EXPLOITATION OF UNINTENTIONAL ETHERNET CABLE EMISSIONS USING CONSTELLATION BASED-DISTINCT NATIVE ATTRIBUTE (CB-DNA) FINGERPRINTS TO ENHANCE NETWORK SECURITY

DISSERTATION

Timothy J. Carbino, Capt, USAF

AFIT-ENG-DS-15-S-008

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-DS-15-S-008

EXPLOITATION OF UNINTENTIONAL ETHERNET CABLE EMISSIONS USING CONSTELLATION BASED-DISTINCT NATIVE ATTRIBUTE (CB-DNA) FINGERPRINTS TO ENHANCE NETWORK SECURITY

DISSERTATION

Presented to the Faculty

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 Doctor of Philosphy

Timothy J. Carbino, B.S.Cp.E., M.S.E.E.

Capt, USAF

17 September 2015

AFIT-ENG-DS-15-S-008

EXPLOITATION OF UNINTENTIONAL ETHERNET CABLE EMISSIONS USING CONSTELLATION BASED-DISTINCT NATIVE ATTRIBUTE (CB-DNA) FINGERPRINTS TO ENHANCE NETWORK SECURITY

DISSERTATION

Timothy J. Carbino, B.S.Cp.E., M.S.E.E.
Capt, USAF

Committee Membership:

Michael A. Temple, PhD
Chairman

Barry E. Mullins, PhD
Member

Mark E. Oxley, PhD
Member

Adedji B. Badiru, PhD
Dean, Graduate School of Engineering and Management

Abstract

Unauthorized access to communication networks remains at the forefront of security concerns for Information Technology (IT) based systems. These concerns are increasing within the Industrial Control Systems (ICS) community as ICS architectures migrate away from legacy IT implementations to modern Internet Protocol (IP) connections. More specifically, the connections that carry critical communications to/from control devices within an ICS are in need of improved security measures to enhance authentication reliability for remote devices and users. Research in Physical Layer (PHY) security mechanisms for wired network devices has been largely ignored and is considered here as a way to augment bit-level security protocols.

This research compared performance of two Distinct Native Attribute (DNA) fingerprinting methods for discriminating device hardware. The first technique was adopted from prior work and is called Radio Frequency-Distinct Native Attribute (RF-DNA) Fingerprinting. RF-DNA Fingerprinting has been widely used for wireless device discrimination and was adopted here to enable comparison with the newly developed Constellation Based-Distinct Native Attribute (CB-DNA) Fingerprinting technique. At its core, the CB-DNA implementation leverages unique PHY attributes to extract device dependent features to enable both *Device Classification* as a 1 vs. M "Looks Most Like?" assessment, and *Device ID Verification* as a "Looks How Much Like?" assessment for authenticating bit-level credentials. A Side-Channel Analysis (SCA) technique was used to collect communication bursts from Ethernet cable emissions for use with both fingerprinting techniques. The RF-DNA technique uses only the preamble response from the communication burst to generate device fingerprints. The CB-DNA technique uses the entire burst response and a non-conventional

signal constellation developed to support the research. The independent and dependent symbol projection regions within the non-conventional constellation are used to generate statistical fingerprint features. The real benefit of CB-DNA lies within the dependent constellation regions, the statistical variation of which vastly improves serial-number discrimination over the RF-DNA technique.

The Cross-Model Discrimination (CMD) results for RF-DNA and CB-DNA *Device Classification* using identical collected bursts show that both methods can easily discriminate devices from four different device manufacturers, with an arbitrary benchmark of percent correct classification ($\%C$) greater than 90% achieved for both methods. Like-Model Discrimination (LMD) discrimination, historically has presented the greatest discrimination challenge, and is performed using 16 total devices, four each from four manufacturers. CB-DNA LMD Fingerprinting benefits considerably with the introduction of subcluster DNA features. Improvement across the range of Signal-to-Noise Ratio (SNR) considered includes an approximate: 1) 5% to 22% increase in $\%C$, and 2) 5 to 19 dB of "gain," measured as the reduction in required SNR relative to what is required for aggregate features to achieve the same $\%C$. Relative to best case RF-DNA performance, CB-DNA is clearly superior and provides 1) nearly 22% of $\%C$ improvement at collected $SNR = 16$ dB, and 2) 9 dB or more "gain" for $\%C \geq 70$, where gain is the reduction in SNR relative to what is required by RF-DNA to achieve the same $\%C$. The *Device ID Verification* results for RF-DNA included an average Rogue Reject Rate (RRR) of $RRR = 85\%$ and CB-DNA achieved $RRR = 85.5\%$. A Constellation Point Accumulation (CPA) enhancement was introduced for CB-DNA, which was not implementable in RF-DNA, and increased Rogue rejection performance to $RRR = 93\%$.

Acknowledgements

I am most grateful to my research advisor, Dr. Michael Temple, for his guidance and patience. His vast knowledge on the subject helped point me in the right direction during my research journey.

To my research committee, Dr. Barry Mullins and Dr. Mark Oxley, who have been valuable mentors during my time as a Ph.D student.

To my children, whose smiles and hugs consistently provided all the motivation one could ever need.

To my astonishing wife, whose love and support kept me going through the most challenging of times. Without her constant encouragement, this research would not have been possible.

Timothy J. Carbino

Table of Contents

Page

Page

List of Figures

List of Tables

List of Acronyms

AAR Authorized Accept Rate

AFIT Air Force Institute of Technology

AUI Attachment Unit Interface

AWGN Additive White Gaussian Noise

BbB Burst-by-Burst

BER Bit Error Rate

BGD Binary Grant/Deny

BPS Bits Per Second

CB Constellation Based

CB-DNA Constellation Based-Distinct Native Attribute

CRT Cathode Ray Tube

CD0 Clocked Data Zero

CD1 Clocked Data One

CMD Cross-Model Discrimination

CPA Constellation Point Accumulation

DHT Discrete Hilbert Transform

DNA Distinct Native Attribute

DRA Dimensional Analysis Reduction

DUT Device Under Test

EER Equal Error Rate

kNN k-Nearest Neighbor

FVR False Verification Rate

FBA Fine Burst Alignment

FT Fourier Transform

GRLVQI Generalized Relevance Learning Vector Quantized-Improved

GSps Giga Samples/sec

GT Gabor Transform

ICS Industrial Control Systems

ID Identification

IP Internet Protocol

IT Information Technology

ISO International Organization for Standardization

LDA Linear Discriminant Analysis

LMD Like-Model Discrimination

MAC Media Access Control

MDA Multiple Discriminant Analysis

MDA/ML Multiple Discriminant Analysis/Maximum Likelihood

ML Maximum Likelihood

MSps Million Samples/sec

NIC Network Interface Card

OFDM Orthogonal Frequency-Division Multiplexing

OSI Open System Interconnect

PAM Phase Amplitude Modulation

PCS Process Control System

PDF Probability Density Function

PHY Physical Layer

PLC Programmable Logic Controller

PPA Projection Point Averaging

PSK Phase Shift Keying

QAM Quadrature Amplitude Modulation

QPSK Quadrature Phase Shift Keying

RAR Rogue Accept Rate

RF Radio Frequency

RF-DNA Radio Frequency-Distinct Native Attribute

RFINT Radio Frequency Intelligence

ROC Receiver Operating Characteristic

ROI Region of Interest

RRR Rogue Reject Rate

SCA Side-Channel Analysis

SCADA Supervisory Control and Data Acquisition

SD Spectral Domain

SDA Subclass Discriminant Analysis

SFD Start Frame Delimiter

SNR Signal-to-Noise Ratio

SSLP Single Slope

SVM Support Vector Machine

TD Time Domain

TWP Twisted Wire Pair

TVR True Verification Rate

EM Electromagnetic

EXPLOITATION OF UNINTENTIONAL ETHERNET CABLE EMISSIONS USING CONSTELLATION BASED-DISTINCT NATIVE ATTRIBUTE (CB-DNA) FINGERPRINTS TO ENHANCE NETWORK SECURITY

I. Introduction

The research involved investigating the exploitability of Ethernet cable emissions for the purpose of achieving reliable device hardware discrimination. The end result was successful development and demonstration of a new Constellation Based-Distinct Native Attribute (CB-DNA) Fingerprinting process. This chapter provides the operational and technical motivation behind CB-DNA development, including the operational motivation in Section 1.1 and technical motivation in Section 1.2. Section 1.3 summarizes research contributions and shows their relationship with prior related work. The organizational structure of the document is covered in Section 1.4.

1.1 Operational Motivation

Over the last 40 years computer networks have permeated our everyday lives. Information can now be shared in a matter of seconds rather than days or weeks, and almost 40 percent of the world's population is connected to the Internet [53]. Data network proliferation and interconnectivity benefits have also introduced millions of potential victims to cyber attacks by providing an avenue for hackers to reach their victims. The use of computer networks to help defend our country has expanded considerably over the last 20 years. Networks are prevalent in every mission aspect, including weapons system deployment and in performance of our daily duties. To complete its mission, our military employs seven million computing devices that are

connected by more than 15,000 data networks [9]. Many security issues today are due to a lack of emphasizing security in the early years of cyber system development. Many of these systems still exist today and fixes are being applied as issues are discovered resulting in a patchwork of fixes. This raises the question of how many vulnerabilities remain to be discovered and can we find and fix them before our adversaries do? The United States infrastructure has experienced a "17-fold increase in computer attacks" between 2009 and 2011 [52]. The Department of Homeland Security (DHS) recently stated that cyber attacks are "one of the most severe national security threats to the United States [9]."

Sun Tzu, a Chinese military general and philosopher, once said "Supreme excellence consists in breaking the enemy's resistance without fighting [69]." Cyber warfare is relatively cheap when compared to traditional warfare and it provides an attack vector for our adversary to potentially degrade our military abilities and disrupt our civilian institutions without physical conflict.

Cyber security threats remain on the top ten lists of multiple security-minded enterprises. They have been identified as:

- the #1 concern of Fortune 1,000 companies for five years in a row according to a 2014 survey [55];
- the #2 concern of the American Security Project in 2015 [30];
- the #3 concern of the United States Intelligence Office in 2012 [3].

As the U.S. modernizes its legacy Industrial Control Systems (ICS) implementations from Information Technology (IT) monitoring and control to more modern Internet Protocol (IP)-based solutions, the noted security threats are becoming a reality in the ICS arena [29]. Many ICS control devices are moving to IP-based solutions (Modbus/TCP, Ethernet/IP, and DNP3) to provide critical communications [7, 61].

A reoccurring theme for these systems is security vulnerability. Critical platforms are inadequately protected, direct access to equipment by non-essential personnel is prevalent, and open wireless and wired access ports on office walls remains a problem [46, 58]. Many ICS architectures and protocols were designed and built without considering security or verification of remote users/devices [46, 61]. As the sophistication of attacks increases, these vulnerabilities are being exploited by attackers to gain network access to hardware, operating systems, or executables [46].

In 2011, the United States Department of Defense deemed cyberspace the fifth warfare domain alongside land, sea, air, and space highlighting the importance of protecting our infrastructure and civilian enterprises. Our leaders understand now more than ever, that the landscape of cyberspace is changing. As stated by General Alexander, Commander of the United States Cyber Command, before the Senate Committee on Armed Services on 27 March 2012, "cyberspace is becoming more dangerous." There are those who believe [40,45] that the cyber environment is turning into the new intelligence gathering efforts of early 1960s and Cold War era.

Network services for Ethernet devices and connections have been standardized by the International Organization for Standardization (ISO) which introduced the Open System Interconnect (OSI) model depicted in Figure 1.1. The seven layer model divides networking communication into seven segments for protocol implementation. Network security implementation normally takes place at the "Data Link" and "Network" layers at which point devices are either granted or denied network access [28,50,62,65]. It has been shown that the security protocols in place at these layers provides an avenue for an attacker to spoof the bit-level security credentials of these layers [5, 13, 18]. The first OSI model layer is considered the Physical Layer (PHY) and has the potential to provide a vast amount of discriminating data that currently is being ignored by the higher OSI layers for network security.

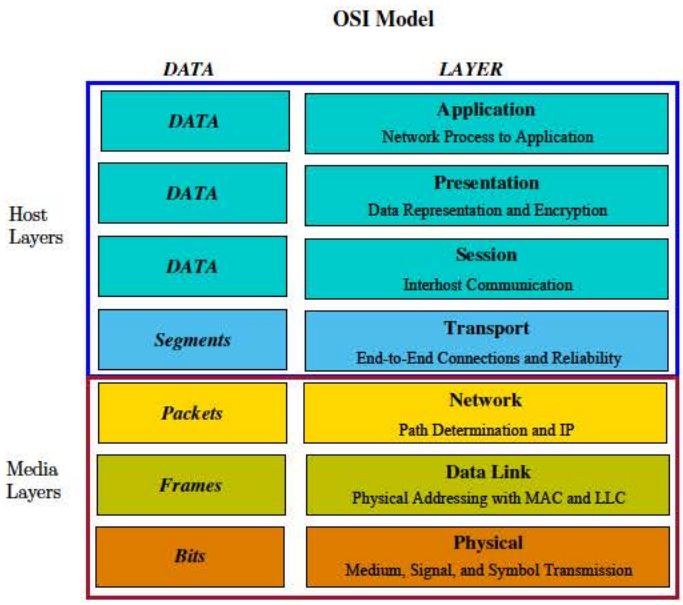


Figure 1.1. Open System Interconnect (OSI) reference model highlighting the 7 layers associated with network communications [65].

Preventing unauthorized network access is necessary to help limit the intelligence gathering efforts of our adversaries. This research investigates Ethernet cable emissions that contain PHY attributes to augment traditional network security protocols such as Media Access Control (MAC) credentials that can be easily spoofed through network monitoring [28]. The variations in the manufacturing process for network devices are enough to cause slight variations in the PHY signaling attributes of each device such that unique features can be extracted from a given signal to increase traditional security mechanisms [15, 20, 35]. The research presented takes the Ethernet emissions and utilizes the unique features present in the device signal to augment current network security protocols. The newly developed approach improves device discrimination through an increase in 1) Device Classification, 2) Device Identification (ID) Verification, and 3) the rejection of rogue devices requesting network access. Prior research in the area focused heavily on wireless device discrimination and have shown that the unique features are useful for security augmentation [20].

1.2 Technical Motivation

A side channel is a result of a system or device's implementation such that an output, whether intentional or not, leaks information relevant to specific operations or data within the system or device. The knowledge base for Side-Channel Analysis (SCA) is extensive and covers many decades of research to include intentional and unintentional byproducts [14–17, 21, 22, 24, 26, 34, 39, 41, 56, 59, 60, 64, 71, 72, 75, 77]. Some pertinent exploitable side channels include network traffic (intentional) [14, 41] and unintentional Radio Frequency (RF) emissions. The unintentional RF emission research can be divided into multiple subareas to include 1) components [15–17, 59, 60, 75], 2) peripherals [21, 22, 34, 39, 64, 71, 72], and 3) cables [22, 56].

The ability to use PHY attributes (RF fingerprinting) as a means to perform device discrimination is not new and there is extensive research in this area covering many decades. Typical utilization of PHY attributes includes generation of unique discriminating features within transient, invariant or entire burst responses [20]. Transient-based approaches [4, 68, 70] are generally avoided given the transient response 1) has limited duration, and 2) is influenced by environmental conditions that affect the communication channel and limit its usefulness [19]. The invariant approaches as in [31–33, 48–51, 73, 74] extract device dependent features from a specific *non-data modulated* Region of Interest (ROI) within the burst (preamble, midamble, etc.). The entire burst is typically used in Constellation Based (CB) approaches as in [6, 19, 20, 25, 35] to extract features from *data modulated* ROI where device dependent modulation errors exists between the ideal transmitted symbols and the received symbols.

1.2.1 Side Channel Analysis (SCA).

Most early SCA literature [34,39,56,64,71,72] focuses on far-field device emissions to recover data being leaked by the device. As a research area, SCA has a considerable knowledge base, but it was evident that there was a gap in this research area such that Ethernet cable emissions have yet to be explored as an exploitable byproduct. The focus for this research is to collect unintentional near-field emissions using a similar process and probe setup used in [15,60,75] and described in Section 3.1. This research effort will then utilize the collected emissions to 1) provide the ability to perform symbol estimation on collected emissions enabling confirmation of payload data and burst destination by an outside system, and 2) enhance traditional MAC based authentication processes through the creation of a non-conventional constellation for device feature extraction.

The details for a Single Slope (SSLP) symbol estimation process are provided in Section 3.4.1 and an expanded CB approach is covered in Section 3.4.3. The latter CB symbol estimation technique creates a non-conventional constellation from the Ethernet emissions and is what enables the development of a CB-DNA Fingerprinting process.

1.2.2 Constellation-Based (CB) Fingerprinting.

At the beginning of this research, it became clear that there was limited literature addressing wired PHY augmentation to MAC based authentication using PHY-based Distinct Native Attribute (DNA) features to form device fingerprints. The conceptualized fingerprinting approach for wired Ethernet devices utilizes new *conditional* constellation regions not present in prior related works [6, 19, 25]. It is required that symbol estimation from collected emissions generate fingerprints that are adequate for device discrimination for both Cross-Model Discrimination (CMD) defined here as

between different manufactures and Like-Model Discrimination (LMD) defined here as between different devices with the same model number and manufacturer.

Current literature in wired device discrimination only contains a correlation based approach [27, 28] which collects Ethernet burst preambles directly from the network card for comparison against a training data set. A couple of drawbacks to this approach is 1) it requires direct access to network card for collection, and 2) it requires sample rates at or greater than 1 Giga samples/sec (GSps).

The current literature in wireless device discrimination utilizes symbol estimation for traditional constellation based signals such as Quadrature Phase Shift Keying (QPSK) and Orthogonal Frequency-Division Multiplexing (OFDM). The vast majority of these techniques create features from errors between the estimated symbol and the ideal symbol location [6, 19, 25, 35]. This approach provides adequate device discrimination for wireless devices but is limited to signals that are modulated using a traditional constellation. The Ethernet protocols for PHY signaling do not utilize a traditional constellation for signal modulation which further complicates the issue, i.e., the collection process captures a transformed version of the communication burst and not an ideal modulated signal representation.

Development details for the CB-DNA process are described in Section 3.7 and builds upon Section 3.4.3 that takes a non-constellation modulated signal and projects its symbols into a non-conventional constellation space. This proved to be an effective means for implementing CB-DNA Fingerprinting and discriminating devices.

At the time of this research, a direct comparison between fingerprinting processes utilizing the same collected emissions has yet to be conducted. Therefore, the Radio Frequency-Distinct Native Attribute (RF-DNA) Fingerprinting process outlined in Section 2.3 will be accomplished in parallel with the newly developed CB-DNA Fingerprinting process on the unintentional Ethernet emissions and results compared.

The goal is to find which fingerprinting process provides the best classification performance for this type of signal.

