	HackRF01	HackRF02	HackRF03	HackRF04	HackRF05	HackRF06	HackRF07	HackRF08	A0F69FE0	A0F69FE7	A0014370	A0015D34	A0F61068	A0F6104E	AOF69FFF	A0F6A00C	A0F6A004	A0F69FEA
HackRF01	88.0/14.8/28.9	0.0/16.0/3.5	0.0/10.1/6.3	11.5/12.7/14.4	0.1/13.3/13.7	0.0/14.6/6.8	0.1/13.9/16.3	0.4/4.6/10.1	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0
HackRF02	0.0/14.5/4.3	99.4/15.5/25.4	0.4/10.3/21.0	0.1/12.9/8.2	0.0/13.8/10.4	0.0/14.8/18.2	0.0/14.1/7.8	0.1/4.0/4.5	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.1/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0
HackRF03	0.0/16.2/6.2	1.5/14.8/23.2	89.1/9.3/18.6	2.2/13.6/9.8	2.5/13.2/10.7	4.2/14.5/15.8	0.1/14.1/9.6	0.5/4.2/6.2	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.1/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0
HackRF04	9.6/14.7/16.9	0.1/15.8/9.3	2.6/10.8/8.6	82.7/13.8/15.6	0.7/14.8/13.3	0.1/12.7/10.3	0.6/12.8/16.9	3.8/4.5/9.1	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.1/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0
HackRF05	0.1/17.9/15.2	0.0/14.5/8.8	2.9/10.0/10.0	0.4/12.2/12.3	91.1/14.5/21.1	0.1/15.2/11.1	0.0/12.0/11.3	5.3/3.6/10.3	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.1/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0
HackRF06	0.0/16.1/9.2	0.0/15.7/18.8	4.2/9.3/14.5	0.1/11.6/11.2	0.1/13.9/12.8	94.3/15.5/16.7	1.2/13.4/10.8	0.0/4.6/6.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0
HackRF07	0.1/16.9/18.3	0.0/15.6/7.5	0.4/10.0/8.2	0.4/12.1/16.2	0.0/12.6/14.3	1.2/15.0/8.9	98.0/13.7/17.2	0.0/4.2/9.2	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0
HackRF08	0.4/15.6/21.0	0.1/15.2/5.1	0.4/8.7/5.8	3.2/12.5/13.4	5.9/16.0/17.7	0.0/14.1/8.3	0.0/12.2/15.0	90.0/4.9/13.1	0.0/0.0/0.1	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.8/0.0	0.0/0.0/0.0	0.0/0.0/0.2	0.0/0.1/0.1	0.0/0.0/0.0	0.0/0.0/0.1	0.0/0.0/0.0
A0F69FE0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	90.5/46.4/91.0	0.7/5.2/1.1	0.4/10.8/0.6	0.1/11.2/0.0	2.7/7.1/4.2	2.7/4.5/0.6	2.5/6.8/2.2	0.2/3.2/0.1	0.1/0.2/0.0	0.3/4.6/0.1
A0F69FE7	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	2.0/7.4/2.9	93.4/57.9/95.8	0.8/1.0/0.0	0.0/2.2/0.0	0.8/0.9/0.5	1.0/14.1/0.4	1.6/3.2/0.4	0.4/5.2/0.0	0.1/5.5/0.0	0.0/2.5/0.0
A0014370	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.6/10.0/0.2	1.2/0.5/0.1	92.5/53.4/98.2	0.1/5.3/0.0	1.6/12.0/0.4	0.4/0.2/0.0	0.6/3.6/0.9	2.7/4.2/0.0	0.2/0.8/0.0	0.2/10.0/0.1
A0015D34	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.4/0.0	0.1/8.8/0.0	0.1/2.1/0.0	0.0/9.2/0.0	98.0/51.2/99.9	0.5/5.1/0.1	0.7/15.6/0.1	0.7/7.0/0.0	0.0/0.4/0.0	0.0/0.0/0.0	0.0/0.2/0.0
A0F61068	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	2.3/10.0/3.5	1.1/1.5/0.1	0.9/26.8/0.2	0.9/4.7/0.2	87.8/30.4/91.3	1.4/3.9/1.0	4.0/3.3/3.2	1.7/9.3/0.4	0.0/2.5/0.0	0.1/7.8/0.0
A0F6104E	0.0/0.1/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.1/0.0	2.9/5.2/2.1	0.5/13.2/1.1	0.4/0.1/0.1	0.8/10.4/0.1	1.4/1.4/0.3	85.0/60.0/91.1	9.0/5.9/5.2	0.1/1.5/0.0	0.0/0.4/0.0	0.0/1.5/0.0
AOF69FFF	0.0/0.0/0.0	0.0/0.1/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.1/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.4/0.0	1.2/14.6/1.1	3.1/5.2/2.0	0.4/15.1/0.6	0.4/15.8/0.0	5.0/5.5/2.4	14.4/24.7/10.0	75.0/13.7/83.8	0.3/1.4/0.1	0.0/0.5/0.0	0.1/3.0/0.0
A0F6A00C	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.1/3.0/0.1	0.5/5.5/0.0	4.5/5.7/0.0	0.0/0.6/0.0	1.4/9.3/0.1	0.1/1.5/0.0	0.1/0.5/0.1	90.3/47.8/98.8	0.9/11.6/0.6	1.9/14.6/0.4
A0F6A004	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.1/0.0	0.0/9.7/0.0	0.1/1.1/0.0	0.0/0.0/0.0	0.0/1.5/0.0	0.0/0.5/0.0	0.0/0.1/0.0	0.4/9.2/0.5	99.6/69.5/99.3	0.0/8.4/0.1
A0F69FEA	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.0/0.0/0.0	0.4/3.4/0.1	0.1/2.6/0.1	0.5/10.1/0.0	0.0/0.1/0.0	0.1/4.0/0.0	0.0/3.5/0.0	0.1/1.0/0.0	1.7/7.8/0.4	0.4/5.9/0.1	96.8/61.6/99.4