As the methodology and implementation of device discrimination via PHY attributes increases in maturity and approaches operational transition, it may be necessary to improve fingerprinting discrimination performance. Other RF-DNA implementations have looked at discovering a more robust feature set through Dimensional Analysis Reduction (DRA) which reduces the number of features needed to perform discrimination while keeping the performance degradation to a minimum [48–50]. This technique does provide for an operational implementation that has a smaller footprint but a drawback is a potential in discrimination performance. Process enhancements such as Constellation Point Accumulation (CPA) and Projection Point Averaging (PPA) are investigated with the goal of improving overall verification performance. The enhancements have the ability to provide an increase in performance that negates the degradation from DRA.

1.3 Research Contributions

The technical areas mentioned in previous sections are summarized in Table 1.1 and provide a relational mapping between previous work in these areas and current contributions presented in this dissertation. Some previously undefined acronyms contained within the table include: Time Domain (TD), Spectral Domain (SD), Gabor Transform (GT), Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML), Generalized Relevance Learning Vector Quantized-Improved (GRLVQI), Support Vector Machine (SVM), k-Nearest Neighbor (kNN), Linear Discriminant Analysis (LDA), and Subclass Discriminant Analysis (SDA)

1.4 Document Organization

The remainder of the document is organized as follows. Chapter II provides relevant background information on topics utilized for this research to include SCA, the adopted RF-DNA Fingerprinting approach, 10BASE-T Ethernet standard, and the device discrimination process. Chapter III provides the methodology for experimental emission collection, post-collection processing, symbol estimation of wired emissions, the adopted RF-DNA implementation, development of the CB-DNA Fingerprinting technique, implementation of *Device Classification* and *Device ID Verification*, and finally some enhancements for CB-DNA and additional verification metrics. Chapter IV presents the CMD and LMD classification results, LMD device ID verification, LMD ID verification enhancements, and lastly a sensitivity analysis associated with probe orientation. Chapter V provides the research summary and conclusion, as well as a brief discussion on potential future work.

Table 1.1. Relational Mapping Between Current Research Contributions and Technical Areas of Previous Work. The X Symbol Denotes Areas Addressed.

Technical Area	Previous Work		Current Research	
	Addressed	Ref #	Addressed	Ref #
TD Features	X	[36, 37, 50, 63, 73, 74]	X	[12]
SD Features	X	[16, 17, 51, 73]		
GT Features	X	[49–51]		
CB Features	X	[6, 19, 20, 25, 35]	X	[11, 12]
Correlation	X	[27, 28]		
Emission Type				
Intentional	X	[31, 36, 37, 50, 63, 73, 74]		
Unintentional	X	[15–17, 59, 60]	X	[10–12]
Burst	X	[31, 36, 37, 50, 63, 73, 74]	X	[10–12]
Continuous	X	[15–17, 59, 60]		
Classification / Verification Process				
MDA/ML	X	[36, 37, 50, 73, 74] [15–17, 31, 51]	X	[11, 12]
GRLVQI	X	[37, 49, 51]		
SVM	X	[6, 19, 25]		
kNN	X	[6, 19]	X	[11]
LDA/SDA	X	[35]		
Classification / Verification Devices				
Wireless Devices	X	[31, 36, 37, 50, 51, 73, 74]		
Wired Devices	X	[27, 28]	X	[10–12]
Device Operations	X	[59, 60]		
Wired Emission Symbol Estimation				
RF SSLP			X	[10, 11]
CB-Based			X	[11]
Side Channel Analysis				
Unintentional Emissions	X	[21, 22, 24, 26, 34] [39, 41, 56, 71, 72]	X	[10–12]
Process Enhancements				
DRA	X	[48–50]		
CPA	X	[6, 35]	X	
PPA			X	

II. Background

2.1 Introduction

This chapter provides background information and key concepts supporting the research methodology in Chapter III and research results presented in Chapter IV. Section 2.2 provides a brief history of Side-Channel Analysis (SCA) as used to capture and exploit unintentional Radio Frequency (RF) emissions from digital devices. The goal is to extract information that can be used to passively characterize device operation or system configuration. RF Fingerprinting is addressed in Section 2.3, to include a description of Radio Frequency-Distinct Native Attribute (RF-DNA) in Section 2.3.1 as adopted for comparison with the newly developed Constellation Based-Distinct Native Attribute (CB-DNA) presented in Section 3.7. Details for previous Constellation Based (CB) discrimination techniques that utilize intentional emission features are presented in Section 2.3.2 for completeness. Standard Ethernet 10BASE-T characteristics are covered in Section 2.4. The final sections address device *discrimination* as two distinct, equally important, related processes as depicted in Figure 2.1. First, the 1 vs. M *Device Classification* assessment process is described in Section 2.5 and a description of Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification is provided. Second, the 1 vs. 1 *Device Identification (ID) Verification* assessment is described in Section 2.6.

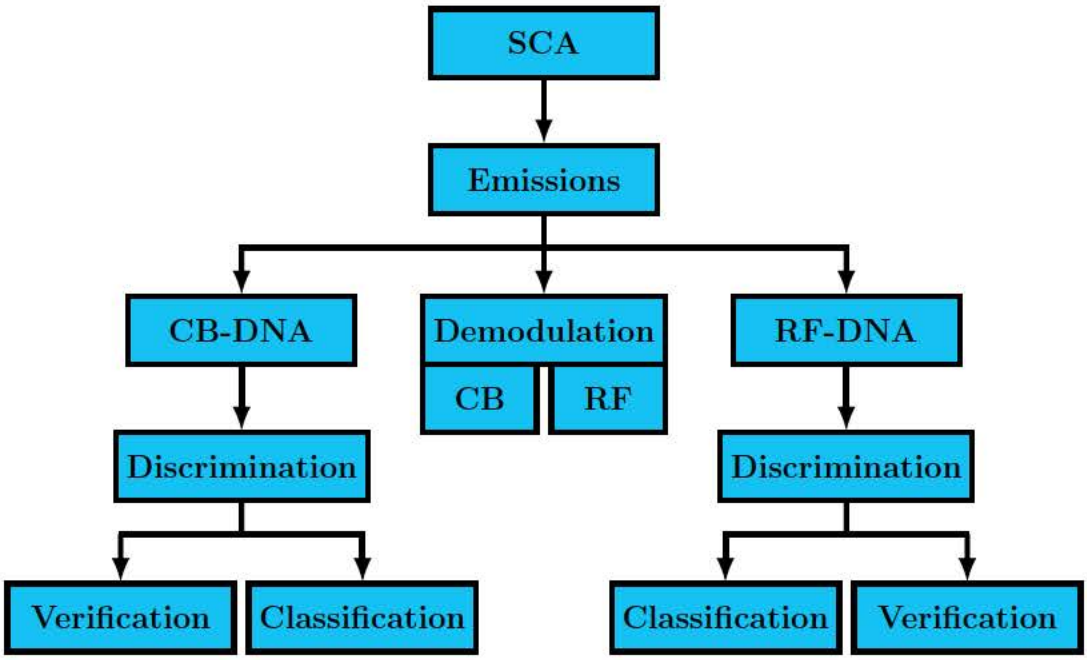


Figure 2.1. Diagram of research paths taken for CB-DNA Fingerprinting development and demonstration.

2.2 Side Channel Analysis (SCA)

It is common knowledge that digital devices leak information in the form of Electromagnetic (EM) emissions. The German army successfully carried out side-channel attacks as early as WWI on field phone lines utilizing far-field emissions [24]. Since then, side channel attacks have expanded to other electronic devices. The miniaturization of components and decreases in production costs has enabled the shrinking of entire devices and opened up a wide area of potential eavesdropping risks.

Cathode Ray Tube (CRT) monitors have been widely exploited in literature using the EM emissions resulting from video signal processing [39, 64, 71]. In 1985, it was first discovered that video displayed on a CRT could be reproduced on a TV screen when the TV receiver was tuned to the appropriate frequency [71]. The EM radiation from a CRT monitor is a direct result of the several hundred volt signal required to operate the monitor. It was discovered that the amplified CRT signal was very similar

to that of a broadcast television signal and theoretical eavesdropping distance for some displays could be as high as 1 km. Moreover, adding additional CRT monitors to the room did not mask the signals with additional noise because each monitor resonated at a separate frequency which simply enabled an attacker to view more screens. Since the original CRT exploration in 1985, several others such as [22, 39, 64] have all accomplished similar attacks each focusing on slightly different SCA aspects.

The work in [39] advanced EM emanation exploitation by disguising hidden transmissions in video display signals. In this case, the video display unit was used to transmit an audio signal that could be picked up with an AM radio. This enabled the transmission of computer data to an eavesdropping station at a rate of approximately $R_b = 50$ Bits/Sec (BPS) [39]. A second type of attack, more along the lines of [71], hid images behind those displayed on the monitor so that the eavesdropper could capture the hidden image on another monitor. A dithering technique which changes the screen pixel modulation was used to carry out these various attacks.

A method to calculate the maximum eavesdropping distance for video emanations being transferred to an Ethernet cable was subsequently developed in [22]. This earlier work determined that an experimental distance of $D_e = 29.5\ m$ was the max distance for video reconstruction. However, the paper itself appeared to have some contradicting statements, and its last few sections lacked structure and rigor.

A novel approach is considered in [21] to recover and detect the keystrokes of a PS/2 keyboard. Crosstalk and EM coupling is used to investigate the information leakage from a computer with a PS/2 keyboard. It was determined that the EM coupling of keyboard keystrokes was present in the power ground line, i.e., at the power outlet. The factors enabling signal propagation are a lack of shielding in the PS/2 cable, data encoded on sharp rise and fall edges of the clock, and frequency of the transmission. Once the data signal is on the PS/2 ground line cable it can

propagate to the ground plane through the power outlet.

The potential for EM-based eavesdropping on an RS-232 cable has been investigated using a standard radio receiver [56]. The eavesdropping was successful for multiple reasons, including: 1) use of high frequency transmissions, 2) use of large signal amplitudes, 3) no cable shielding, 4) serial data transmission, and 5) low bit transmission rates. It was shown in [56] that RS-232 cable eavesdropping can occur at distances of $D_e = 9\ m$ and $D_e = 7\ m$ between the AM radio and the unshielded and shielded cable, respectively. The only requirement for this type of attack is an AM/FM radio with a few minor modifications and a way to store the received signal. One drawback is that distances are reduced when one piece of equipment is connected to a proper ground.

The work presented herein expands on prior SCA techniques by collecting RF emissions from an Ethernet cable and performing symbol estimation to extract addressing information and payload data from individual Ethernet frames.

2.3 Radio Frequency (RF) Fingerprinting

RF Fingerprinting is a generic term used to describe techniques that utilizes RF emissions, whether intentional or unintentional, to create a digital fingerprint from unique features contained within the emissions. The generated fingerprints are then used to perform discrimination between devices or specific device states. Device hardware fingerprinting is possible due to variations in manufacturing processes and device components. These variations inherently induce Physical Layer (PHY) feature differences that vary across devices [35]. Amplifiers, capacitors, inductors and oscillators also possess slight imperfections that influence device fingerprints [6, 19, 25, 35]. The resultant variation can cause deviations in communication symbol rate, center frequency, and AM/FM/PM conversion [35]. Thus, "it is possible to exploit

device imperfections even when the intrinsic components used are supposedly identical [17, 20]" [12].

A physical layer identification survey by [20] summarizes various RF Fingerprinting approaches used to create digital fingerprints into three basic approaches 1) transient responses, 2) invariant responses *non-data modulated*, and 3) varying *data modulated* burst response regions. "Transient-based approaches are generally avoided given [19] 1) the limited duration of the transient response, and 2) the transient response being influenced by environmental conditions that affect the communication channel and limit its usefulness [12]." It is for those two reasons the research presented in this document focuses on the two approaches that utilize the invariant and varying responses to perform device fingerprinting. Section 2.3.1 provides the background details on RF-DNA approach which utilizes the invariant response region. Section 2.3.2 provides background on previous work in the area of varying (*data modulated*) burst response regions.

2.3.1 RF-DNA Fingerprinting.

This section provides an introduction to traditional RF-DNA fingerprinting and the techniques associated with it. The conventional RF-DNA implementation historically extracts the invariant (*non-data modulated*) [16, 17, 31, 32, 36, 48, 50, 51, 59, 63, 73, 74] burst responses. A few of these implementations include Time Domain (TD) [48], Spectral Domain (SD) [73], Fourier Transform (FT) [73], and Gabor Transform (GT) [51] and then generate features from various Region of Interest (ROI) (i.e., transient, amble, and preamble). Another use for RF-DNA fingerprinting is to detect normal or abnormal behavior of programmable logic components as described in [60, 75]. Here, a low sensitivity RF probe is used to collect near-field emissions from a Programmable Logic Controller (PLC) in an effort to digitally fingerprint a series of

operations that the device performs. The capability of this approach provides a way to tell whether or not a device is genuine and its original design has not been altered by additional logic gates.

Prior to this research, the majority of the previous research in RF-DNA fingerprinting has relied on *intentional* signal responses of wireless devices [36, 48, 51, 63, 73, 74] to perform device fingerprinting. However, the research presented here uses the technique introduced in [10] and explained in Section 3.1 for collecting *unintentional* RF emissions from Ethernet cables to produce RF-DNA fingerprints on a burst-by-burst basis for wired network cards. The subsequent paragraphs discuss the adopted RF-DNA approach described in [49,50]. The relevant parameters associated with fingerprint generation are covered in Section 3.6 and are used to generate the discrimination results presented in Section 4.4 and Section 4.5.

RF-DNA uses the steady-state response of the communication signal usually in the form of an "amble", and extracts native attributes to create a feature-based fingerprint [17,48–51]. This work adopts the RF-DNA fingerprinting approach utilizing the specifics of the RF-DNA procedures outlined in [17, 50, 59] for Time Domain (TD) responses and is restated here for completeness. Traditional RF-DNA TD fingerprinting starts by partitioning the ROI into subregions and finding the instantaneous amplitude, phase, and frequency responses of the individual subregions.

Individual RF-DNA fingerprints F^{RF} are generated from N_k samples extracted from a real-valued discrete signal defined as $cs(k)$. The number of individual TD feature responses $N_{resp} = 3$ and consists of amplitude $\{\bar{a}_c(k)\}$, phase $\{\bar{\phi}_c(k)\}$, and frequency $\{\bar{f}_c(k)\}$ with $k = 1, \ldots, N_k$ as provided in (2.1) - (2.3). Before the instantaneous phase (2.2) and frequency (2.3) can be calculated, the real-valued signal $cs(k)$ must first be converted into I-Q samples via the Hilbert transform [42], which results in $cs(k) = cs_Q(k) + cs_I(k)$ where

$$a(k) = \sqrt{cs^2(k)}, \tag{2.1}$$

$$\phi(k) = \tan^{-1}\left[\frac{cs_Q(k)}{cs_I(k)}\right], \tag{2.2}$$

$$f(k) = \frac{1}{(2\pi)}\left[\frac{d\phi(k)}{dk}\right]. \tag{2.3}$$

Consistent with other work [36, 50, 73] the TD features are also normalized (denoted with an over bar) and centered (denoted with a subscript c) and provided in (2.4) - (2.6) where, $k = 1, \ldots, N_k$, and the calculated means across N_k are $\mu(a)$, $\mu(\phi)$, and $\mu(f)$ for amplitude, phase, and frequency, respectively. The function denoted by $max\{\cdot\}$ is the maximum value of each sequence's centered response [50].

$$\bar{a}_c(k) = \frac{a(k) - \mu(a)}{\max\limits_k\{a_c(k)\}}, \tag{2.4}$$

$$\bar{\phi}_c(k) = \frac{\phi(k) - \mu(\phi)}{\max\limits_k\{\phi_c(k)\}}, \tag{2.5}$$

$$\bar{f}_c(k) = \frac{f(k) - \mu(f)}{\max\limits_k\{f_c(k)\}}, \tag{2.6}$$

The selected ROI containing N_k samples is divided into N_R equal subregions, such that the number of samples per subregion is an integer. Statistical features $N_{stat} = 4$ are then generated for each of the normalized and centered instantaneous responses $N_{resp} = 3$, where the statistical features include standard deviation (σ), variance (σ^2), skewness (γ), and kurtosis (κ) as depicted in Figure 2.2. It is also common practice to utilize the entire ROI as an $N_R + 1$ subregion. For each instantaneous, response a N_{R_i} regional fingerprint is created according to (2.7) and concatenated as in (2.8). Then

the individual feature vectors for a given instantaneous response are concatenated to form the final composite fingerprint F_C^{RF} as in (2.9).

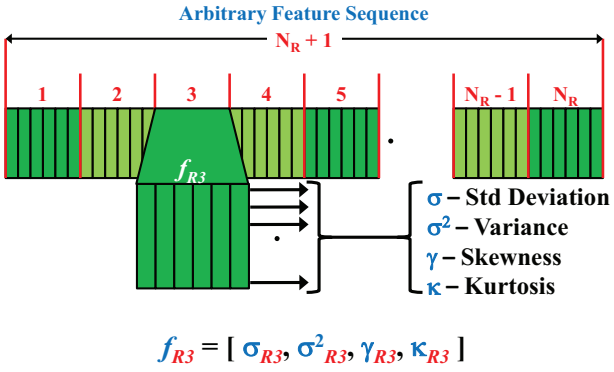


Figure 2.2. Standard RF-DNA regional fingerprint format for generating centered and normalized feature sequences [59, 73].

$$F_{R_i}^{RF} = [\sigma_{R_i}, \sigma_{R_i}^2, \gamma_{R_i}, \kappa_{R_i}]_{1\times 4} \tag{2.7}$$

$$F_{a,\phi,f}^{RF} = [F_{R_1}^{RF} : F_{R_2}^{RF} : F_{R_3}^{RF} : \cdots : F_{R_{N_R+1}}^{RF}]_{1\times[4(N_R+1)]} \tag{2.8}$$

$$F_C^{RF} = [F_a^{RF} : F_\phi^{RF} : F_f^{RF}] \tag{2.9}$$

The number of features in a RF-DNA fingerprint are dependent on the number of instantaneous responses N_{resp}, statistical features N_{stat}, and subregions N_R selected. For example $N_{resp} = 3$, $N_{stat} = 3$, $N_R = 20$ results in a statistical feature vector of length $3 \times 3 \times 20 = N_{feat} = 180$ features. The RF-DNA parameters used for this research are covered in Section 3.6.

RF-DNA was introduced for two reasons: 1) the unintentional Ethernet emissions are a new, previously uninvestigated emission type under the RFINT program, and 2) to enable direct performance comparison of prior RF-DNA and newly developed CB-DNA fingerprinting methods utilizing *identical* collected emissions.

2.3.2 Constellation-Based Fingerprinting.

This section provides background on previous CB device fingerprinting techniques. The objective of CB fingerprinting is to take the intentional RF emissions (*data modulated*) burst responses of wireless a device and extract unique features from the constellation responses to identify a device by its physical-layer attributes. CB device discrimination is also affected by slight variations in components such as amplifiers, capacitors, inductors, and oscillators used in the manufacturing devices [6,8,19,25,35]. The component variations cause deviations in symbol rate, frequency, noise, AM-AM compression and AM-PM conversion as discussed in [35]. Most of the prior work associated with using signal constellations involves extracting features from constellation errors depicted in Figure 2.3 [6, 8, 20, 25, 35].

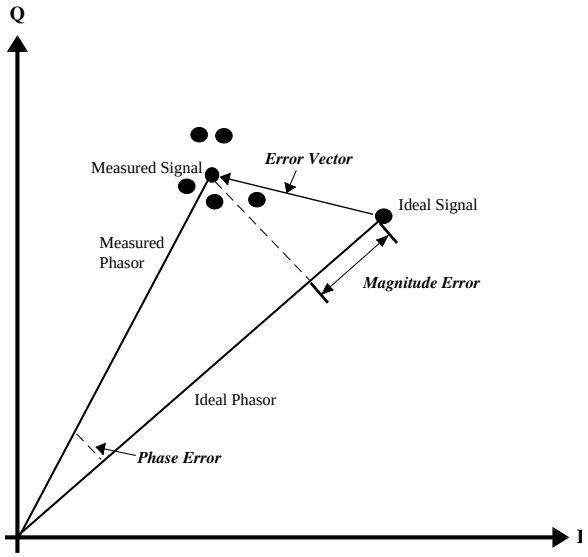


Figure 2.3. Representation of the typical errors previous constellation based fingerprinting techniques [6].

The Phase, Magnitude and Error vector presented in Figure 2.3 highlights the main components used to create features for prior work in CB device discrimination. A few other metrics were also mentioned and include SYNC correlation and I/Q offset [6, 25]. Several feature extraction methods and classifiers have been looked at

to include Linear Discriminant Analysis (LDA) and Subclass Discriminant Analysis (SDA) in [35], Brik *et al.* used a Support Vector Machine (SVM) and k-Nearest Neighbor (kNN) in [6], Maximum Likelihood (ML) and weighted voting is used in [8].

What is not evident in [6, 8, 20, 25, 35] is how the constellation statistics (mean, variance, etc.) are compiled into feature vectors. The works generally mentioned that features are generated based on symbol estimation errors for each symbol within a given communication burst. It is not clear in these prior works how all the individual errors are compiled into a single feature in the radiometric signatures created [6,8,20,25,35]. The work in [6,35] does mention that an improvement in accuracy was observed when multiple bursts were used for training. However, basic implementation details were given on training bins and the same bins did not appear to be used for testing signatures. In [35] it states that "multiple frames are averaged to improve Signal-to-Noise Ratio (SNR)" which is different than the approach described in Section 3.10.1 where features are based on accumulation of projected points. Results in [6, 35] are presented that do show some improvement in accuracy when increasing the number of bursts in a training bin but again it is somewhat unclear how the binning works.

The newly developed CB-DNA Fingerprinting method differs considerably from prior constellation-based works given it relies on symbol cluster distributions versus simple transmitted-vs-received constellation error metrics.

2.4 Ethernet Signaling Characteristics

The original IEEE Ethernet Standard was comprised of multiple individual standards, and as new techniques and transmission mediums were used, new standards would be created making it difficult to keep up with changes. Therefore in 2012, all the individual standards were placed into one Ethernet standard 802.3-2012 which was subsequently divided into clauses [1] representing individual standards.

Table 2.1 gives a brief comparison of three Ethernet signaling clauses in the IEEE 802.3-2012 standard. The Manchester encoding scheme is employed by the full-duplex 10BASE-T Ethernet that utilizes the clocks falling edge and data stream to encode the transmitted data sequences [57]. The 10BASE-T clause has a symbol duration of $T_{Sym} = 100\ ns$ and it uses serial data transmission over two Twisted Wire Pair (TWP)'s, including one pair for transmission and one pair for receiving. For a specific symbol interval, a Clocked Data Zero (CD0) symbol is defined as having a high voltage level for the first half of the symbol duration and a low voltage level for the second half. Alternately, a Clocked Data One (CD1) symbol is defined as having a low voltage level for the first half of the symbol duration and a high voltage level for the second half.

Table 2.1. Ethernet Comparison for Three Clauses [1].

Signaling Type	**10BASE-T**	100BASE-TX	100BASE-T2
Encoding	**Manchester**	Muti-Level Transmit-3 (MLT3)	Pulse-Amplitude Modulation-5 (PAM5)
Symbol Time	**100ns**	8ns	40ns
Transmission	**Serial**	Serial	Parallel
TWPs to Transmit	**One**	One	Two*
TWPs to Receive	**One**	One	Two*
Data Scrambler	**No**	Yes	Yes

* Simultaneous Transmit and Receive on Same Wire

A network card implementing the 10BASE-T sits idle when it has no data to send, and therefore, unintentional emissions of interest are only present when the device is actively transmitting data frames. The preamble is used at the beginning of each data transmission to synchronize clocks between transmitter and receiver so that the receiver can perform symbol estimation. The preamble consists of $N_{pre} = 56$ symbols that alternate between CD1 and CD0. Immediately following the preamble

is the Start Frame Delimiter (SFD) that has a specific $N_{sfd} = 8$ symbol sequence of '10101011'. The SFD's purpose is inform the receiving device that data is immediately following. An inter-frame gap $T_{ifg} = 9.6\ \mu s$ is an exploitable feature in the 10BASE-T standard as it provides a delay in the transmission of subsequent communication bursts between the end of one transmission and the beginning of the next as depicted in Figure 2.4. The implementation of the other two clauses mentioned require that the network card is always actively transmitting data symbols; however, when no requested data is being transmitted an idle symbol is sent instead. The other two clauses still use the same sequence of bits for the preamble but it is no longer used to synchronize clocks. However, the SFD is still used to indicate the start of a new frame.

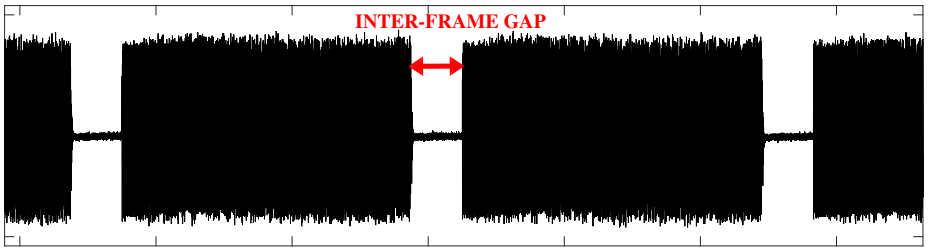


Figure 2.4. A sequence of 10BASE-T bursts highlighting the inter-frame gap between bursts [2].

Turn-on steady-state responses of 10BASE-T communication bursts and the inter-frame gap enables reliable burst detection and ROI extraction for both RF-DNA and CB-DNA Fingerprinting.

2.5 MDA/ML Device Discrimination

The specific elements of MDA/ML device classification described herein are directly adopted from [15, 50] and its use is consistent with previous RF-DNA fingerprinting works [16, 17, 48–51, 59, 73, 74]. The MDA/ML process is used to generate the classification results in Chapter IV.

Consistent with previous device discrimination work, *Device Classification* is defined for this research as a 1 vs. M assessment where an unknown device fingerprint is compared to all known devices and a decision is made as to which known device looks "most like" the unknown device. In essence, the best match is always returned to one of the known devices even if the input device has never been seen by the model. The classification approach herein can be divided into two steps 1) model development using Multiple Discriminant Analysis (MDA) an expansion of Fisher's LDA from an $N_C = 2$ class problem to an $N_C > 2$ class problem, where N_C is the number of classes [51]. The goal of MDA is to reduced the feature dimensionality from d dimensions to $N_C - 1$ dimensions while maximizing the distance between class means and minimizing the variance within a given class [23, 66], and 2) the device classifier utilizes the ML classification technique which is accomplished by comparing an unknown fingerprint against all class models and a measure of similarity is returned for each N_C. It is then said that the unknown fingerprint belongs to the class with the highest similarity measure because it looks the "most like" that class [15,50].

2.5.1 Multiple Discriminant Analysis (MDA).

The first step in MDA is to find the scatter matrices that reduces the intra-class variance ($\mathcal{S}_w$) in (2.10) and maximizes the distant between the inter-class means ($\mathcal{S}_b$) in (2.11) [66]:

$$\mathcal{S}_w = \sum_{i=1}^{C} P_i(\mu_i - \mu_0)(\mu_i - \mu_0)^T, \tag{2.10}$$

$$\mathcal{S}_b = \sum_{i=1}^{C} P_i \Sigma_i, \tag{2.11}$$

where the prior probability of class c_i is P_i and Σ_i is the covariance matrix. Probabilities and costs are assumed to be equal for all classes. A projection matrix $\mathbf{W}$ is then formed using (2.10) and (2.11) by $\mathbf{W} = {\mathcal{S}_w}^{-1}\mathcal{S}_b$ and selecting $N_C - 1$ eigenvectors.

Device fingerprints $\mathcal{F}$ are then projected into the $N_C - 1$ dimensional space via:

$$\mathcal{F}_i^{\mathbf{W}} = \mathbf{W}^{\mathbf{T}}\mathcal{F}. \tag{2.12}$$

A projected training matrix $\mathcal{F}^{\mathbf{W}}$ is created by taking a total of N_{Tng} training fingerprints from each class and projecting them with (2.12) as in:

$$\mathcal{F}^{\mathbf{W}} = \left[\mathcal{F}_1^{\mathbf{W}}, \mathcal{F}_2^{\mathbf{W}}, \ldots, \mathcal{F}_{N_{Tng}}^{\mathbf{W}}\right]^T_{N_{Tng}\times(N_C-1)}. \tag{2.13}$$

A multivariate normal distribution is fitted to the projected MDA training data for classifier development using projected class means ($\hat{\mu}_i^{\mathbf{W}}$) and covariance matrices ($\hat{\Sigma}_i^{\mathbf{W}}$). The MDA process outputs 1) projection matrix $\mathbf{W}$, 2) N_C sets of $\mathcal{F}^{\mathbf{W}}$, 3) N_C estimated mean vectors $\hat{\mu}_i^{\mathbf{W}}$, and 4) N_C covariance matrices $\hat{\Sigma}_i^{\mathbf{W}}$. These four outputs are then used for ML classification (estimation) of subsequent testing fingerprints $\hat{\mathcal{F}}$ [66] as described in Section 2.5.2.

2.5.2 Maximum Likelihood (ML) Classification.

This section uses the outputs from the previous section to perform ML classification via a similarity measure described by the Bayesian posterior probability and assuming equal prior probabilities and costs. To do this, the covariance matrices $\hat{\Sigma}_i^{\mathbf{W}}$ are first pooled according to:

$$\hat{\Sigma}_P^{\mathbf{W}} = \frac{1}{N_{Tng} - N_C}\sum_{i=1}^{N_C}\hat{\Sigma}_i^{\mathbf{W}}, \tag{2.14}$$

where N_C is the total number of devices and $\hat{\Sigma}_P^{\mathbf{W}}$ is the pooled covariance over $\hat{\Sigma}_i^{\mathbf{W}}$.

Device classification is then performed using some similarity criterion through a one-to-many comparison of a single device fingerprint with a template reference from each device modeled. A best match is found by calculating similarity score between

an unknown projected device fingerprint $\hat{\mathcal{F}}$ and each of the N_C reference models. The unknown projected device fingerprint $\hat{\mathcal{F}}$ is then assigned to class m_i according to:

$$P(m_i|\hat{\mathcal{F}}) < P(m_j|\hat{\mathcal{F}}) \forall j \neq i, \tag{2.15}$$

where $i = 1, 2, \ldots, N_C$ and $P(m_i|\hat{\mathcal{F}})$ is the conditional posterior probability that $\hat{\mathcal{F}}$ belongs to m_i. The conditional probability is then computed according to Bayes' Rule as in [23, 66]

$$P(m_i|\hat{\mathcal{F}}) = \frac{P(\hat{\mathcal{F}}|m_i)P(m_i)}{P(\hat{\mathcal{F}})}. \tag{2.16}$$

A simplification of (2.16) can occur because of the assumption of equal prior probabilities and cost ($P(m_i) = 1/N_C$) allow for the $P(m_i)$ term to be ignored. The denominator also remains constant and can likewise be ignored in (2.16) reducing to only the $P(\hat{\mathcal{F}}|m_i)$. This reduction then allows for the ML to be estimated from likelihood values of a projected fingerprint $\hat{\mathcal{F}}$ [23, 66] as in the conditional probability

$$P(\hat{\mathcal{F}}|m_i) = \frac{1}{(2\pi)^{(N_C-1)/2}\sqrt{|\hat{\Sigma}_P^{\mathbf{W}}|}}\, exp(\mathsf{F_e}), \tag{2.17}$$

where

$$\mathsf{F_e} = -\frac{1}{2}(\hat{\mathcal{F}} - \hat{\mu_i})^T(\hat{\Sigma}_P^{\mathbf{W}})^{-1}(\hat{\mathcal{F}} - \hat{\mu_i}). \tag{2.18}$$

The performance of the system is quantified by the percent correct classification $\%C$ performance metric that is based on the number correctly identified fingerprints divided by the total number of trials.

2.5.3 Cross-Validation.

A cross-validation mechanism can be used to improve MDA/ML reliability. This involves: 1) dividing the training fingerprints into K equal size disjoint blocks of

N_{Tng}/K fingerprints, 2) holding out one block and training on K-1 blocks to produce projection matrix $\mathbf{W}$ as outlined in Section 2.5.1, and 3) validating the model by using the holdout block and $\mathbf{W}$ to perform device classification according to Section 2.5.2 [23]. The $\mathbf{W}$ from the training iteration that had the highest percent correct classification $\%C$ is output and used for subsequent MDA/ML *testing* assessment. The analysis of the classification errors is accomplished with the use of a confusion matrix which will be discussed in more detail in Section 3.8.

2.6 Device ID Verification

This section provides the definition of *Device ID Verification* and explains the process for device ID verification. The specific elements of device verification described herein are adopted from [15, 50] and its use is consistent with previous RF-DNA fingerprinting works [16, 17, 49, 59]. The device ID verification process is a 1 vs. 1 comparison for assessing "how much" a fingerprint for a claimed identity looks like the reference model for that identity. The device verification assessment enables authentication of a device's claimed identity via the devices fingerprint and its claimed bit-level identity to include but not limited to Media Access Control (MAC) credentials.

For this research, there are two types of device designations that include: 1) an *authorized* device presents its own (true) credentials to request network access while its credentials are compared against a stored reference for that device, and 2) a *rogue* device presents (false) credentials matching an authorized device and attempts to gain unauthorized network access. Note that it is possible for an authorized device to turn rogue (e.g., insider threat) and present false credentials. The purpose of verification is to compare the claimed identity with that of the reference model for the true identity [15]. The resultant of this comparison is a binary decision that either grants

the device access (rightly/wrongly) or denies the device access (rightly/wrongly). The binary decision is based solely on a verification test statistic Z_V and a predetermined threshold value $t_V(d)$ as in:

$$\begin{aligned} Z_V \geq t_V(d) &\Rightarrow Accept, \\ Z_V < t_V(d) &\Rightarrow Reject, \end{aligned} \tag{2.19}$$

where $d = 1, 2, \ldots, N_C$ is the index of the reference model for the true identity.

The binary decision in (2.19) is applied to both authorized and rogue devices resulting in four possible outcomes detailed in Table 2.2 with the bold entries considered as outcome errors.

Table 2.2. Verification Outcome Decisions with Bold Entries Denoting Errors.

Input	Verification Decision (Output)	
	Authorized	Rogue
Authorized	Authorized Accept (AA)	**Authorized Reject (AR)**
Rogue	**Rogue Accept (RA)**	Rogue Reject (RR)

The two types of errors in Table 2.2 are summarized below [15, 19, 50]:

1. An *Authorized Reject* (AR) from Table 2.2 is when an *authorized* device experiences a reject outcome from (2.19).

2. A *Rogue Accept* (RA) from Table 2.2 is when a *rogue* device experiences an accept outcome from (2.19).

Results are typically presented as rates in terms of percentages such that:

1. True Verification Rate (TVR) is the total number of AA over all authorized attempts ($AA + AR$).

2. False Verification Rate (FVR) is the total number of AR over all authorized attempts ($AA + AR$) or simply ($1 - TVR$).

3. Rogue Reject Rate (RRR) is the total number of RR over all rogue attempts ($RR + RA$).

4. Rogue Accept Rate (RAR) is the total number of RA over all rogue attempts ($RR + RA$) or simply ($1 - RRR$).

The verification threshold $t_V(d)$ for device d is set using a Receiver Operating Characteristic (ROC) curve which is created by plotting the TVR against FVR while varying $t_V(d)$ as depicted in Figure 2.5. Setting the $t_V(d)$ to the same point as the Equal Error Rate (EER) point on the curve serves two purposes: 1) the classification system operates under equal errors such that $FVR = (1 - TVR)$ and RAR are equal and, 2) the EER point is a common statistic used to compare across classification systems. The lower the EER for a given system typically indicates better performance for that system [15, 50]. Depending on the security needs of the classification system the threshold value $t_V(d)$ can be increased or decreased.

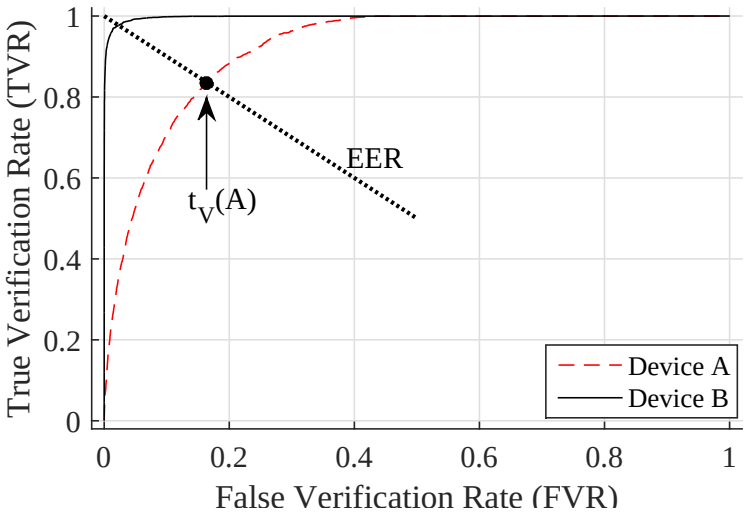


Figure 2.5. A Receiver Operating Characteristic (ROC) curve for Device A and B with diagonal dashed line representing the Equal Error Rate (EER) and highlighting the selection of the (EER) point as the verification threshold for Device A as $t_V(A)$.

The ID verification steps include: 1) developing a reference model, 2) selecting a similarity measure, 3) determining device-dependent threshold values $t_V(d)$ with, $(d = 1, 2, \ldots, N_C)$ based on desired TVR and FVR performance, 4) generating a test statistic Z_V for each unknown fingerprint from the device presenting the claimed ID and, 5) comparing Z_V with threshold $t_V(d)$ according to (2.19) and making a final accept (grant network access) or reject (deny network access) decision.