Table 9. Confusion Matrix for RZ USBstick $N_d = 10$ and HackRF $N_d = 8$ at $E_b/N_0 = 0\,dB$. *Yellow*: Cross-Class Confusion

Classified Devices (%)

Input Device (%) CB/RF/COR	HackRF01	HackRF02	HackRF03	HackRF04	HackRF05	HackRF06	HackRF07	HackRF08	A0F69FE0	A0F69FE7	A0014370	A0015D34	A0F61068	A0F6104E	AOF69FFF	A0F6A00C	A0F6A004	A0F69FEA
HackRF01	18.4/5.9/8.1	10.0/6.7/7.4	7.0/4.5/7.3	13.8/4.2/7.5	12.2/5.0/7.1	9.2/5.0/6.9	14.1/7.8/7.4	15.0/6.2/8.5	0.0/5.9/4.1	0.1/4.8/3.7	0.0/6.0/4.0	0.2/4.2/6.8	0.0/5.5/4.0	0.0/4.8/4.2	0.0/5.1/4.2	0.0/4.4/3.6	0.0/6.4/2.5	0.0/7.8/2.8
HackRF02	8.2/6.1/6.2	28.1/7.3/10.4	9.8/5.2/9.8	8.3/4.0/9.6	10.6/6.6/8.4	10.8/4.9/9.6	10.1/8.0/7.8	13.8/6.3/6.5	0.1/4.5/3.7	0.0/4.5/3.2	0.1/5.2/2.4	0.1/4.5/6.0	0.0/5.1/3.5	0.1/4.5/3.2	0.0/5.0/2.6	0.0/3.5/2.5	0.0/5.9/2.2	0.1/9.0/2.1
HackRF03	11.3/6.2/6.8	16.6/5.9/11.1	9.2/5.6/8.8	9.5/4.0/8.0	13.2/5.1/8.3	15.6/5.7/9.4	14.1/6.9/8.6	10.4/5.3/7.3	0.1/5.9/3.3	0.0/6.0/2.9	0.0/5.5/2.4	0.0/4.9/5.5	0.0/5.7/4.0	0.1/4.4/3.5	0.0/4.9/3.0	0.0/2.8/2.5	0.1/6.2/2.1	0.0/9.0/2.4
HackRF04	15.3/6.7/6.5	14.0/5.0/8.2	9.4/5.7/8.0	11.6/4.8/7.5	11.7/6.0/7.0	10.9/5.9/8.8	12.5/7.6/8.3	14.4/6.1/8.5	0.1/4.5/3.9	0.0/4.6/4.3	0.0/5.4/4.1	0.0/4.5/6.5	0.0/5.7/3.7	0.1/4.4/3.4	0.0/4.8/3.6	0.0/3.9/2.6	0.0/5.8/2.6	0.1/8.6/2.4
HackRF05	11.6/5.4/8.6	11.6/6.0/8.9	9.1/4.9/7.4	7.5/5.2/8.8	19.6/5.4/8.2	13.3/5.7/8.7	10.0/8.7/8.1	17.2/6.2/7.7	0.0/5.1/3.5	0.1/4.7/3.6	0.0/6.7/2.8	0.1/4.9/6.3	0.0/5.0/3.5	0.0/4.3/2.8	0.0/4.2/3.9	0.1/3.4/2.9	0.0/6.3/2.1	0.0/8.1/2.1
HackRF06	9.7/6.8/6.7	12.5/4.5/10.1	10.6/6.1/8.9	6.5/4.3/8.7	12.6/5.5/7.1	23.2/4.9/8.5	16.3/8.1/7.7	8.5/6.3/7.1	0.1/5.3/4.2	0.1/4.9/2.7	0.0/5.6/3.6	0.0/4.5/5.9	0.0/5.1/4.0	0.0/4.5/4.0	0.1/4.5/3.3	0.0/3.6/2.9	0.0/5.7/1.8	0.0/9.8/2.9
HackRF07	12.7/6.2/7.2	12.0/5.9/10.1	9.7/5.3/7.3	9.2/4.7/6.8	9.1/6.4/9.1	16.4/5.0/7.4	23.4/7.7/7.4	7.3/6.3/8.2	0.1/5.5/3.5	0.1/5.2/3.0	0.1/3.9/3.5	0.1/4.9/6.9	0.1/5.3/3.7	0.0/5.1/4.5	0.0/4.2/4.0	0.0/3.8/2.8	0.0/6.1/2.4	0.0/8.2/2.2
HackRF08	14.6/6.5/8.3	14.8/5.5/7.9	7.7/5.7/7.1	11.4/4.2/7.7	15.6/5.9/7.0	8.2/6.2/6.7	7.0/8.2/8.3	20.5/5.2/7.4	0.0/5.2/4.5	0.0/5.1/3.4	0.0/5.1/3.1	0.1/3.9/7.1	0.0/5.4/4.3	0.0/5.2/4.3	0.1/4.3/4.2	0.1/3.7/2.9	0.0/5.1/2.4	0.0/9.6/3.3
A0F69FE0	0.0/4.3/3.9	0.0/4.9/3.7	0.0/5.5/3.9	0.0/4.2/3.4	0.0/5.5/5.0	0.0/4.8/3.5	0.0/7.0/3.5	0.0/5.2/4.9	38.4/6.3/10.1	3.1/4.3/5.1	8.0/6.8/7.5	9.8/4.5/5.5	11.7/4.3/7.6	5.0/5.1/5.1	5.0/5.1/6.3	4.8/4.3/7.1	8.6/7.4/6.9	5.8/10.5/7.0
A0F69FE7	0.0/5.8/3.4	0.0/5.0/3.0	0.0/4.5/2.5	0.0/2.4/2.4	0.0/4.8/3.5	0.0/4.0/3.2	0.1/7.7/2.6	0.1/5.9/3.2	5.5/4.9/5.5	47.9/4.5/15.0	4.5/7.0/8.1	3.4/4.7/3.6	2.9/5.3/3.5	6.8/5.5/7.0	10.5/5.0/8.2	4.3/4.6/7.3	4.5/7.5/7.8	9.5/11.1/10.1