III. Methodology

This chapter provides the methodology for generating results presented in Chapter IV. The experimental setup for collecting the Electromagnetic (EM) responses of Ethernet cards using a Category 6 Ethernet cable is presented in Section 3.1. This includes details for the collection receiver, Ethernet card operation, and EM probe-cable location. Section 3.3 covers post-collection processing and defines the Region of Interest (ROI) for both Radio Frequency-Distinct Native Attribute (RF-DNA) and Constellation Based-Distinct Native Attribute (CB-DNA). The details for the symbol estimation techniques are presented in Section 3.4. Information regarding variation in the Signal-to-Noise Ratio (SNR) is covered in Section 3.5. The adopted RF-DNA methodology and parameters used for RF-DNA fingerprint generation are covered in Section 3.6. Section 3.7 provides details for the CB-DNA Fingerprinting approach developed under this research and demonstrated herein. The CB-DNA development uses the symbol projection and bit estimation using the non-conventional constellation, and generates CB-DNA fingerprints comprised of projected symbol statistics in the new constellation space.

Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) implementation is introduced for device discrimination, including the *Device Classification* process in Section 3.8 and *Device Identification (ID) Verification* process in Section 3.9. CB-DNA enhancements that demonstrate achievable device ID verification improvement are also considered and includes 1) Constellation Point Accumulation (CPA) in Section 3.10.1, and 2) MDA/ML Projection Point Averaging (PPA) in Section 3.10.2. Lastly, a section on additional verification metrics is included in Section 3.11 as a way to compare this research with other works.

3.1 Experimental Hardware Setup

The experimental hardware setup included a Dell Precision T7500 desktop computer with two Network Interface Card (NIC) slots. One slot hosted the NIC used to collect emissions of interest using a LeCroy WavePro 760Zi-A 6 GHz oscilloscope. As will be noted in Section 3.1.1, two different, like-model, different serial number oscilloscopes were used for collections. For these collections, a low-pass baseband filter with a bandwidth of $W_{BB} = 32\ MHz$ was placed in-line between the oscilloscope and a Riscure 205HS "High Sensitivity" near-field probe to capture the EM signal. The oscilloscope settings included: 1) a sample rate of $f_s = 250$ MSamp/Sec (MSPS), 2) a 1.0 volts/div vertical scale, 3) a 2.0 msec/div horizontal time scale, and 4) a trigger offset of $t_{Off} = -25.0\ ms$.

The second desktop NIC slot hosted the Ethernet Devices Under Test (DUT) in Table 3.1, i.e., the transmitting Ethernet cards to be fingerprinted. The DUTs were connected to a Dell Precision laptop via a given length (L_C) of Category 6 Ethernet cable and configured for 10BASE-T Ethernet signaling with full duplex enabled. As indicated in Table 3.1, a total of 16 Ethernet cards used for proof-of-concept demonstration, including four devices (D) from each of four different manufacturers (M). MATLAB® was used to generate transmitted DUT data, trigger the collection oscilloscope, and write/store the collected signals to disk. A communication delay between MATLAB® and the Device Under Test (DUT) necessitated the use of a negative collection trigger offset t_{Off}.

As discussed earlier in Section 2.4, 10BASE-T full duplex operation only requires two of the four available Twisted Wire Pair (TWP)s within the Ehternet cable. This includes a TWP wire for transmitting (TWP of interest for extracting fingerprints) and a different TWP for receiving communications from the connect network card. The connected network card was not actively transmitting data frames. The re-

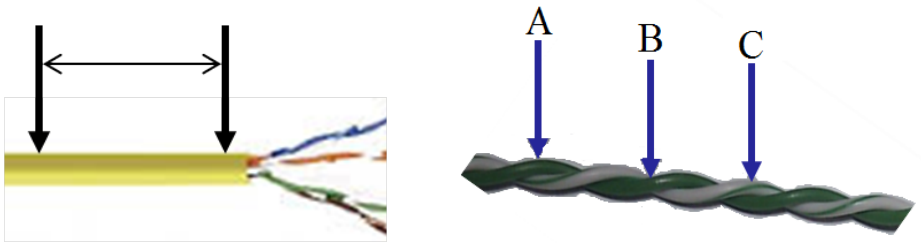
Table 3.1. Ethernet Devices Under Test (DUT) Utilizing a Manufacturer (M) Device (D) Combinations (M#:D#) as Device Reference.

D-Link		Intel		TRENDnET		StarTech	
Dev ID	MAC	Dev ID	MAC	Dev ID	MAC	Dev ID	MAC
M1:D1	D966	M2:D1	1586	M3:D1	9B55	M4:D1	32CB
M1:D2	DA06	M2:D2	1A93	M3:D2	9334	M4:D2	32B4
M1:D3	DA07	M2:D3	1A59	M3:D3	9B54	M4:D3	96F4
M1:D4	60E0	M2:D4	1A9E	M3:D4	9B56	M4:D4	3048

maining two TWPs remained inactive during DUT emission collections. Thus, the Ethernet communication "channel" was relatively benign with the only possible interference coming from network traffic on the receiving TWP wire. This environment was sufficient for proof-of-concept demonstration. Performance analysis in a less benign, more fully loaded Ethernet channel (additional TWPs active), was beyond the scope of the research and remains an area for future work.

3.1.1 Probe-Cable Orientation.

The EM collection probe could be located anywhere along the Category 6 Ethernet cable. For a selected collection point, the probe was positioned such that it was just touching the cable without inducing physical distortion (no pressure). Various emission collection points and probe-cable orientations are depicted in Figure 3.1a. Note that the probe location changes in this figure correspond to linear (along the cable) displacement. The following points also apply for radial (around the cable) displacement. As indicated in Figure 3.1a, at any given location along the cable the probe is within close proximity to one of four TWPs within the cable; since the sheath is not removed for collection, the TWP closest to the probe is unknown. Also, as depicted in Figure 3.1b there are multiple probe-wire orientations for a given TWP. Thus, the experimentally collected EM response (amplitude, phase, power, etc.) for the wire of interest changes with probe position.



(a) Ethernet Cable (b) TWP Locations

Figure 3.1. Orientation of RF probe with respect to (a) Ethernet cable Twisted Wire Pairs (TWP) (b) wires within a given TWP.

The TWP in Figure 3.1b includes the wire of interest with letters A, B, and C representing three unique probe-wire positions. When the probe is at location A the signal response is most affected by the EM field generated by the colored wire. The same is true for the response at location C but for the white wire. In an ideal environment, the response collected at locations A and C would be perfectly out-of-phase by 180°. In addition, the response at location B would be zero given it would be equidistant from both wires and the EM fields would cancel out. Thus, establishing a repeatable procedure for probe location (axial and radial orientation) was an important step for Ethernet cable emission collection.

A "good" probe location (linear and radial) was arbitrarily established as being a probe-cable orientation that produced burst responses having peak amplitudes of 2-3 volts as displayed on the collection oscilloscope. For a given length cable and collection oscilloscope combination (two combinations were used), the probe location was determined using one of the Ethernet cards and maintained for subsequent collections from all cards using a jig to keep the probe-cable orientation fixed. The two cable-oscilloscope collection configurations included: 1) an $L_C = 8\ m$ length cable with oscilloscope #1 (Config #1), and 2) an $L_C = 100\ m$ length cable with oscilloscope #2 (Config #2). Developmental and baseline performance results in Section 4.4 and Section 4.5 are based on Config #1 using a probe location of $L_P \approx 2\ m$ from

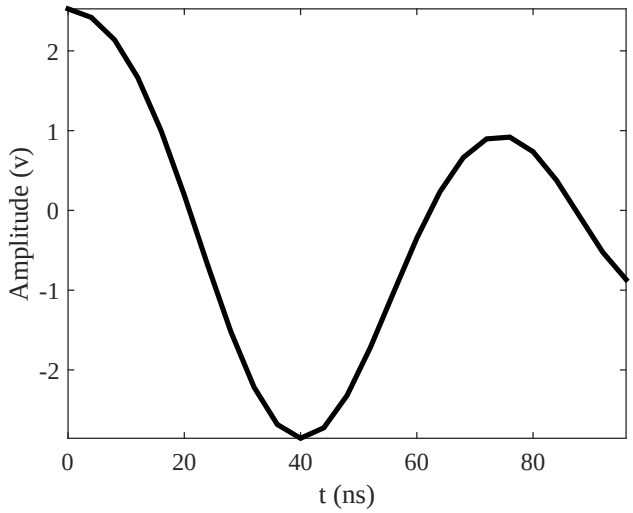
the transmitting DUT. Revalidation and sensitivity analysis results in Section 4.7 are based on Config #2 using probe locations of $L_P \approx 2\,m$ (revalidation) and $L_P \approx 98.0\,m$ (sensitivity analysis) from the transmitting DUT.

3.2 Response Analysis

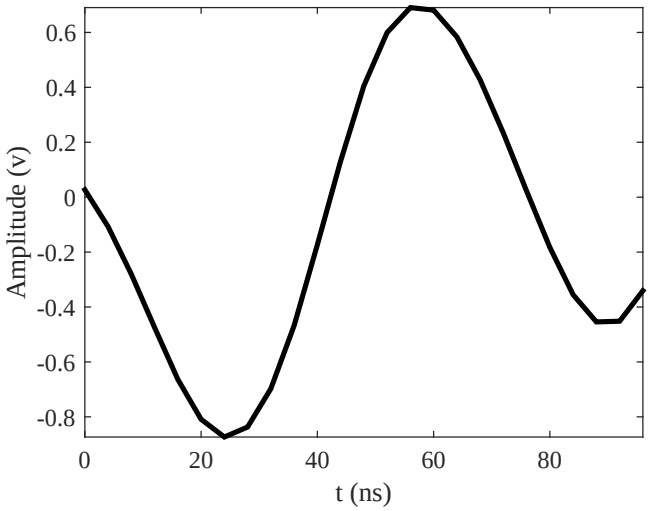
This section provides the technical details for response analysis for both the wire and Electromagnetic (EM) 10BASE-T responses. A voltage change on the wire represents the transmission of symbols in 10BASE-T Ethernet signaling. Figure 3.2a shows an example of the measured wire response for a Clocked Data One (CD1) an oscilloscope. As current flows along the wire an EM field is generated around the wire and the Radio Frequency (RF) probe measures the change in the EM field to generate an EM response for a CD1 as in Figure 3.2b.

In an ideal situation, the two subfigures in Figure 3.2 would be the derivative of each other as given by (3.1), which represents the instantaneous current $i(t)$ given instantaneous voltage $v(t)$ for a single wire [67]. In (3.1) the current, $i(t)$, is equal to the capacitance of a single wire C times the derivative of the voltage, with respect to time. However, Ethernet uses the TWP to reduce common mode noise, crosstalk between adjacent wires, and the reduce the distance that RF signals can travel. The TWP concept does not provide an ideal situation and therefore causes varying responses based on probe placement.

$$i(t) = C \times \frac{dv(t)}{dt} \tag{3.1}$$



(a) Wired Response



(b) EM Response

Figure 3.2. The wired response in (a) is numerically derived from the experimentally collected EM response in (b).

3.3 Post-Collection Processing

This section contains information specific to the processing of individual collections to extract the response Regions of Interest (ROI) used for both RF-DNA and CB-DNA fingerprinting. The post-collection processing occurred exclusively using MATLAB®, after emission collection described in Section 3.1. Each collection was

approximately $T_{Col} \approx 4.5\ ms$ in duration and contained 25 bursts (frames). Figure 3.3 shows a typical collection with various burst durations. The space between two ROI bursts corresponds to what is called the "inter-frame gap" which has a minimum specified duration of $T_{ifg} = 9.6\ \mu s$. The highlighted region in Figure 3.3 is expanded in Figure 3.4 and highlights an area containing a single ROI for both CB-DNA and RF-DNA fingerprinting approaches. For the remainder of the document the term "burst" will be used more widely instead of "frame" as the CB-DNA approach discussed in later sections can be expanded to other types of communication protocols; however, "frame" will be used when specifically talking about the Ethernet.

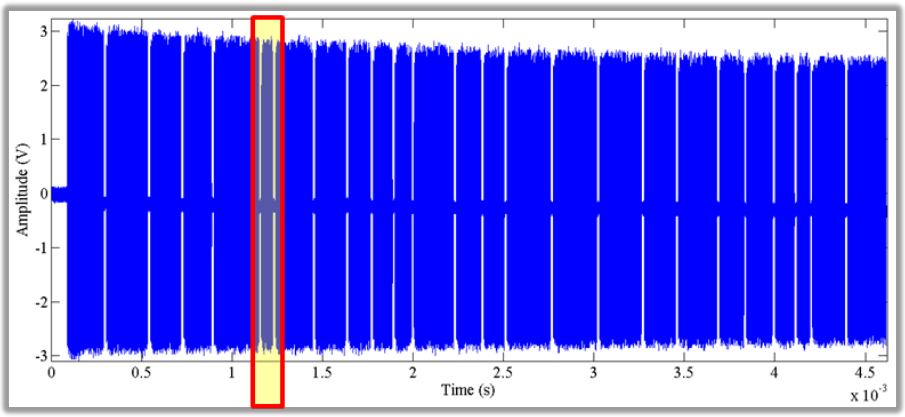


Figure 3.3. Representative 10BASE-T EM probe response collection containing 25 bursts. Highlighted region expanded in Figure 3.4.

3.3.1 Course Burst Detection.

A course burst c_b is extracted from the collected emissions as described herein. The course burst detection process begins with an input sequence of collected samples $\{cs(k) : for\ 1 \leq k \leq N_{CS}\}$, where N_{CS} is the total number of samples in the collected sequence. Two variables are empirically set for course burst detection, including 1) a noise level threshold $V_{NL} = 0.4$ v, and 2) the number of processing window samples $N_{pw} = 800$. The processing window subsequence is given by $\text{pw}(\{m\}) \in \{cs(k)\}$ where m is a consecutive set of discrete samples contained in

$\{cs(k)\}$ such that $m = \{n+1, n+2, \ldots, n+N_{pw}\}$ and $1 \leq n \leq N_{CS} - N_{pw}$. The value of $N_{pw} = 800$ was empirically chosen to equal one-third the number of discrete samples contained within the "inter-frame gap", as defined in [1] and to ensure there would be at least one $pw(\{m\})$ having no value above $N_L = 0.4$.

One of two outcomes is possible within processing window $pw(\{m\})$:

Case A: No value in set m exists such that $pw(\{m\}) > N_L = 0.4$ (noise region)

Case B: > 1 value in set m exists such that $pw(\{m\}) > N_L = 0.4$ (burst region)

Case A and *Case B* conditions describe the extraction of bursts as the processing window slides across $\{cs(k)\}$ in increments of N_{pw} until the end of the collection is reached $(N_{CS} - N_{pw})$. The start and end indexes for a burst within $pw(\{m\})$ are found using the following process. The burst start index is the m satisfying *Case B*, when the previous processing window $pw(\{m - N_{pw}\})$ satisfies *Case A*. At this time, the start index m_s of the detected burst is defined as the first index in $pw(\{m\})$ such that $pw(m_s) > V_{NL}$. The end of the burst is described as the $pw(\{m\})$ being in *Case A* when the previous $pw(\{m - N_{pw}\})$ was in *Case B*. At this time, the end index m_e of the detected burst is the last index in $pw(\{m\})$ for processing window $pw(\{m - N_{pw}\})$ such that $pw(m_e) > V_{NL}$. The burst is extracted according to the start m_s and end m_e indexes and stored for fine burst alignment.

The course burst detection process is illustrated in Figure 3.4 using the entire highlighted region in Figure 3.3 to represent $\{cs(k)\}$. It can be seen that the noise floor (green line) between adjacent bursts is below the $V_{NL} = 0.4$ v threshold and the red line represents a binary decision such that a 1 is represented by at least one $m \subset pw(\{m\}) > V_{NL}$ and a 0 represents that $m \not\subset pw(\{m\}) > V_{NL}$. The red line goes above and below V_{NL} near the burst turn-on and turn-off transition boundaries representing the start (m_s) and end (m_e) indexes of the extracted c_b burst. The fine

burst alignment process in Section 3.3.2 uses the course burst detection output c_b to more precisely locate the ROI prior to RF-DNA and CB-DNA fingerprint generation.

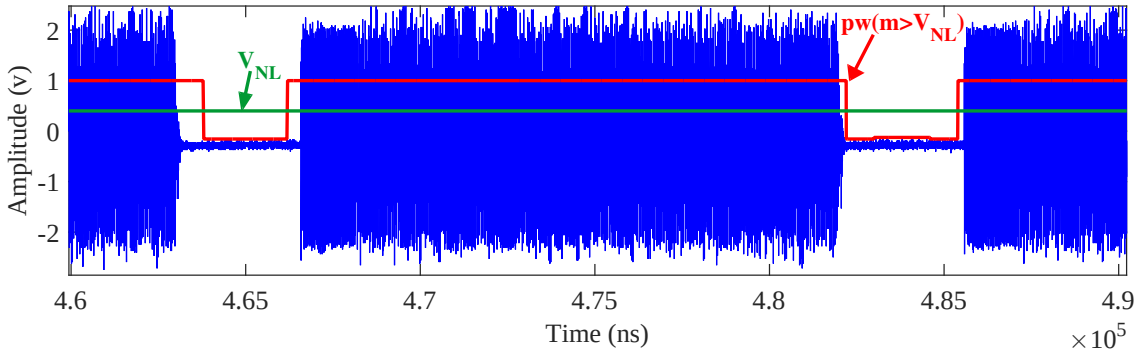


Figure 3.4. Representative $\{cs(k)\}$ from Figure 3.3.

3.3.2 Fine Burst Alignment.

Fine burst alignment is an important step prior to symbol estimation, which is covered in Section 3.4, and both RF-DNA and CB-DNA fingerprinting approaches are covered in Section 3.6 and Section 3.7, respectively. Fine burst alignment enables reliable symbol estimation and ROI determination for both CB-DNA and RF-DNA fingerprinting. Fine burst alignment was accomplished here using correlation. The implementation includes correlating the course detected burst c_b response extracted in Section 3.3.1 with a selected preamble reference response as shown in Figure 3.5.

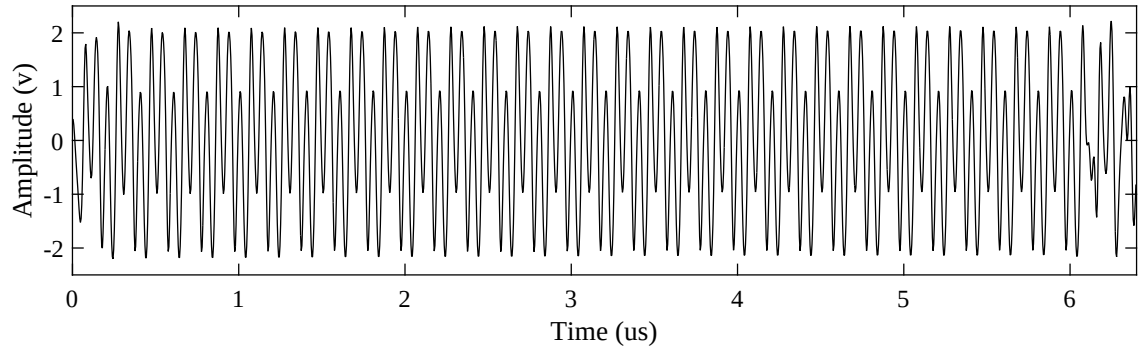


Figure 3.5. Representative 10BASE-T preamble time domain amplitude response used for Fine Burst Alignment (FBA) [10].

The start of the ROI (S_{ROI}) is defined as the sample index number where maximum correlation occurs; the same fine aligned bursts are used for generating both RF-DNA and CB-DNA fingerprints. Fine burst alignment ensures that all ROI's are extracted using the same technique for all devices. The end of the ROI for RF-DNA is $E_{rfROI} = S_{ROI} + N_{DTS}$, where $N_{DTS} = 1600$ is the number of discrete time samples in an Ethernet preamble. The end of the ROI for CB-DNA varies from $S_{ROI} + N_{DTS} + 14,400 < E_{CBROI} < S_{ROI} + N_{DTS} + 57,000$ and is based on the length of the transmitted burst. The number of discrete samples contained in RF-DNA is $N_{RFROI} = N_{DTS}$. The number of samples in a CB-DNA varies on a burst-by-burst basis, and is defined as $N_{CBROI} = m_e - S_{ROI}$, where m_e is the end of a c_b defined in Section 3.3.1. An example burst that has gone through fine burst alignment is presented in Figure 3.6, where the ROI for both RF-DNA (RF_{ROI}) and CB-DNA (CB_{ROI}) are highlighted.

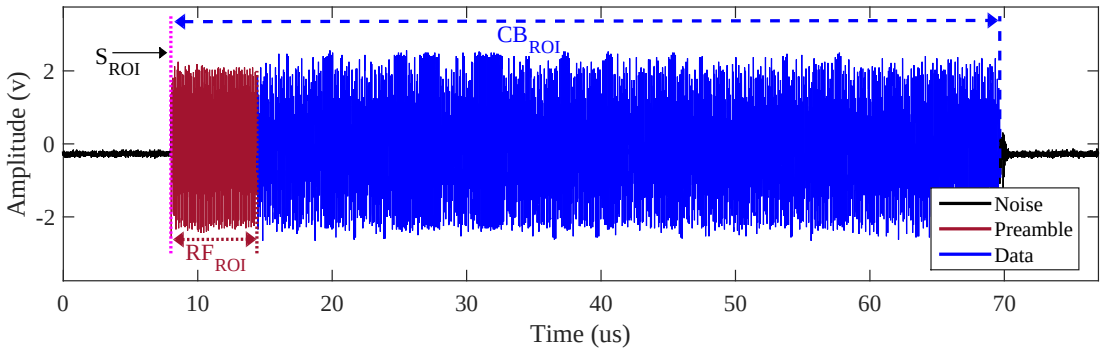


Figure 3.6. An example Ethernet packet highlighting the Regions Of Interest (ROI) for both RF-DNA and CB-DNA.

Fine burst alignment is not perfect and some alignment jitter remains. Jitter is defined here as a delay/lag between S_{ROI} in c_b and the first peak in the preamble of c_b, where units are number of samples. Results for the alignment jitter are covered in Section 4.1.

3.4 Wired Emission Symbol Estimation

This section provides development details for two symbol estimation processes: 1) the original Single Slope (SSLP) symbol estimation technique used to extract Ethernet frame data from Ethernet cable emissions [10], and 2) the expanded Constellation Based (CB) symbol estimation technique that was ultimately used for CB-DNA process development. Proper synchronization is a must for reliable and repeatable symbol estimation. The finely aligned bursts from Section 3.3.2 are considered adequately synchronized and ready for the symbol estimation processes.

Eye diagrams are typically used to analyze communication signal characteristics by visualizing the time-dependent variation between multiple symbols transmitted within a single frame [54, 76]. All eye diagrams used in this research were created after fine burst alignment and were used to verify symbol synchronization and detect the CD1 and Clocked Data Zero (CD0) symbols. The representative eye diagram in Figure 3.7 was constructed by superimposing approximately 2,200 consecutive symbols from a single Ethernet frame.

3.4.1 Single Slope (SSLP) Symbol Estimation.

Eye diagram analysis aided in the development of the test statistic used to perform symbol estimation for SSLP. Visual analysis of Figure 3.7 in the highlighted $T_G(k)$ region shows two groups of signals having amplitudes making either a negative-to-positive and or positive-to-negative transition around the $T_G(k)$ midpoint; these two groups represent CD1 (red) and CD0 (blue) symbols. There also appears to be other symbol variants within each of the two CD1 and CD0 symbols that is revisited later in Section 3.7.1.

The SSLP symbol estimation process for 10BASE-T binary signal reception is described with the aid of Figure 3.8. First, consider a sequence of symbol samples

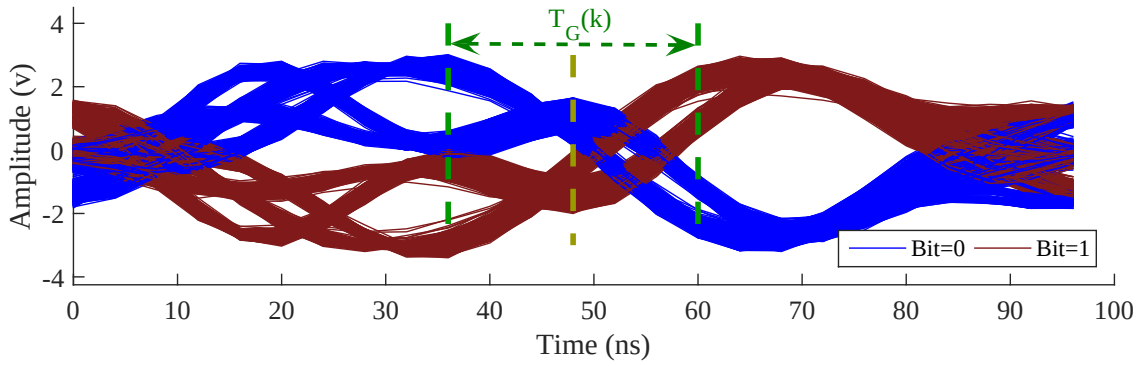


Figure 3.7. Eye diagram from one 10BASE-T collected emission showing 100ns symbol duration.

$\{s(k)\}$ for $1 \leq k \leq N_{TS}$, where N_{TS} is the total number of samples spanning symbol interval T_S in Figure 3.8. For $N_{TS} = 25$ as used here, $T_S \approx 100\ ns$ as shown in (3.2), where $F_{Sample} = 250$ Million Samples/sec (MSps). Elements of $T_G(k)$ are calculated according to (3.3), where N_Δ is the number of samples right and left of the midpoint $T_G(k_m)$ in Figure 3.8. The total number of elements N_{TG} is calculated according to (3.4). It was empirically determined through visual analysis of multiple eye diagrams that a value $N_\Delta = 3$ provided adequate SSLP symbol estimation.

The transition of the symbols from low to high for a CD1 and high to low for a CD0 enabled the use of the mean gradient of $T_G(k)$ as a reliable test statistic (Z_G) to estimate symbol value as in (3.5).

$$T_S = (N_{TS})/F_{Sample} \approx 100\ nSec \tag{3.2}$$

$$T_G(k) = s(k) \quad for \quad (k_m - N_\Delta \leq k \leq k_m + N_\Delta) \tag{3.3}$$

$$N_{TG} = 2 \times N_\Delta + 1\ Samples, 1 \leq N_\Delta \leq (N_{TS} - 1)/2 \tag{3.4}$$

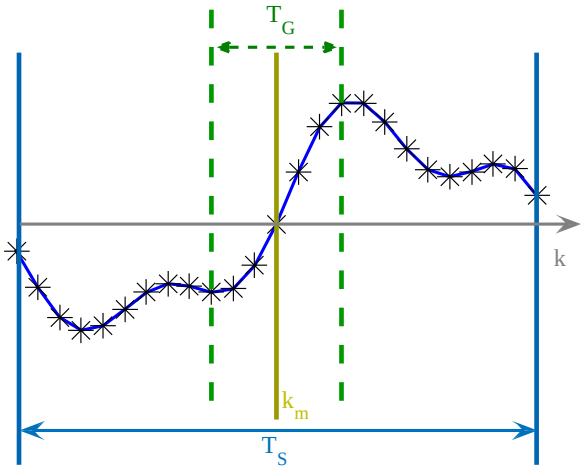


Figure 3.8. Near-field probe response for a Clocked Data One (CD1) symbol with gradient test statistic T_G generation region highlighted.

$$Z_G = Mean\Big[Gradient\{T_G(k)\}\Big] \tag{3.5}$$

The sign of the test statistic values determines whether a symbol is estimated as a CD1 or CD0 according to the following threshold:

$$Z_G > 0 \rightarrow 1,$$
$$Z_G \leq 0 \rightarrow 0. \tag{3.6}$$

3.4.2 Non-Conventional Constellation Development.

The 2D binary constellation described in this section is used for symbol estimation (bit estimation) and CB-DNA fingerprinting that creates cluster statistics based on the clusters formed during symbol projection in Section 3.7. The symbol estimation boundary is presented and its use for symbol estimation is explained. The process used for locating and synchronizing to individual burst responses in the collected traces was as described in Section 3.3.2.

Generation of the 2D constellation for 10BASE-T binary signal reception is an expansion of the SSLP estimation process described in Section 3.4.1 and used for CB symbol estimation in Section 3.4.3. The 2D projection process will be described with the aid of Figure 3.9 and (3.2 - 3.4) from Section 3.4.1. The 2D projection process starts by first considering a sequence of symbol samples $\{s(k)\}$ for $1 \leq k \leq N_{TS}$, where N_{TS} is the total number of samples spanning symbol interval T_S. For $N_{TS} = 25$ as used here, $T_S \approx 100ns$ as shown in (3.2). Elements of $T_G(k)$ are calculated according to (3.3), where N_Δ is the number of samples right and left of the midpoint $T_G(k_m)$. The total number of elements N_{TG} is calculated according to (3.4).

The difference in the symbol estimation process begins here where CB symbol estimation uses $N_\Delta = 7$ for T_G calculation which is an increase of 4 over SSLP symbol estimation approach. The increase in N_Δ was done to capture the variations in the symbols that occur closer to the boundaries of the T_S region in Figure 3.9. Section 3.7.1 has more details about variation affects at the T_S boundaries.

With the new $N_\Delta = 7$ and the sequence mid-point $s(k_m)$ at index k_m, two new gradient-based test statistics are generated using two sub-sequences, $\{T_G^-(k)\}$ and $\{T_G^+(k)\}$, on either side of $s(k_m)$ in Figure 3.9 according to (3.7) and (3.9) [11], where each sub-sequence contains $N_\Delta + 1$ samples. MATLAB® *gradient* operation is used in (3.8) and (3.10) which results in an instantaneous gradient calculation at each sample point that calculates the slope across points $(k-1,\ k,\ k+1)$ for each point k contained in $\{T_G^-(k)\}$ and $\{T_G^+(k)\}$ resulting in $N_\Delta + 1$ total slope values [43]. The resultant Z_G^- from (3.8) and Z_G^+ from (3.10) are used to form the 2D (Z_G^-,Z_G^+) constellation. This is illustrated in Figure 3.10 which shows a representative received symbol constellation for each device manufacturer. The use of these non-conventional constellations for symbol estimation is discussed in Section 3.4.3.

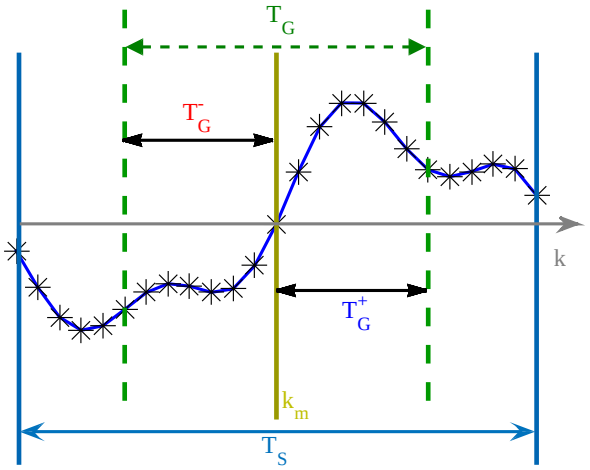


Figure 3.9. Near-field probe response for a Clocked Data One (CD1) symbol with gradient test statistic $T_G^-(k)$ and $T_G^+(k)$ generation regions highlighted.

$$T_G^-(k) = s(k) for (k_m - N_\Delta < k < k_m) \tag{3.7}$$

$$Z_G^- = Mean\Big[Gradient\{T_G^-(k)\}\Big] \tag{3.8}$$

$$T_G^+(k) = s(k) for (k_m < k < k_m + N_\Delta) \tag{3.9}$$

$$Z_G^+ = Mean\Big[Gradient\{T_G^+(k)\}\Big] \tag{3.10}$$

3.4.3 Constellation-Based (CB) Symbol Estimation.

The symbol estimation in this research varies from that of traditional symbol estimation due in part that the transmitted signal was not based on a constellation and the derivative effect of the RF probe on the current passing through the wire. A traditional symbol estimation method compares a projected received symbol against

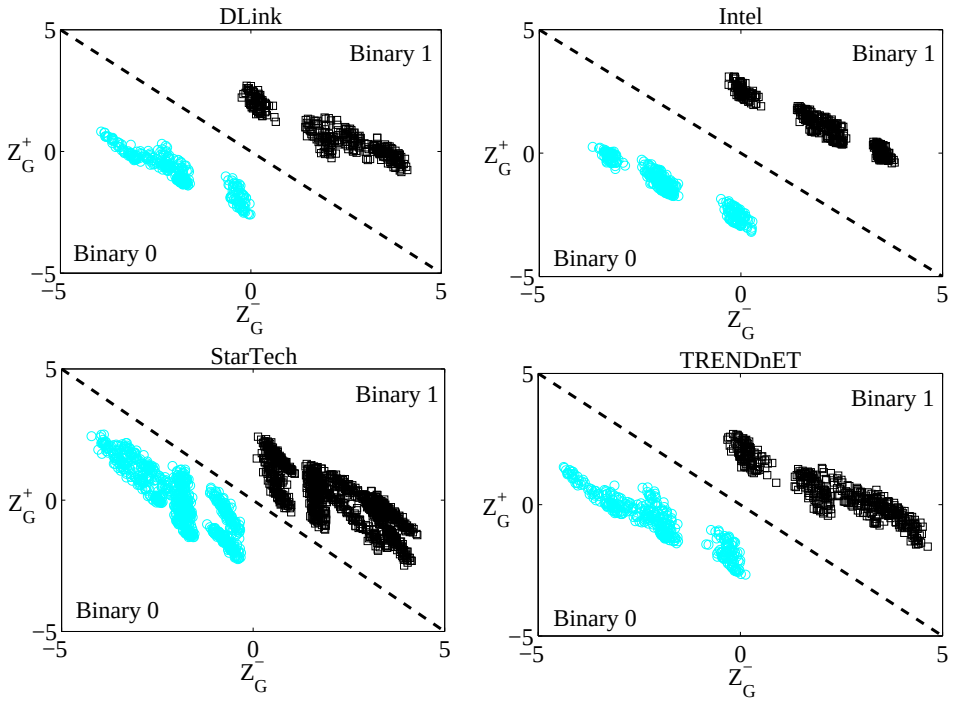


Figure 3.10. 2D binary constellation diagram, symbol estimation boundary for all card manufacturers.

the ideal constellation points and selects the closest ideal constellation point to the received projection to estimate its bit value. This work performs symbol estimation on a symbol-by-symbol basis using a diagonal line denoted by Z_C in Figure 3.11 which represents the 2D binary symbol estimation boundary and is described in (3.11).

$$Z_C \rightarrow Z_G^- = -(Z_G^+) \tag{3.11}$$

To provide symbol estimates the incoming symbols are projected into the 2D constellation space via the (Z_G^-,Z_G^+) pair from Section 3.4.2. Symbols mapped to the left of Z_C are estimated as a binary 0 while symbols mapped to right of Z_C are estimated as a binary 1.

A Bit Error Rate (BER) assessment was conducted on the CB symbol estimation approach and compared to the SSLP approach in Section 3.4.1. The assessment was conducted to assess the impact of BER on the CB-DNA Fingerprinting process

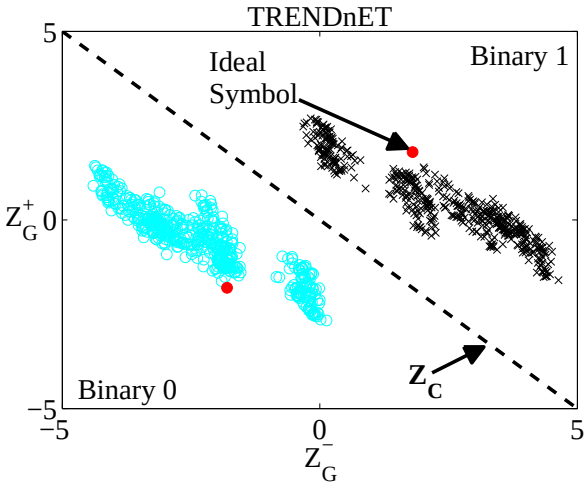


Figure 3.11. 2D binary constellation diagram, symbol estimation boundary, and ideal symbol location for card manufacturer TRENDnET (M3) [11].

in Section 3.7.3 given it relies on symbol estimates to assign projected symbols to clusters. The results of the BER assessment are presented in Section 4.2.

3.5 Signal-to-Noise Ratio (SNR) Variation

An important aspect of device discrimination is to perform fingerprinting assessment under varying channel conditions, i.e., at varying Signal-to-Noise Ratio (SNR). Experimentally collected bursts averaged across all devices provide an SNR of $SNR_C \approx 16$ dB for Config #1, $SNR_C \approx 26$ dB for Config #2 ($L_P \approx 2\ m$), and $SNR_C \approx 24$ dB for Config #2 ($L_P \approx 98\ m$). The calculated SNR for all devices can be found in Table 3.2.

To assess channel variation effects, a total of $N_{Nz} = 6$ independent like-filtered Additive White Gaussian Noise (AWGN) realizations were generated and power scaled in MATLAB® then added to the collected bursts to achieve analysis $SNR_A = \{2x | x \in , 2 < x < 16\}$ dB, (SNR is used in place of SNR_A henceforth for brevity). Each AWGN realization was 1) randomly generated from a Gaussian distribution, 2) baseband filtered with a $W_{BB} = 40$ MHz and a $O_{filt} = 16$ order filter, 3) power-scaled to achieve the appropriate SNR value, and 4) added to the collected signal responses.

This process was repeated for all collected signal responses $N_S = 1,000$ per card to generate a total of $N_F = N_S \times N_{Nz} = 6,000$ fingerprints for model development and device verification in Sections 3.8 and 3.9, respectively.