A0014370	0.0/5.1/3.9	0.0/3.9/2.7	0.0/4.1/2.8	0.1/4.4/3.5	0.0/4.2/3.2	0.0/4.5/3.2	0.0/6.0/3.3	0.1/4.3/4.2	12.1/6.7/7.0	8.2/5.1/8.3	15.8/7.1/8.7	9.0/4.4/5.2	8.1/5.8/5.5	7.4/4.6/6.6	9.7/4.9/7.3	11.3/5.0/8.6	7.1/8.2/8.1	11.2/11.8/8.0
A0015D34	0.0/5.1/5.8	0.0/5.7/4.2	0.0/4.9/4.7	0.0/3.6/5.9	0.0/5.0/5.2	0.0/4.7/4.1	0.0/5.9/6.4	0.1/4.2/7.1	7.3/6.3/5.2	3.4/4.2/4.7	4.8/5.8/4.2	58.0/5.3/14.3	7.0/6.3/5.7	7.6/5.3/5.0	6.4/5.1/4.8	3.6/4.1/4.7	0.9/8.0/5.4	0.9/10.6/2.5
A0F61068	0.0/5.1/4.2	0.0/4.7/3.2	0.0/4.3/2.8	0.0/4.9/3.2	0.0/4.7/4.1	0.0/4.8/3.5	0.0/5.5/3.2	0.0/4.5/3.6	11.5/6.6/7.4	2.5/5.2/4.2	6.3/6.9/7.0	9.2/4.5/6.8	31.8/6.3/8.9	9.5/5.0/6.6	5.1/4.7/6.2	9.2/4.3/7.8	7.8/7.0/10.1	7.3/10.9/7.0
A0F6104E	0.0/6.0/4.2	0.1/5.4/4.5	0.0/5.0/3.7	0.1/3.6/3.9	0.0/4.7/5.2	0.0/5.1/3.2	0.0/6.0/3.5	0.0/4.5/5.0	7.6/5.5/6.0	7.9/5.1/8.2	8.2/6.2/6.4	13.8/5.3/6.0	11.5/5.3/6.6	19.6/4.7/7.6	14.8/6.1/6.6	4.7/3.8/5.9	1.8/7.3/6.4	10.0/10.3/7.0
AOF69FFF	0.0/4.5/4.2	0.0/4.5/3.5	0.0/4.9/3.9	0.0/4.0/3.6	0.0/5.3/4.0	0.1/5.3/3.8	0.1/5.9/3.5	0.1/4.9/4.4	5.7/6.5/5.7	14.8/4.7/9.8	8.2/6.6/6.8	10.6/4.4/4.5	12.0/6.5/5.9	16.0/4.7/7.6	18.2/5.4/8.9	4.2/4.5/6.6	1.5/7.0/5.5	8.7/10.4/7.8
A0F6A00C	0.0/5.1/2.9	0.0/4.5/1.9	0.0/4.6/2.7	0.0/4.0/2.1	0.1/4.5/1.8	0.0/4.7/2.3	0.0/7.2/2.8	0.0/5.1/2.8	7.4/5.0/8.3	5.1/4.2/7.4	10.0/6.2/8.2	6.3/4.1/5.5	11.1/6.0/7.3	4.3/3.2/5.5	2.8/5.2/6.6	21.6/4.5/10.2	17.5/8.6/12.0	13.9/13.2/9.5
A0F6A004	0.0/5.3/1.5	0.1/4.9/1.6	0.0/4.7/2.5	0.0/3.3/1.4	0.0/4.6/1.7	0.0/3.9/2.1	0.0/6.1/1.9	0.0/4.1/2.1	7.4/5.5/7.8	3.4/5.3/6.6	2.8/6.6/7.1	1.8/4.9/5.4	7.9/6.5/7.4	1.2/5.1/5.3	0.6/5.1/4.3	12.8/4.2/10.0	51.6/7.9/19.4	10.3/12.2/12.2
A0F69FEA	0.0/4.5/2.4	0.0/5.3/1.8	0.0/4.4/1.7	0.0/4.0/1.4	0.0/4.2/1.8	0.0/3.7/2.1	0.0/6.1/1.5	0.0/4.0/1.4	5.0/5.3/7.0	8.8/5.5/9.8	7.1/6.7/8.5	1.9/4.4/2.6	7.5/6.0/7.3	5.1/4.9/7.3	4.9/5.5/6.6	11.3/5.6/9.2	13.2/8.2/12.4	35.1/11.8/15.0

4.5 Comparison of All Tests' Mean % Correct

This section does not present any new information but provides an easy comparison of all the previous tests' results. Figure 28, is a side-by-side depiction of the mean $\%C$ for the previous four tests. It shows that CB-DNA reaches a mean $\%C \geq 95\%$ in all tests. At mean $\%C > 50\%$, CB-DNA has an average E_b/N_0 gain of 7 dB over COR-DNA and an average gain of 18 db where RF-DNA has a mean $\%C \geq 50\%$. The results of the these tests showed that CB-DNA had the highest mean $\%C$ for all E_b/N_0 except for two cases where COR-DNA was marginally higher for $E_b/N_0 \geq 11\,dB$, Figure 28 (a),(c).