Table 3.2. Calculated Signal-to-Noise-Ratios (SNR) for All 16 Device Manufacturers at Probe to Transmitter Distances of $L_P = 2\ m$ and $98\ m$ Along the Cable.

Device ID	Config #1 $L_P = 2\ m$	Config #2 $L_P = 2\ m$	Config #2 $L_P = 98\ m$
M1:D1	15.0	26.0	23.6
M1:D2	15.1	26.0	23.4
M1:D3	14.7	26.0	23.6
M1:D4	14.9	25.7	23.4
M2:D1	19.3	24.4	24.7
M2:D2	17.6	25.1	23.7
M2:D3	19.5	24.6	24.5
M2:D4	21.7	25.2	24.5
M3:D1	14.1	25.7	23.4
M3:D2	13.4	25.6	23.4
M3:D3	18.7	25.6	19.8
M3:D4	13.5	25.4	23.8
M4:D1	13.9	25.4	24.3
M4:D2	13.8	25.6	24.5
M4:D3	13.5	25.7	24.2
M4:D4	13.3	25.6	24.0
Average	15.7	25.5	23.7

Variations in the SNR are attributed to the differences in the collection receiver, as well as the probe-to-cable orientation.

3.6 RF-DNA Fingerprinting

This section provides the implementation of the adopted RF-DNA fingerprinting approach discussed in Section 2.3 to include the relevant parameters associated with fingerprint generation used during device discrimination.

3.6.1 RF-DNA Fingerprint Generation.

The preamble of the Ethernet frame was selected as the ROI for implementation of the RF-DNA approach as highlighted in Figure 3.6 and is subsequently expanded in Figure 3.12 to show only the preamble response. The preamble response shown in Figure 3.12 is RF_{ROI}, where each RF_{ROI} contains $N_{DTS} = 1600$ discrete time samples and consists of only $N_{rSym} = 64$ transmitted symbols per ROI.

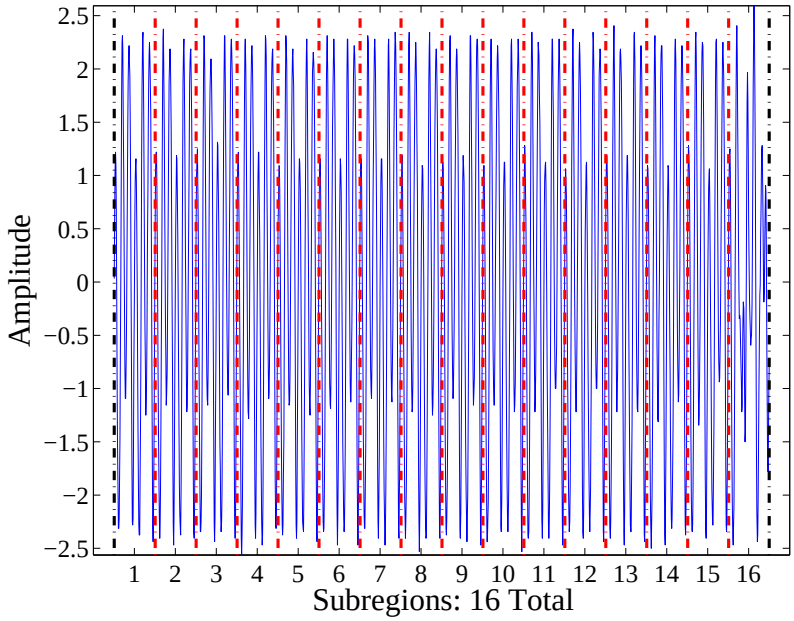


Figure 3.12. Representative 10BASE-T Region of Interest (ROI) for RF-DNA and used for fingerprint generation. The RF_{ROI} contains $N_{DTS} = 1600$ and divided into $N_R = 16$ subregions.

To extract a unique DNA feature set, each Time Domain (TD) ROI is divided into N_R equal length subregions as illustrated in Figure 3.12 for $N_R = 16$, where each N_R subregion has an equal number of discrete times samples k. Instantaneous amplitude $\{a(k)\}$, phase $\{\phi(k)\}$, and frequency $\{f(k)\}$ are TD sequences used for RF-DNA fingerprint generation. Composite RF-DNA fingerprints are generated by: 1) centering (mean removal) and normalizing $\{a(k)\}$, $\{\phi(k)\}$, and $\{f(k)\}$, 2) calculating three statistical features of variance (σ^2), skewness (γ), and kurtosis (κ) for *each*

TD sequence to form *Regional Fingerprint* $F_{R_i}^{RF}$ as in (3.12) for $i = 1, 2, \ldots, N_R$, and concatenate into an instantaneous response vector as in (3.13)and, 3) concatenate instantaneous response vectors $F_{a,\phi,f}^{RF}$ to form the final $1 \times (9N_R)$ *Composite RF-DNA Fingerprint* F_C^{RF} as in (3.14) [16, 17, 73].

$$F_{R_i}^{RF} = [\sigma_{R_i}^2, \gamma_{R_i}, \kappa_{R_i}]_{1\times 3} \tag{3.12}$$

$$F_{a,\phi,f}^{RF} = [F_{R_1}^{RF} : F_{R_2}^{RF} : F_{R_3}^{RF} : \cdots : F_{R_{N_R+1}}^{RF}]_{1\times N_R} \tag{3.13}$$

$$F_C^{RF} = [F_a^{RF} : F_\phi^{RF} : F_f^{RF}]_{1\times(9N_R)} \tag{3.14}$$

The total number of RF-DNA features in (3.14) is a function of N_R, TD responses, and statistics. Varying N_R provides a means to investigate performance for various feature vector sizes. Fingerprints were generated over the ROI using three TD responses ($\{a(k)\}$, $\{\phi(k)\}$, $\{f(k)\}$), three statistics (σ^2, γ, κ) per response, for $N_R = 16, 32, 80$ with (3.14) and produced RF-DNA fingerprints having $N_{Feat} = 144, 288, 720$ total features, respectively. A total $N_{Nz} = 6$ independent AWGN realizations were added to each of the $N_S = 1,000$ collected bursts as described in Section 3.5 to provide a total of $N_F = N_S \times N_{Nz} = 6,000$ fingerprints for each device at each analysis $SNRs$.

3.7 CB-DNA Development

This section provides technical details for developing a two-dimensional (2D) signaling constellation from symbol projections. This development was required given that the near-field probe response represents the time derivative of signals passing through the Ethernet cable and no previous constellation was associated with the

derivative signal. CB symbol estimation was covered in Section 3.4.3. Section 3.7.1 explains *conditional* and *unconditional* cluster regions within the constellation space. The CB-DNA approach is explained in Section 3.7.2 which exploits the subcluster (*conditional*) and aggregate (*unconditional*) regions for fingerprint generation in Section 3.7.3.

3.7.1 Constellation Cluster Analysis.

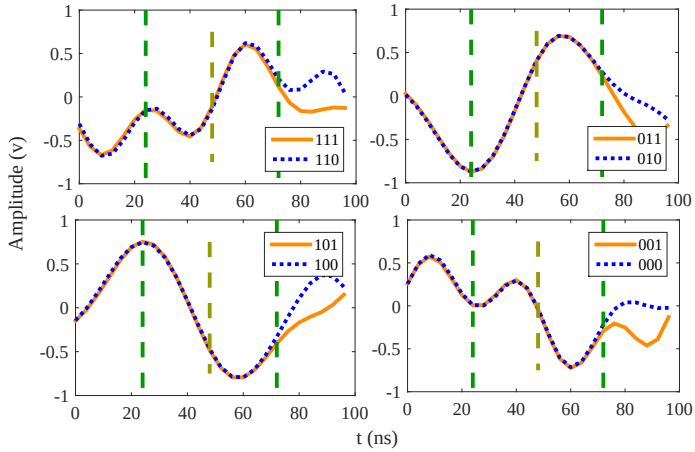
The 10BASE-T Ethernet Standard 802.3, Clause 14 states that only two symbols are used to transmit a data one and zero. However, Section 3.4.1 postulated that the Ethernet cable emissions collected by the RF probe contained multiple variations of those symbols based on the appearance of the eye diagram in Figure 3.7. The symbol projection process developed in Section 3.4.2 further supports the idea of subclusters in the constellations presented in Figure 3.10 because cluster regions are easily identifiable within the aggregate clusters of ones and zeros. For example, Figure 3.10 shows that the Intel constellation has six distinct groupings, with three on each side of Z_C.

To highlight the symbol variants responsible for the subclusters within a projected constellation, each symbol variant is separated by their demodulation value and grouped based on preceding and succeeding symbol estimations. As a result, four symbol shapes emerge that represent an estimated CD1 and four that represent an estimated CD0 for a total of eight distinct symbol shapes. Figure 3.13 displays the eight symbols for two manufacturers. When referring to the subplots in Figure 3.13 a quadrant system is used. The upper left quadrant is referred to as quadrant one and the quadrants are increased numerically in a clockwise rotation until the quadrant 4 (lower left) is reached. For both card manufacturers the symbols in quadrants one and two represent an estimated symbol value of a one and in quadrants three and

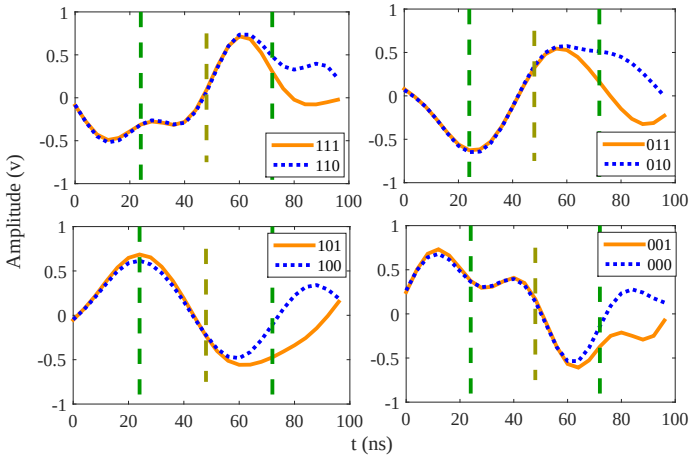
four an estimated symbol value of a zero. Quadrants two and three have a preceding estimated symbol of a one, and quadrants one and four have a preceding estimated symbol of a zero. In Figure 3.13, a succeeding estimated symbol of a one is represented by a solid line in all quadrants, whereas a zero is a dashed line. Each symbol was generated by averaging $N_{sym} = 200$ symbols for each of the eight bit combinations, $[000], [001], [100], [101], [111], [110], [011], [010]$. A quadrant by quadrant comparison between, Figure 3.13a and Figure 3.13b shows that symbol shapes are similar near the midpoint of the symbols between the card manufacturers. However, slight variations can be seen in the amplitude and signal behavior at the left edge of T_G^- and right edge of T_G^+ regions denoted as green dashed lines.

With the new information gained through cluster analysis a new color constellation was created by plotting each of the eight symbols with a different (symbol/color) combination to highlight the effect of preceding and succeeding bit combinations on constellation shapes. The new constellation is displayed in Figure 3.14 where it is apparent that *independent* aggregate clusters in Figure 3.11 are made up of four *dependent* subcluster regions.

Figure 3.14 displays eight distinct conditional subcluster regions for StarTech (M3:D1). The two legends denote the bit combinations used to assign projected symbols to a given subcluster. Middle bit values represent the current bit being estimated. For example, the red open circles are estimated to be a zero and the estimated bit before and after the current bit are also estimated as a zero. The dependent subcluster regions are also provided for the remainder of the four manufacturers in Figure 3.15 where it is visually evident that Intel (M2) and StarTech (M4) constellations are discernibly different than DLink (M1) and TRENDnET (M3). In Figure 3.15 it is also apparent that M1 and M3 are the most similar and would be difficult to tell apart visually. It is these variations in subcluster sizes and locations



(a) M1:D1



(b) M2:D1

Figure 3.13. Averaged symbol shapes presented for card manufacturer M1 (a) and M2 (b) with each symbol representing an average of $N_{sym} = 200$ symbols. The dashed yellow vertical line is the symbol midpoint k_m and the dashed green vertical lines represent the boundaries of T_G from Figure 3.9.

that the CB-DNA fingerprinting approach capitalizes on when creating a fingerprint feature set.

3.7.2 CB-DNA Fingerprinting Approach.

As with the RF-DNA fingerprinting approach, a majority of prior constellation-based fingerprinting works rely on features extracted from intentional RF emissions. However, unlike RF-DNA approaches that extract relevant features *prior* to symbol

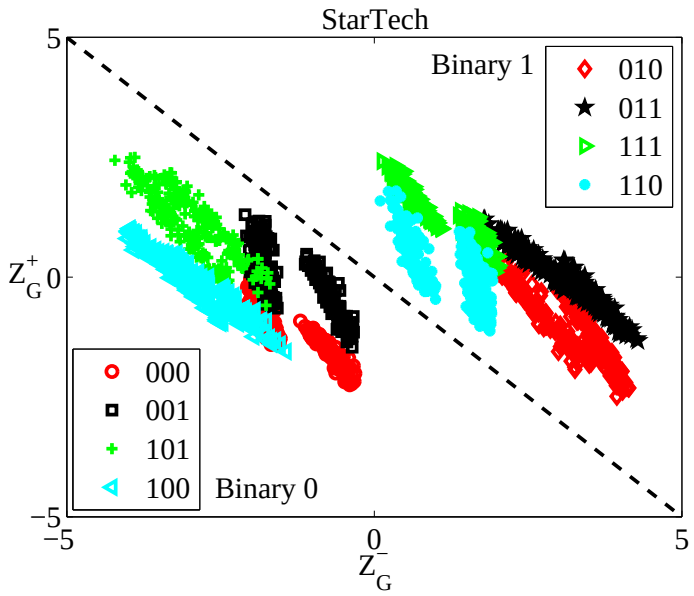


Figure 3.14. 2D binary constellation diagram, symbol estimation boundary and sub-cluster regions for card manufacturer StarTech (M3).

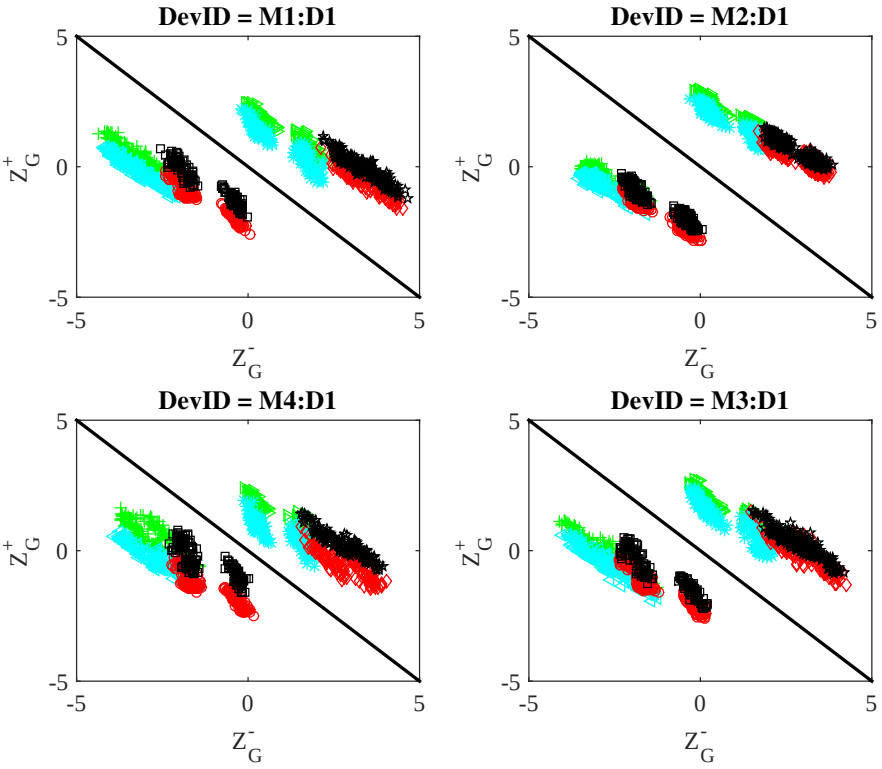


Figure 3.15. 2D binary constellation diagram, symbol estimation boundary and sub-cluster regions for all card manufacturers.

constellation mapping, the constellation-based methods rely on this mapping and extract unique features derived from modulation errors within the constellation space, i.e., differences (error) between received projected symbol points and ideal transmitted constellation points [6, 20, 25, 35]. The CB-DNA approach developed here also relies on projected symbol mapping, but differs from previous approaches by extracting statistical features from projected symbols grouped as: 1) *Unconditional* aggregated clusters, and 2) *Conditional* subclusters comprising the aggregated cluster. The aggregated clusters are qualified as *unconditional* given that projection assignment to these clusters is *independent* of prior and subsequent symbol projections (bit values) given that only a single communication symbol within the burst is required for assignment. The subcluster regions are qualified as *conditional* given that projection assignment to subclusters is *dependent* on both the prior and subsequent symbol projections (bit values prior to and succeeding the current bit to be estimated) three consecutive communication symbols within a burst are required for assignment.

The entire Ethernet communication burst is used as the ROI for the CB-DNA fingerprinting approach as highlighted in Figure 3.6. Given the variable payload of Ethernet transmissions, the number of communication symbols available in each burst used for CB-DNA fingerprint generation ranges from $N_{sym} = 576$ to $N_{sym} = 2,280$ including the preamble symbols. As such, each subcluster region averages between 72 and 285 projected symbols. When compared to the RF-DNA ROI which only includes the preamble response $N_{sym} = 64$, the CB-DNA ROI provides 9 to 33 times more symbols to generate fingerprint statistics.

Unique CB-DNA feature sets are extracted from the burst ROI using the following steps on a burst-by-burst basis: 1) individual communication symbols within the burst are projected into the constellation space described in Section 3.4.3, 2) resultant $(Z_G^-,\ Z_G^+)$ pairs are placed in one of eight groups based on three consecutive symbol

projections, i.e., [0 X 0], [0 X 1], [1 X 0], and [1 X 1], where X denotes the symbol being currently projected, 3) statistical features of mean (μ), variance (σ^2), skewness (γ), kurtosis (κ), covariance (Cov), coskewness ($\beta_{1\times2}$), and cokurtosis ($\delta_{1\times3}$) are calculated for the two *unconditional* aggregated and eight *conditional* subcluster regions, and 4) fingerprints sets are formed according to the Section 3.7.3.