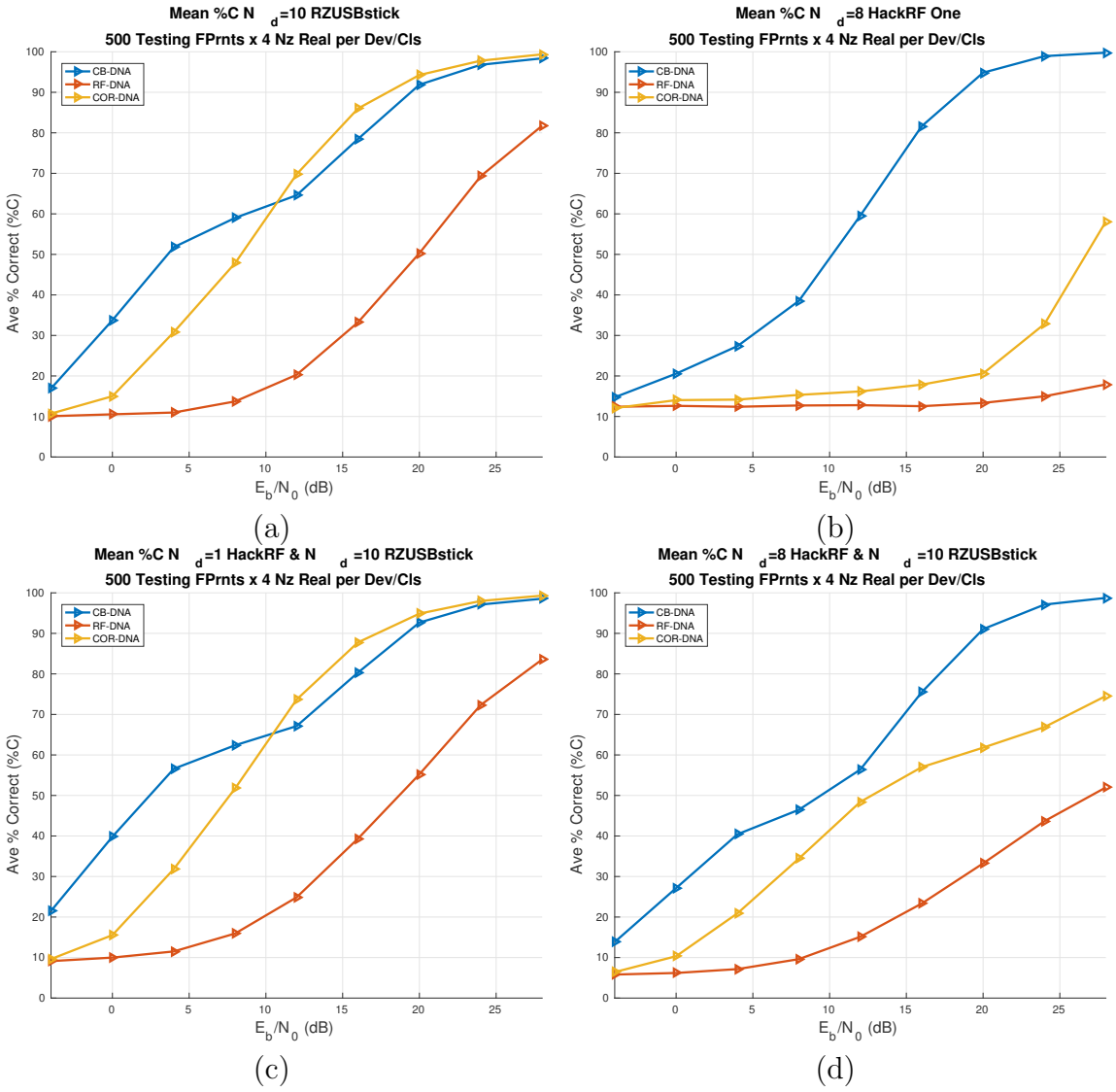


Figure 28. Mean % Correct for CB-DNA, RF-DNA, and COR-DNA for: (a) $N_d = 10$ RZ USBstick, (b) $N_d = 8$ HackRF One, (c) $N_d = 10$ RZ USBstick and $N_d = 1$ HackRF One, and (d) $N_d = 10$ RZ USBstick and $N_d = 8$ HackRF One.

4.6 Combining Fingerprints

The intent of this test was to determine if combining fingerprinting techniques would lead to an increase in the mean $\%C$. This test was only conducted on the maximum number of available devices from both classes, as was done for section 4.4.

The results of the test in Figure 29 show that any combination with RF-DNA resulted in a mean $\%C$ improvement of only $1-3\%$ verses CB-DNA and COR-DNA alone.

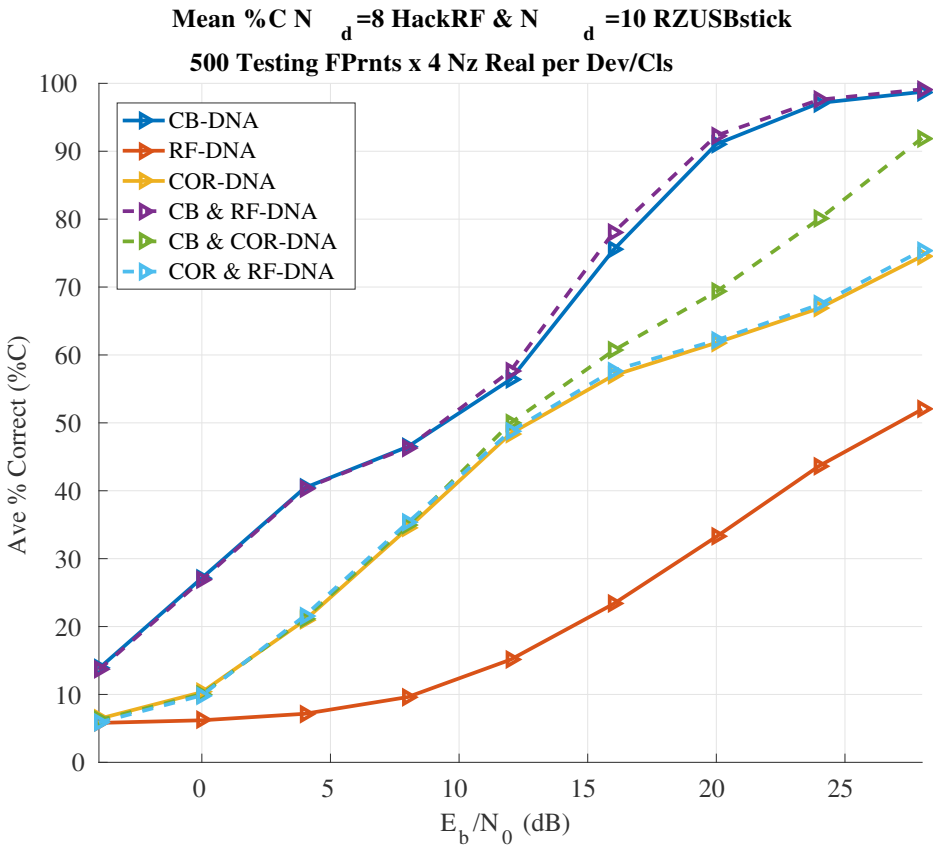


Figure 29. Mean % Correct for CB-DNA, RF-DNA, and COR-DNA along with combined fingerprints of CB&RF-DNA, CB&COR-DNA, and COR&RF-DNA for $N_d = 10$ RZ USBstick and $N_d = 8$ HackRF One.

4.7 Qualitative Dimensional Reduction Analysis

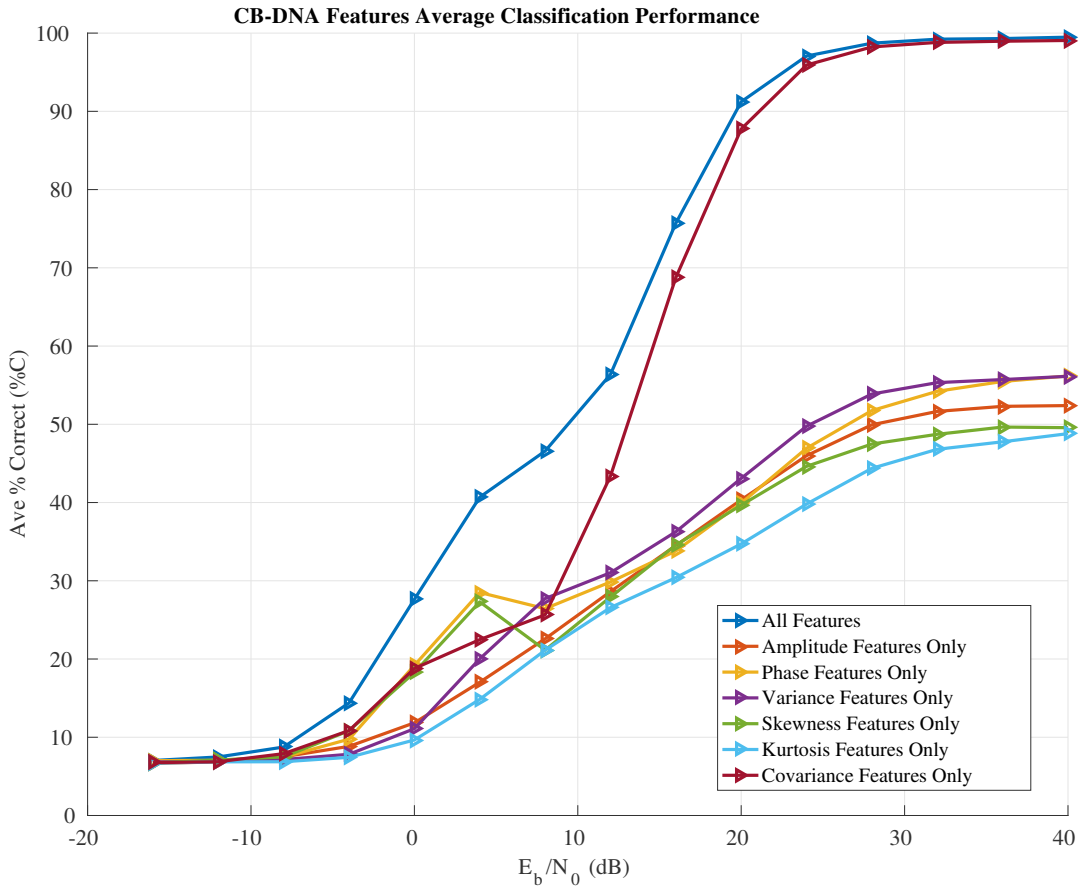


Figure 30. Dimensional Reduction Analysis Mean % Correct for CB-DNA for $N_d = 10$ RZ USBstick and $N_d = 8$ HackRF One.