3.7.3 CB-DNA Fingerprint Generation.

Calculation of statistical CB-DNA fingerprint features originate within designated aggregate and subcluster regions of the constellation described in Section 3.7.1 for a total of $N_{CR} = 2 + 8 = 10$. Statistical CB-DNA features are then calculated for each cluster region using the mean (μ), variance (σ^2), skewness (γ), and kurtosis (κ) along the Z_G^- and Z_G^+ dimensions shown in Figure 3.14. Joint statistics in both the Z_G^- and Z_G^+ direction are also considered and include covariance (cov), coskewness ($\beta_{1\times2}$), and cokurtosis ($\delta_{1\times3}$). The resultant statistics form a *Regional Cluster Fingerprint* $F_{R_i}^{CB}$ given by (3.15), where the superscripted $-/+$ sign denotes constellation dimension and $i = 1, 2, \ldots, N_{CR}$. The final *Composite CB-DNA Fingerprint* F_C^{CB} is of dimension $1 \times (14 \times N_{CR})$ and constructed by concatenating $F_{R_i}^{CB}$ from (3.15) as shown in (3.16) [11].

$$F_{R_i}^{CB} = \left[\mu_{R_i}^-, \mu_{R_i}^+, \sigma_{R_i}^{2-}, \sigma_{R_i}^{2+}, \gamma_{R_i}^-, \gamma_{R_i}^+, \kappa_{R_i}^-, \kappa_{R_i}^+, cov_{R_i}, \beta_{1\times2}^{R_i}, \delta_{1\times3}^{R_i}, \right]_{1\times14} \tag{3.15}$$

$$F_C^{CB} = \left[F_{R_1}^{CB} : F_{R_2}^{CB} : F_{R_3}^{CB} : \cdots : F_{R_{N_{CR}}}^{CB}\right]_{1\times(14N_{CR})} \tag{3.16}$$

The total number of CB-DNA features in (3.16) is a function of N_{CR}, statistics, and dimensions i.e., Z_G^- and Z_G^+. Varying N_{CR} provides a means to investigate performance for various feature vector sizes. Fingerprints were generated using $N_{CR} = 2, 8, 10$, with 4 statistics (μ, σ^2, γ, κ) from each of the Z_G^- and Z_G^+ dimen-

sions and 6 joint statistics (cov, $\beta_{1\times2}$, $\delta_{1\times3}$) producing CB-DNA fingerprints having $N_{Feat} = 28,112,140$ total features, respectively. A total $N_{Nz} = 6$ independent, like-filtered AWGN realizations were added to each of the $N_S = 1,000$ collected bursts as described in Section 3.5. This yields a total of $N_F = N_S \times N_{Nz} = 6,000$ fingerprints per device for each analysis SNR.

3.8 Device Classification

This section describes the specific implementation of MDA/ML processing in Section 2.5 that was used to generate results in Chapter IV. The general term *class* is used to describe either a group of network devices from a specific manufacturer (manufacturer class) or an individual network card (device class). Cross-Model Discrimination (CMD) is used herein to mean discrimination of classes representing devices from different manufacturers. Like-Model Discrimination (LMD) is used herein to mean discrimination of classes representing devices from the same or different manufacturers, of the same model number, and differing only in serial number.

Device classification represents a "1 vs. M" assessment where fingerprints from an unknown device (one authorized or rogue device) are compared against fingerprints from all known authorized devices (the many) and a decision made that assigns an identity (rightly or wrongly) to the unknown device matching one of the authorized devices. This is a "best match" assessment that can yield both good and poor matches.

The effect of varying SNR on discrimination performance was assessed to characterize the effect of varying channel conditions and to provide an assessment of the relationship between collection probe placement and Ethernet card separation distance. This was accomplished by adding independent like-filtered Additive White Gaussian Noise (AWGN) N_{Nz} realizations to each experimentally collected emission as outlined in Section 3.5. For Monte Carlo simulation results in Chapter IV, a total of

$N_{Nz} = 6$ independent AWGN realizations were used to generate fingerprints across the desired $SNR_A = \{2x | x \in, 2 < x < 16\}$ dB. Given $N_{Nz} = 6$ AWGN realizations and $N_S = 1,000$ collected signal responses per card, a total of $N_F = N_S \times N_{Nz} = 6,000$ independent fingerprints per card were used for discrimination assessment at each SNR.

The adopted MDA/ML processing approach used here is from [50] and used to compare RF-DNA and CB-DNA device classification performance. Both CMD and LMD is considered using $N_C = 4$ and $N_C = 16$ classes, respectively. An identical number of *Training* (N_{Tng}) and *Testing* (N_{Tst}) fingerprints are used for each class. A total of $N_F = 24,000$ (CMD) and $N_F = 6,000$ (LMD) fingerprints were generated at each SNR for each N_C per Section 3.6.1 for RF-DNA and Section 3.7.3 for CB-DNA. Classifier cross-validation is implemented using a factor of $K = 5$ to improve MDA/ML reliability.

Plots of average cross-class percent correct ($\%C$) versus analysis SNR and raw classification confusion matrices are used in Section 4.4 to quantify classification performance. This provides an accurate picture of overall performance for the classification model across all SNR explored. The confusion matrices are used to assess performance at a specific SNR and to highlight correct and incorrect cross-class performance that is not evident in $\%C$ plots. The confusion matrix representations used here are consistent with literature [27, 28], with 1) correct classification reflected in diagonal entries, and 2) misclassification reflected in off-diagonal entries, i.e., how one class is confused with another class in the model.

3.9 Device ID Verification

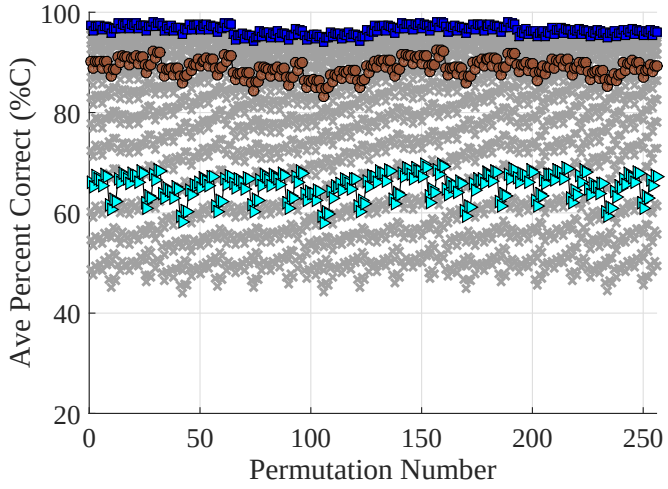
This section provides the specific implementation for device verification as outlined in Section 2.6 and is used to generate the verification results in Chapter IV. The Euclidean distance metric is chosen as the measure of similarity for device verification.

The development of the reference model/models is the first step in verification as outlined in Section 2.6 which involves selecting rogue devices from the pool of available devices from Table 3.1 to hold out during MDA/ML model development. To keep the model of authorized devices as robust as possible the original set of $N_C = 16$ was divided into two disjoint sets representing $N_{A(i)} = 12$ authorized devices and $N_{R(i)} = 4$ rogue devices where $i = 1, 2, 3, ..., N_{Perm}$ denotes permutation number. For each permutation, the $N_{R(i)}$ rogue set contains 1-of-4 devices from each manufacturer and are selected as four-choose-one on a per manufacturer basis, yielding a total of $N_{Perm} = 256$ possible rogue permutations sets. Accordingly, the $N_{A(i)}$ authorized sets contain the remaining 3-of-4 devices from each manufacturer. Table 3.3 provides ten representative permutations where, $\mathsf{X} \in N_{A(i)}$ and $\{\text{R1, R2, R3, R4}\} \in N_{R(i)}$. For each permutation, all $N_{R(i)} = 4$ rogues present false credentials matching *each* of the $N_{A(i)} = 12$ authorized devices, for a total of $4 \times 12 = 48$ rogue scenarios per permutation. Accounting for $N_{A(i)} = 12$ authorized devices and $N_{Perm} = 256$ rogue permutations of $N_{R(i)} = 4$ rogue devices provides a total of $12 \times 256 \times 4 = 12,288$ possible rogue assessment scenarios.

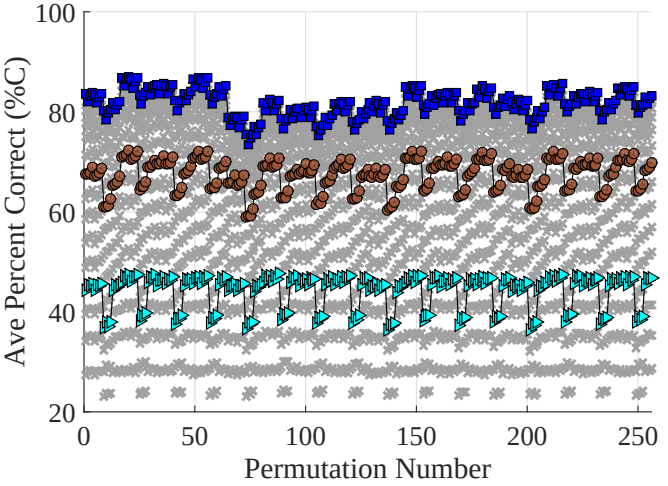
Providing results for all $N_{Perm} = 256$ permutations would be tedious; therefore, a reduced number of results will be presented in Chapter IV. The process for selecting the limited number of permutations discussed in Section 4.5 is based on the examination of the %C for all $N_{Perm} = 256$ authorized permutations. All $N_{Perm} = 256$ MDA/ML permutations were generated with CB-DNA and RF-DNA approaches and a visual inspection of Figure 3.16 shows no apparent outliers but instead shows a periodic trend is evident in $\%C$ for each SNR over all $N_{Perm} = 256$ permutations.

Per the legend in Figure 3.17, $\%C$ results for three specific SNR are highlighted with periodic behavior attributed to how devices were assigned to each permutation.

With no apparent visual outliers in Figure 3.16a, the lowest and highest $\%C$ for



(a) CB-DNA



(b) RF-DNA

Figure 3.16. LMD average $\%C$ for 256 permutations (i=1, 2,. . . , 256) with $N_{A(i)}$=12 devices chosen as 3 devices from each of 4 manufacturers. All SNR ranges are plotted with specific SNRs highlighted according to Figure 3.17.

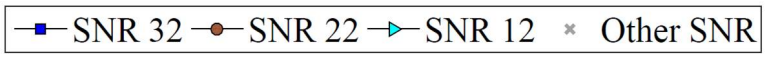


Figure 3.17. Legend for Figure 3.16.

Table 3.3. Manufacturer-Device (M:D) Combinations Used for Verification Assessments. Shows 10 of 256 Permutations with X Denoting $N_{A(i)} = 12$ (i = 29, 32, 74, 105, 106, 107, 108, 157, 159 and 160) Authorized Devices and 4 Rogue Devices {R1, R2, R3, R4} [?].

Reference	MAC Address Last Four	Perm (i)									
		29	32	74	105	106	107	108	157	159	160
M1:D1	D966	R1	R1	X	X	X	X	X	X	X	X
M1:D2	DA06	X	X	R1	R1	R1	R1	R1	X	X	X
M1:D3	DA07	X	X	X	X	X	X	X	R1	R1	R1
M1:D4	60E0	X	X	X	X	X	X	X	X	X	X
M2:D1	1586	X	X	R2	X	X	X	X	X	X	X
M2:D2	1A93	R2	R2	X	X	X	X	X	R2	R2	R2
M2:D3	1A59	X	X	X	R2	R2	R2	R2	X	X	X
M2:D4	1A9E	X	X	X	X	X	X	X	X	X	X
M3:D1	9B55	X	X	X	X	X	X	X	X	X	X
M3:D2	9334	X	X	X	X	X	X	X	X	X	X
M3:D3	9B54	X	X	R3	R3	R3	X	X	X	X	X
M3:D4	9B56	R3	R3	X	X	X	R3	R3	R3	R3	R3
M4:D1	32CB	R4	X	X	R4	X	X	X	R4	X	X
M4:D2	32B4	X	X	R4	X	R4	X	X	X	X	X
M4:D3	96F4	X	X	X	X	X	R4	X	X	R4	X
M4:D4	3048	X	R4	X	X	X	X	R4	X	X	R4

each SNR are taken from Figure 3.16a and provided in Figure 3.18 for comparison. Again no visual outliers are present and the expected relationship of increasing $\%C$ with increasing SNR is evident. Therefore, a representative set of $N_{A(i)}$ permutations in Table 3.3 were chosen for presentation given they are statistically representative of highest ($i = 29, 32, 157, 159, 160$) and lowest ($i = 74, 105, 106, 107, 108$) $\%C$. These permutations are subsequently used for rogue assessment in Section 4.5 at an analysis $SNR = 20$ dB that corresponds to the first time that $\%C > 90\%$ in Figure 3.18.

Verification results presented in Section 4.5 are based on Table 3.3, which provides ten representative permutations for, X$\in N_{A(i)}$ and $\{R1,\ R2,\ R3,\ R4\} \in N_{R(i)}$, where ($i = 29, 32, 74, 105, 106, 107, 108, 157, 159, 160$). For each permutation, all $N_{R(i)} = 4$

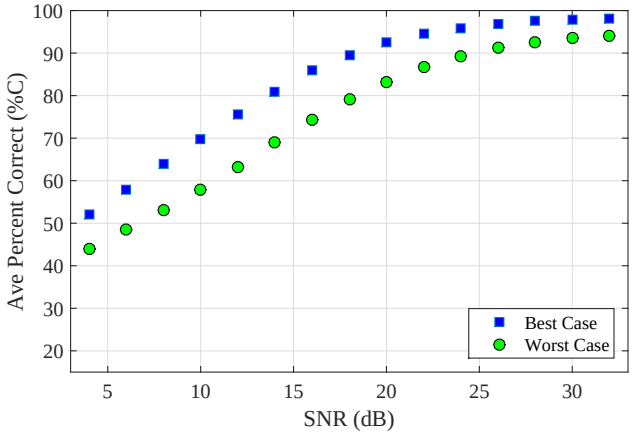


Figure 3.18. Highest and lowest $\%C$ performance across all permutations in Figure 3.16 at each *SNR* considered.

rogue devices present false credentials matching *each* of the $N_{A(i)} = 12$ authorized devices, for a total of $4 \times 12 = 48$ rogue scenarios per permutation.

3.9.1 Authorized Device Assessments.

Test statistics Z_V are calculated for authorized devices from $N_{Tng} = 3,000$ and $N_{Tst} = 3,000$ fingerprints to assess the ability for an authorized device to correctly gain access to the network. The test statistics are used to generate the authorized device Probability Mass Functions (PMF) for the training and testing sets. The generated PMFs are then used to create the Receiver Operating Characteristic (ROC) curves which provide a measure of system performance as outlined in Section 2.6. An example ROC curve is displayed in Figure 3.19 and is used to set device dependent threshold values, $t_V(d)$ for $d = 1, 2, \ldots, N_{A(i)}$, which are set here at the Equal Error Rate (EER) for consistency with other related research.

The assessment criteria for an authorized device is based on True Verification Rate (TVR) and False Verification Rate (FVR) such that $TVR > 0.9$ and $FVR < 0.1$, which results in a Binary Grant/Deny (BGD) access decision with respect to the authorized ROC curves. Solid lines in the authorized device ROC curves have suc-

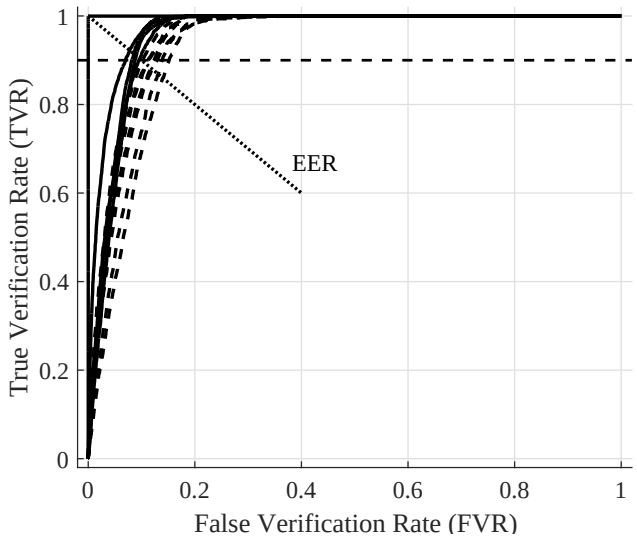


Figure 3.19. A general Receiver Operating Characteristic (ROC) curve with horizontal dashed lined representing the 90 % benchmark and solid (Grant) and dashed (Deny) curves represent the Binary Grant/Deny (BDG) access decision.

cessfully met the BGD criteria and gained access to the network while dashed lines represent those that do not. The Authorized Accept Rate (AAR) is a metric that measures all the BGD decisions for a given permutation. When $AAR = 100\%$ for a given permutation, all $N_A = 12$ devices have successfully gained access to the network.

Figure 3.20 displays an alternative way to look at a ROC curve by plotting the individual test statistics that make up the PMFs from which the ROC curves are generated. In Figure 3.20 the blue circles represent an authorized device being correctly granted access to the network and the red X's denote when the authorized device was incorrectly denied access to the network. Each test statistic is representative of a single burst attempt at network access and thereby results will be presented as Burst-by-Burst (BbB). The horizontal black lines represent the threshold value $t_V(d)$ at the EER for each authorized device $A1 \ldots A12$ from Figure 3.19.

BbB attempts are reported using an TVR metric. The BbB metrics are based on $N_A = 12$ authorized devices with each attempting $N_{Tst} = 3,000$ network access attempts. This results in $N_{aa} = 3,000$ access attempts for each device and when $TVR = 100\%$ that device was correctly granted access for all N_{aa} access attempts.

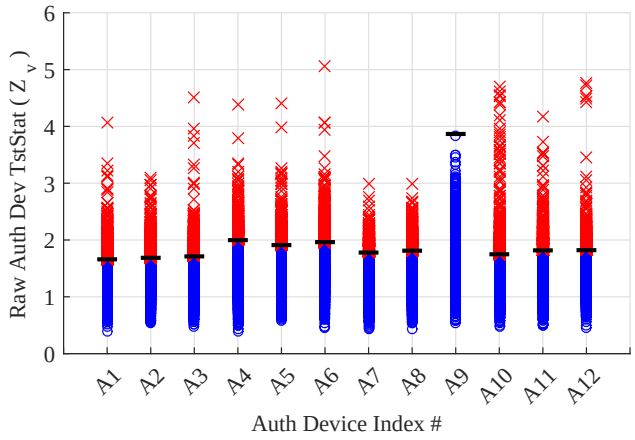


Figure 3.20. Individual euclidean distance test statistics. Solid horizontal lines are device dependent $t_V(d)$ thresholds corresponding to ROC EER in Figure 3.19. Authorized devices are listed as (A1–A12). Individual ID verification test statistics are represented by either blue circles correctly granted access or red X's incorrectly denying access.

3.9.2 Rogue Device Assessments.

Rogue assessment results in Section 4.5 are based $N_{Tst} = 6,000$ rogue testing fingerprints being compared against each of the $N_A = 12$ authorized devices, for a total of $Z_V = 6,000 \times 12 = 72,000$ test statistics per rogue device for a given rogue assessment. With each permutation having $N_R = 4$ rogue devices, the resultant number of test statics calculated per permutation considered is $NZ_V = 288,000$.