The intent of this test was to do a Dimensional Reduction Analysis (DRA) for CB-DNA. This fingerprinting technique was chosen due to the fact that the results from the other tests show that CB-DNA generally had the highest mean $\%C$. DRA was applied for $N_d = 10$ RZ USBstick and $N_d = 8$ HackRF One. Full dimensional CB-DNA had $N_{feats} = 270$ features. DRA reduced N_{feats} to the following: $N_{feats} = 90$ features for amplitude, phase, and covariance; $N_{feats} = 60$ features for variance, skewness and kurtosis.

DRA test show that the performance of covariance features was most similar to the full-dimensional results, especially for $E_b/N_0 \geq 12\,dB$. All the other reduced

dimensional features $\%C$ values stayed within a $10\%C$ range. It is noted that the covariance only results differ do not follow the same general shape as the other reduced dimension results. It is also noted that the $N_{feats} = 90$ subset of covariance features are not found in any of the other reduced dimensional features.

V. Conclusion

5.1 Research Summary

The applications of wireless communication networks continue to grow as does the demand for more autonomous sensor networks. ZigBee, a Low-Rate Wireless Personal Area Networks (LR-WPAN) framework, is often used due to its low-cost, low-power, and versatility in assuming many different topologies[4]. Many current security efforts for protecting ZigBee networks are based bit-level measures such as knowing a network key. These securities are at risk with readily available and inexpensive open source tools that are designed to capture and replay ZigBee signals that mimic authorized network devices. Previous research efforts have studied the effects of Physical-Layer (PHY) based security in order to supplement already in place security measures in ZigBee devices. The purpose of this research was to compare differences in fingerprinting methods to determine which method was more effective at generating distinguishable fingerprints for ZigBee devices.

Three techniques were provided in this research as methods to create a device profile based on statistical measurements of uniquely generated distributions of data from the intentional RF emissions. The first method was Constellation Based-Distinct Native Attributes (CB-DNA) where fingerprinting was conducted in the Quadrature Phase Shift Keying (QPSK) symbol constellation plane. The second method was Radio Frequency-Distinct Native Attributes (RF-DNA) whose fingerprints are generated from the RF wave's Time Domain (TD) features. Lastly, Correlation Based-Distinct Native Attributes (COR-DNA) fingerprints were derived from a 16-ary Quasi-Orthogonal Receiver. The techniques were tested independently as well as in different combinations. Fingerprinting was for each individual device for both device classes consisting of 10 RZ USBstick(s), a ZigBee device manufactured by At-

mel, and 8 HackRF One, a Software-Defined Radio (SDR) programmed to mimic a ZigBee device.

The analysis of the fingerprinting techniques was done with the outputs of the Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classifier. Any difference in the output was quantified in terms of Average % Correct Classification ($\%C$) and by confusion rates. These were the metrics by which the fingerprints were compared.

5.2 Research Findings

The performance of the classifier was a function of signal to noise power ratio, presented as energy per bit to noise power spectral density ratio (E_b/N_0). The tests were done with different device class configurations to simulate different real world scenarios.

5.2.1 Intra-Class Test.

The RZ USBsticks classification results showed that at $E_b/N_0 = 10\,dB$ CB-DNA provided a $\%C$ improvement ($\Delta\%C$) over RF-DNA and COR-DNA of $\Delta\%C = 45\%, 4\%$, respectively. The maximum $\%C$ ($\%C_{max}$), where $E_b/N_0 = 28\,dB$, was $\%C_{max} = [98.4\%, 81.8\%, 99.4\%]$ for CB-DNA, RF-DNA, and COR-DNA, respectively.

The difference in results was much more pronounced with the HackRF One devices. CB-DNA $\Delta\%C = 37\%, 35\%$, at $E_b/N_0 = 10\,dB$, and $\%C_{max} = [99.8\%, 17.9\%, 58.1\%]$

5.2.2 Inter-Class Test: 1 SDR.

CB-DNA was also had the best results in a multi-class test. When one SDR was included with all RZ USBsticks, the CB-DNA $\Delta\%C = 45\%, 3\%$, at $E_b/N_0 = 10\,dB$, and $\%C_{max} = [98.6\%, 83.6\%, 99.3\%]$.

5.2.3 Inter-Class Test: All Devices.

CB-DNA was also had the best results when all devices were tested. The CB-DNA $\Delta\%C = 40\%, 10\%$, at $E_b/N_0 = 10\,dB$, and $\%C_{max} = [98.8\%, 52.0\%, 74.6\%]$. CB-DNA also had the lowest maximum cross-class confusion rate of 0.1% at $E_b/N_0 = 0\,dB$

5.2.4 Combined DNA.

A single test was done with three DNA combinations, CB&RF-DNA, CB&COR-DNA, and COR&RF-DNA. It was discovered that combining RF-DNA with either of the other two fingerprints added no significant increase in mean $\%C$.

5.2.5 Qualitative Dimensional Reduction Analysis.

The last test was a Dimensional Reduction Analysis (DRA) on CB-DNA. It was discovered that a reduction from a full-dimensional fingerprint of $N_{feats} = 270$ features to $N_{feats} = 90$ covariance only features still provides a mean $\%C \geq 95\%$ for $E_b/N_0 \geq 24\,dB$.

5.3 Research Contributions

This study supports the use of CB-DNA over other fingerprinting techniques under the conditions described herein. ZigBee is a low-power, LR-WPAN platform and is not likely to operate at $E_b/N_0 > 15\,dB$. CB-DNA consistently had the highest $\%C$ for $E_b/N_0 < 15\,dB$. CB-DNA had the lowest cross-class confusion percentages also even at a low $E_b/N_0 = 0\,dB$.

COR-DNA is a new fingerprinting technique, based on the lack of supportive documentation in the literature review. It did have a higher mean $\%C$ than CB-DNA for $E_b/N_0 \geq 15\,dB$ in two tests. However, it is computationally expensive for full dimensional sized fingerprints of $N_{feats} = 2,304$ features.

5.4 Future Research

This research demonstrated that CB-DNA fingerprints provide better classification results using MDA/ML than RF-DNA under the constraints presented by the testing bed. The results apply only to the scope that has been describe, but the do support future research in the following, but not limited to, areas:

1. Increase scope to include different classifiers: There were different classification techniques presented in previous research efforts, such as, Generalized Relevance Learning Vector Quantized Improved (GRLVQI)[11, 24] which have been shown to have advantages over MDA/ML in some cases.

2. Compare fingerprinting techniques by including MDA/ML verification: Classification provides a means to measuring how much an unknown signal compares to a known fingerprint. Verification answers the question that if a rogue device claims to be an authorized device what is the true positive rate vs false positive rate? This measurement is more meaningful when detecting rogue devices.

3. Repeat previous research with CB-DNA where only RF-DNA was utilized: The literature review provided more documentation for RF-DNA research efforts than for CB-DNA. The results discovered in this research support that CB-DNA could be a better PHY based security measurement.

Bibliography

1. T. J. Carbino, M. A. Temple, and J. Lopez, "Conditional Constellation Based-Distinct Native Attribute (CB-DNA) fingerprinting for network device authentication," in *IEEE International Conference on Communications (ICC)*, 2016.

2. R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern classification, 2nd edition*, Wiley-Interscience, 2000.

3. "IEEE Standard for Low-Rate Wireless Networks," *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, April 2016.

4. D. Liu and H. Yu, "An efficient improvement approach for topology formation in zigbee network," in *World Congress on Information and Communication Technologies*, Oct 2012, pp. 1081–1085.

5. Q. He, Q0 Qi, Y. Zhao, W. Huang, and Q. Huang, "The application of chaotic encryption in industrial control based on zigbee wireless network," in *2nd International Symposium on Systems and Control in Aerospace and Astronautics*, Dec 2008, pp. 1–5.

6. A. Mendez-Villalon, S. Greedy, and D. W. P. Thomas, "Robustness study of ZigBee networks in an EM environment for railway signaling systems," in *IEEE International Conference on Intelligent Rail Transportation (ICIRT)*, 2016.

7. G. V. Vivek and M. P. Sunil, "Enabling IOT services using WIFI - ZigBee gateway for a home automation system," in *Proceedings of IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, 2016.

8. A. B. Batiller, E. F. I. Bugayong, A. A. Caisip, N. P. Coligado, C. A. C. Padilla, and M. A. A. Pedrasa, "Prepaid metering system for isolated microgrids," in *IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia)*, Nov 2016, pp. 529–534.

9. C.Swedberg, "Air force hospital eliminates equipment loss, reduces labor hours," *RFID Journal*, May 2011.

10. M. Lukacs, P. Collins, and M. Temple, "Device identification using active noise interrogation and RF-DNA "fingerprinting" for non-destructive amplifier acceptance testing," in *IEEE 17th Annual Wireless and Microwave Technology Conference (WAMICON)*, April 2016, pp. 1–6.

11. D. R. Reising, M. A. Temple, and M. E. Oxley, "Gabor-based rf-dna fingerprinting for classifying 802.16e wimax mobile subscribers," in *International Conference on Computing, Networking and Communications (ICNC)*, Jan 2012, pp. 7–13.

12. W. Lowder, "Real-Time RF-DNA Fingerprinting of ZigBee Devices Using a Software-Defined Radio with FPGA Processing," M.S. thesis, Air Force Institute of Technology, Wright-Patterson AFB, OH, Mar. 2015.

13. B. W. Ramsey, B. E. Mullins, M. A. Temple, and M. R. Grimaila, "Wireless intrusion detection and device fingerprinting through preamble manipulation," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 585–596, Sept 2015.

14. A. Rerkratn and A. Kaewpoonsuk, "ZigBee based wireless temperature monitoring system for shrimp farm," in *15th International Conference on Control, Automation and Systems (ICCAS)*, 2015.

15. I. E. Berliandhy, A. Rizal, S. Hadiyoso, and R. Febyarto, "A multiuser vital sign monitoring system using zigbee wireless sensor network," in *International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, Sept 2016, pp. 136–140.

16. O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, "Three practical attacks against zigbee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned," in *14th International Conference on Hybrid Intelligent Systems*, Dec 2014, pp. 199–206.

17. B. Stelte and G. D. Rodosek, "Thwarting attacks on zigbee - removal of the killerbee stinger," in *Proceedings of the 9th International Conference on Network and Service Management (CNSM)*, Oct 2013, pp. 219–226.

18. B. W. Ramsey, B. E. Mullins, W. M. Lowder, and R. M. Speers, "Sharpening the stinger: Tuning killerbee for critical infrastructure warwalking," in *IEEE Military Communications Conference*, Oct 2014, pp. 104–109.

19. J. Wright, "Killerbee: Practical zigbee exploitation framework," in *ToorCon*, October 2011.

20. Great Scott Gadgets, "HackRF One," `http://greatscottgadgets.com/hackrf/`, Accessed: 2017-02-02.

21. B. Sklar, *Digital Communications, 2nd ed.*, Prentice-Hall, Inc., Upper Saddle River, NJ, 2001.

22. Q. Ren, S. Shi, D. Li, and X. Gu, "Demodulation of Low SNR QPSK Signal Based on Chaotic Synchronization," in *Sixth International Conference on Instrumentation Measurement, Computer, Communication and Control (IMCCC)*, July 2016, pp. 609–613.

23. T. J. Carbino, M. A. Temple, and T. J. Bihl, "Ethernet card discrimination using unintentional cable emissions and constellation-based fingerprinting," in *International Conference on Computing, Networking and Communications (ICNC)*, Feb 2015, pp. 369–373.

24. M. Lukacs, P. Collins, and M. Temple, "Classification performance using rf-dna fingerprinting of ultra-wideband noise waveforms," *Electronics Letters*, vol. 51, no. 10, pp. 787–789, 2015.

25. D. R. Reising and M. A. Temple, "WiMAX mobile subscriber verification using Gabor-based RF-DNA fingerprints," in *IEEE International Conference on Communications (ICC)*, June 2012, pp. 1005–1010.

26. S. Miller and D. Childers, *Probability and Random Processes, 2nd ed.*, Academic Press, Waltham, MA, 2012.

27. C. Campopiano and B. Glazer, "A coherent digital amplitude and phase modulation scheme," *IRE Transactions on Communications Systems*, vol. 10, no. 1, pp. 90–95, March 1962.

28. A. Betances, K. M. Hopkinson, and M. D. Silvius, "Detection of Primary User Emulation Attacks Using Constellation-Based Distinct Native Attribute Techniques," *AFIT Technical Report*, 2016.

29. T. Mravec, P. Vestenick, and M. Hrubo, "Application of correlation receiver on the rfid marker localization signals," in *ELEKTRO*, May 2016, pp. 440–444.

30. H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving zigbee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Transactions on Reliability*, vol. 64, no. 1, pp. 221–233, March 2015.

31. S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume II Detection Theory*, Prentice-Hall, Inc., Upper Saddle River, NJ, 1998.

32. Ramsey Electronics, "STE 4400," `http://ramseytest.com/product.php?pid=17`, Accessed: 2017-02-02.

33. A. Oppenheim and R. Schafer, *Discrete-Time Signal Processing, 3rd ed.*, Pearson Education, Inc., Upper Saddle River, NJ, 2010.

34. F. Gustafsson, "Determining the initial states in forward-backward filtering," *IEEE Transactions on Signal Processing*, vol. 44, no. 4, pp. 988–992, Apr 1996.

35. G. Hu, S. Wu, X. Hu, M. Jing, and Y. Gao, "Blind Frequency and Symbol Rate Estimation for MSK Signal under Low Signal-to-Noise Ratio ," *Journal of Computational Information Systems*, vol. 9, pp. 16–6651, 2013.

36. F. J. Harris and M. Rice, "Multirate digital filters for symbol timing synchronization in software defined radios," *IEEE Journal on Selected Areas in Communications*, 2001.

37. M. L. Lipschutz S., Lipson, *Linear Algebra, 4th ed.*, McGraw Hill, Inc., New York City, NY, 2009.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
23–03–2017	Master's Thesis	Sept 2015 — March 2017

4. TITLE AND SUBTITLE

Comparative Analysis of RF Emission Based Fingerprinting Techniques for ZigBee Device Classification

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Cameron W. Coon, Captain, USAF

5d. PROJECT NUMBER

16G178

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-MS-17-M-017

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

Air Force Research Lab Information Directorate (RI)
525 Brooks Road
Rome Lab AFB NY 13441
DSN 587-4478
Email: michael.gudaitis@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RITE

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

LR-WPAN are increasingly being fielded to complete tasks in autonomous sensor networks, industrial control systems, and other critical infrastructure. ZigBee is a versatile LR-WPAN platform that also open to risks of sophisticated bit-level attacks. PHY based security measures have been shown in previous research efforts as effective supplemental security measures that a not susceptible to bit-level attacks. This research effort intends to quantify the differences in various RF fingerprinting techniques via comparative analysis of MDA/ML classification results. The findings herein demonstrate a methodology for the generation of CB-DNA, RF-DNA, and COR-DNA fingerprints. The results show that CB-DNA generated fingerprints had the highest mean correct classification rates followed by COR-DNA and then RF-DNA in most test cases and especially in low E_b/N_0 ranges, where ZigBee is designed to operate.

15. SUBJECT TERMS

CB-DNA, RF-DNA, COR-DNA, Physical Layer, Device Classification, ZigBee, O-QPSK

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. Kenneth M. Hopkinson
U	U	U	U	89	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636 x4579