The assessment criteria for rogue devices is based on TVR and Rogue Rejection Rate (RAR) such that $TVR > 0.9$ and $RAR < 0.1$ which also results in a BGD access decision with respect to the rogue ROC curves. Solid lines in rogue device ROC curves are denied access to the network by because they met the rogue BGD criteria, while dashed lines represent those that have been erroneously granted access. The Rogue Rejection Rate (RRR) ($RRR = 1 - RAR$) is a metric that measures all the BGD decisions for a given permutation. When $RRR = 100\%$ for a given permutation, then all $N_A = 12 \times N_R = 4 = 48$ rogue access attempts have been successfully denied access to the network.

BbB attempts are also reported using an RRR metric. The BbB metrics are

based on $N_R = 4$ rogue devices with each attempting $N_{Tst} = 6,000$ network access attempts as each of the $N_A = 12$ authorized devices. The resultant number of access attempts is $N_{aa} = 4 \times 6,000 \times 12 = 288,000$. When $RRR = 100$, all $N_{aa} = 288,000$ access attempts were correctly denied network access. A similar BbB figure will be used for RRR comparisons as was used for TVR of authorized devices.

3.10 Device ID Verification Enhancements

This sections provides two enhancements called CPA and PPA to improve the performance of device ID verification. Figure 3.21 represents the general process for each of the enhancements. CPA is covered in Section 3.10.1 and PPA in Section 3.10.2.

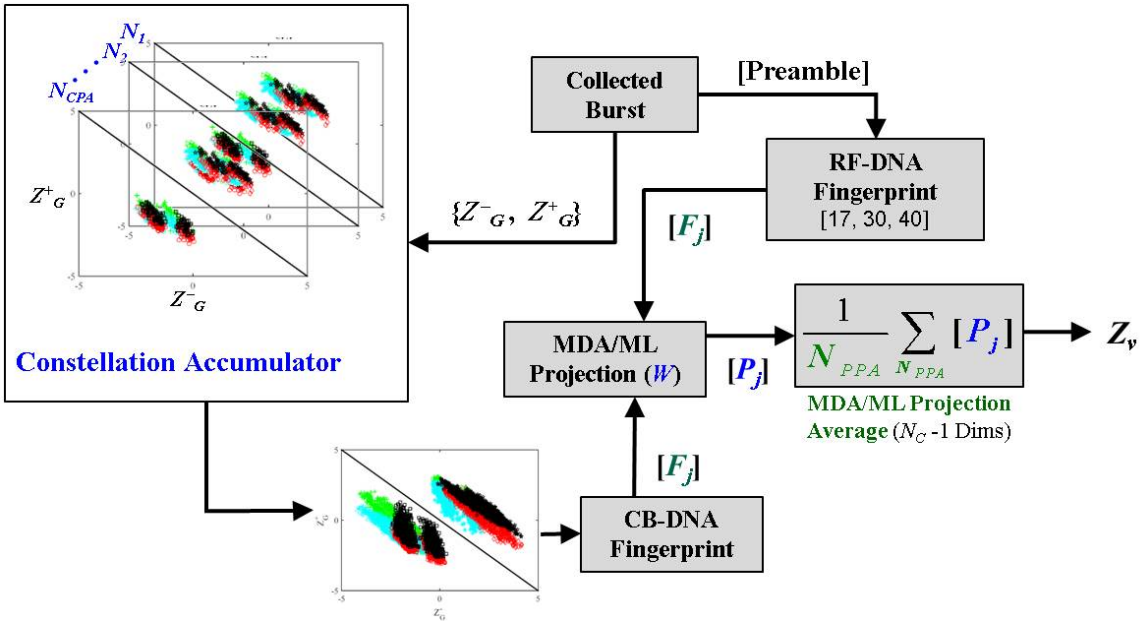


Figure 3.21. Device ID verification improvement methodology, including: 1) Constellation Point Accumulation (CPA) for CB-DNA, and 2) MDA/ML Projection Point Averaging (PPA) for both RF-DNA and CB-DNA.

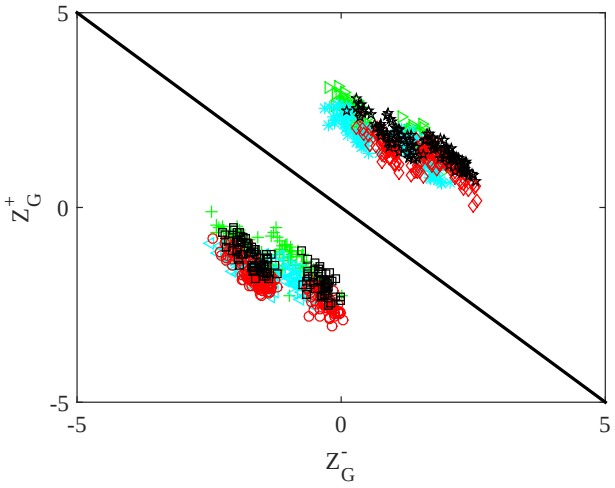
3.10.1 Constellation Point Accumulation (CPA).

This section provides an explanation of CPA. Two figures are presented to provide an example of CPA effects on N_{CR} regions, 3) The CPA process and fingerprint

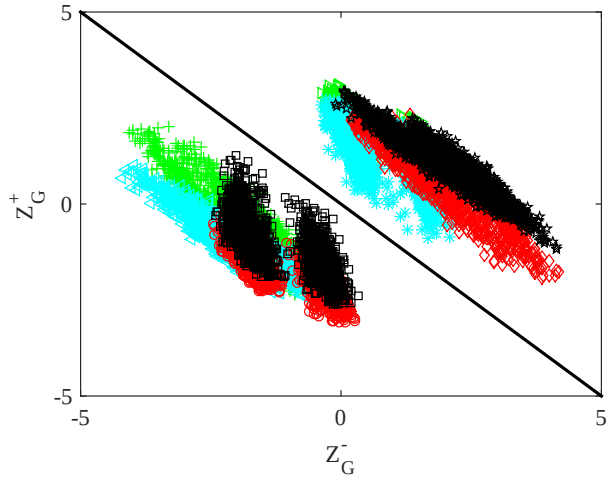
generation based on the increased size of N_{CR} regions is explained.

Constellation point accumulation is accomplished prior to fingerprint generation and is used to increase the number of projected symbols per N_{CR} region. The idea for this enhanced process is that the more points included in the calculation of statistical features discussed in Section 3.7.3 would provide more veritable fingerprint features and thus increase device discrimination performance.

An example of the effects of CPA on constellation shape and density is provided in Figure 3.22 where it is clearly evident that the number of symbol projections have increased in Figure 3.22b from Figure 3.22a.



(a) $N_{CPA} = 1$



(b) $N_{CPA} = 9$

Figure 3.22. The effects of Constellation Point Accumulation (CPA) on cluster regions for device M4:D1 (StarTech).

The process of CPA takes multiple bursts $N_B(i)$, $(i = 1, \ldots, N_{CPA})$ and divides each $N_B(i)$ into their respective $N_{CR}(i, j)$, $(j = 1, 2, \ldots, 10)$ cluster regions as outlined in Section 3.7.1 and Section 3.7.2. The $N_{CR}(i, j)$ regions are then merged over i to form larger $MN_{CR}(j)$ subcluster regions as outlined in (3.17).

$$
\begin{array}{cccc}
N_{CR}(1,1), & N_{CR}(1,2), & \ldots & ,N_{CR}(1,10) \\
\downarrow & \downarrow & \downarrow & \downarrow \\
N_{CR}(2,1), & N_{CR}(2,2), & \ldots & ,N_{CR}(1,10) \\
\vdots & \vdots & \ddots & \vdots \\
N_{CR}(N_{CPA},1), & N_{CR}(N_{CPA},2), & \ldots & ,N_{CR}(N_{CPA},10) \\
\downarrow & \downarrow & \downarrow & \downarrow \\
MN_{CR}(1), & MN_{CR}(2), & \ldots & ,MN_{CR}(10)
\end{array}
\tag{3.17}
$$

The newly formed $MN_{CR}(j)$ regions in (3.17) are then processed in the same manner as outlined in Section 3.7.3 and are used for fingerprint generation in the same manner as N_{CR} cluster regions for a single burst. Results were generated and are available for $N_{CPA} = 1, 3, 6, 9$; however, only results for $N_{CPA} = 1$ and $N_{CPA} = 9$ are discussed in Section 4.6.

3.10.2 Projection Point Averaging (PPA).

This section provides details on PPA as a second enhancement to the CB-DNA approach to provide increased performance for device discrimination, if needed. This method was previously considered in the Air Force Institute of Technology (AFIT) RFINT program and used here as a comparison to CPA.

The timing of PPA varies from that of CPA in that PPA takes place after the model has been developed according to Section 2.5 and occurs during the verification process. More specifically, PPA is accomplished during the verification process after the $N_{Tst} = 3,000$ fingerprints have been projected into the Fisher space and converted to P_j projected testing fingerprints, where $j = 1, 2, \ldots, N_{Tst}$. The set of $\{P_j\}$'s are then averaged according to the value of N_{PPA}, where $sum(P_{j \ldots j+N_{PPA}-1})/N_{PPA}$, results in a total number of $P_{Ave}(i)$, where $(i = 1, 2, \ldots, N_{Tst}/N_{PPA})$. The Euclidean

similarity measure is then applied to each of the averaged projections $P_{Ave}(i)$ and verification for authorized and rogue devices continues as outlined in Section 2.6. The results presented in Section 4.6 are based on $N_{PPA} = 1$ and $N_{PPA} = 5$.

3.11 Additional Verification Metrics

This section provides the relationship between metrics defined in Section 2.6 and used in Chapter IV and similar metrics used in [27, 28]. Work in [27, 28] uses a correlation based approach to exploit 10BASE-T Ethernet preambles and is most closely related to the research presented herein. The main difference in the approaches is that, here, CB-DNA discrimination is based on signal constellation features versus waveform correlation features. Additionally, direct access to network cards is required for the process in [27,28], whereas the CB-DNA approach developed here only requires access to the Ethernet cable. The metrics used for assessments in [27, 28] include Accuracy, Precision, Recall, and Specificity as described in [38]. Some of these metrics were highlighted as being of interest during peer reviews of this work. Thus, the additional metrics are summarized here for completeness and may aid readers who are unfamiliar with metrics commonly used in AFITs published RF-DNA works and adopted herein. The alternate metrics are based on the following type of network access attempts: 1) the total number of network access attempts by an authorized device results in either an Authorized Accept (AA) or Authorized Reject (AR), and 2) the total number of network access attempts by a rogue device results in either a Rogue Reject (RR), Rogue Accept (RA). For example, if authorized Device A attempted access to the network 25 times for a given period and it received a $AA = 20$ then the resultant $AR = 5$ over the same period. Similarly, if unauthorized Device B attempted to access to the network 25 times for a given period and received $RA = 5$ then the resultant $RR = 20$ over the same period.

Accuracy is defined in (3.18) with $Accuracy = 1$ for a particular device being desired and reflecting that 1) the device's $AR = 0$, and 2) no rogues were accepted using its credentials resulting in $RA = 0$.

Precision is defined in (3.19) and provides insight into how easily an authorized device's identity can be stolen and how often it is denied access. When $Precision = 1$ for a given device, $AR = 0$ (it is always granted access) however, the value of RR is unknown as (3.19) reduces to $RR/RR = 1$. When $Precision = 0$ device credentials are easily stolen and we have no insight into false verifications because the numerator is zero.

Recall is defined in (3.20) and is equivalent to what is calculated as RRR in Section 3.9.2. This metric characterizes the vulnerability for a given device to have its credentials stolen. When $Recall = 1$ for a given authorized device then any other unauthorized device trying to gain access as that authorized device is rejected such that $RA = 0$.

Specificity is defined in (3.21) and is equivalent to what is calculated as TVR in this work. This metric characterizes a particular devices ability to gain authorized network access as itself. For a device with $Specificity = 1$ it is always correctly granted network access.

$$Accuracy = \frac{RR + AA}{[(RA + RR) + (AA + AR)]} \tag{3.18}$$

$$Precision = \frac{RR}{(RR + AR)} \tag{3.19}$$

$$Recall = \frac{RR}{(RA + RR)} \tag{3.20}$$

$$Specificity = \frac{AA}{(AA + AR)} \tag{3.21}$$

Consistent with prior related RF-DNA works, RRR (*Recall*) and TVR (*Specificity*) are predominantly used here for verification performance assessments in Chapter 4. Given refereed paper feedback which suggest that *Accuracy* is the most "telling of the four additional metrics, *Accuracy* metrics are given some attention as well in Section 4.5.1 to assess CB-DNA device ID verification performance.

IV. Results

This chapter starts by providing some analysis results for the alignment jitter in Section 4.1, the Bit Error Rate (BER) assessment in Section 4.2, and the device chip-set analysis in Section 4.3, which are used to explain some of the classification and verification results in the latter sections. Results are then presented for *Device Classification* and *Device ID Verification* using Radio Frequency-Distinct Native Attribute (RF-DNA) and Constellation Based-Distinct Native Attribute (CB-DNA) device fingerprinting techniques based on the methodology described in Chapter III. The RF-DNA results were generated using a process adopted from previous related work [16, 51, 73] and implemented as described in Section 3.6. The CB-DNA results were generated using the process developed under this research and described in Section 3.7. Furthermore, comparative results are presented for RF-DNA and CB-DNA fingerprinting techniques using device fingerprints generated from the *same* collected emissions as described in Chapter III. The Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) results for *Device Classification* are based on a 1 vs. M "Looks Most Like?" assessment and are presented in Section 4.4 for both $N_C = 4$ and $N_C = 16$ authorized device class models. Results for *Device ID Verification* are based on 1 vs. 1 "Looks How Much Like?" assessment and are presented in Section 4.5 for $N_C = 12$ *Authorized* device class models and $N_R = 4$ *Rogue* devices as described in Section 3.9. Preliminary results for process enhancements are provided in Section 4.6 and demonstrate achievable improvement resulting from cross-burst 1) Constellation Point Accumulation (CPA), and 2) MDA/ML Projection Point Averaging (PPA). Lastly, a sensitivity analysis and probe placement comparison is accomplished in Section 4.7 by moving the probe-to-card location from $L_P \approx 2\ m$ to $L_P \approx 98\ m$.

4.1 Burst Alignment Jitter

This section discusses the alignment jitter for all devices for both Config #1 (oscope #1, cable #1 of length $L_C = 8\ m$) and Config #2 (oscope #2, cable #2 of length $L_C = 100\ m$). The alignment jitter A_j is defined as the number of samples between the max correlation point and the first peak in the preamble.

Table 4.1 shows the standard deviation on the number of samples between the S_{ROI} and the first peak in the alignment process. For the Config #1 listed in Table 4.1, relatively the same amount of jitter is present for all devices except M3:D3 from manufacturer TRENDnET. Config #2 with $L_P \approx 2\ m$ shows that the standard deviations are fairly consistent across all devices. When the collection probe is moved to the $L_P \approx 98\ m$ location in Config #2 the fine alignment jitter A_j varies considerably as seen in Table 4.1 with M3:D3 having the highest standard deviation.

The misalignment for device M3:D3 (Config #1) is explained with the help of Figure 4.1 where three signals are present to include: 1) the red dashed line (reference preamble), 2) the solid brown signal (M3:D2), and 3) the solid black signal (M3:D3). The S_{ROI} is denoted with a dashed vertical green line at index 1. The measured alignment jitter for device M3:D2 is shown with the aid of the brown double arrow which extends from the S_{ROI} to the vertical dashed brown line which represents the first maximum value of the aligned signal with $A_j = 3$. The measured alignment jitter for device M3:D3 is shown with the black double arrow which extends to the dashed black line representing the first maximum value of that aligned signal with $A_j = 21$. This phenomenon was discussed earlier in Section 3.1.1 and is caused by how signals are transmitted over the twisted pair. The effects of the alignment jitter A_j have a varying net positive effect on device classification for both RF-DNA and CB-DNA. As the N_R subregions for RF-DNA are increased, more features will be based on the misaligned subregion making it easier for MDA/ML to exploit the

Table 4.1. The Standard Deviation Associated with Fine Burst Alignment Between the Start of the ROI and the First Peak in the Aligned ROI.

Device ID	Config #1 $L_P = 2\ m$	Config #2 $L_P = 2\ m$	Config #2 $L_P = 98\ m$
M1:D1	1.2	1.2	42
M1:D2	1.2	1.2	56
M1:D3	1.2	1.2	52
M1:D4	1.2	1.2	49
M2:D1	1.4	1.3	28
M2:D2	1.5	1.3	64
M2:D3	1.5	1.3	23
M2:D4	1.6	1.3	65
M3:D1	1.2	1.2	69
M3:D2	1.2	1.2	75
M3:D3	10.6	1.2	698
M3:D4	1.2	1.2	35
M4:D1	1.1	1.1	117
M4:D2	1.1	1.1	108
M4:D3	1.1	1.1	125
M4:D4	1.1	1.1	364

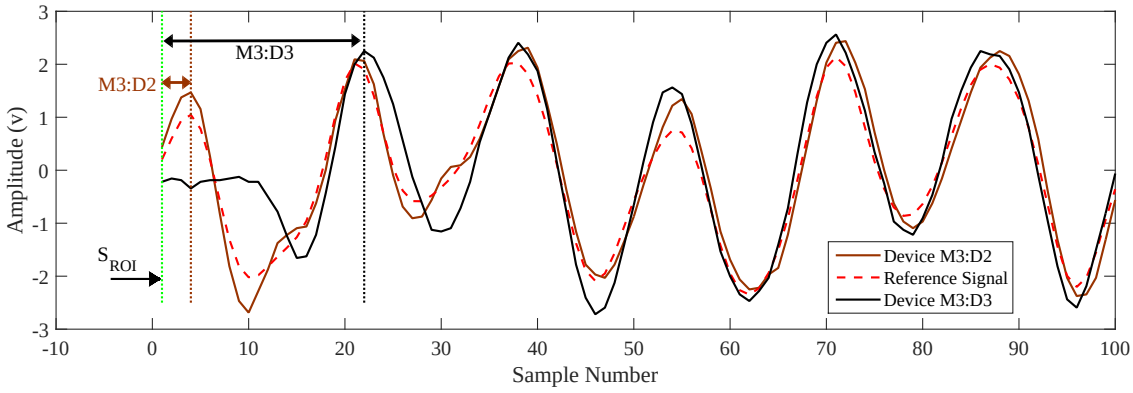


Figure 4.1. Illustration of alignment jitter showing how the maximum correlation point occurs before the ROI start.

affected statistics. The CB-DNA approach only has one projected symbol adversely affected by the misalignment resulting in a smaller net effect to CB-DNA fingerprints. Because of this disparity, RF-DNA has an advantage over CB-DNA for both *Device Classification* and *Device ID Verification*.

4.2 BER Assessment

The BER assessment provided in this section is based on $N_{sym} \approx 1.7$ billion collected symbols per manufacturer (pooled symbols from 4 cards). The BER results are presented in Table 4.2 where the Single Slope (SSLP) results were generated according to Section 3.4.1 [10] and Constellation Based (CB) results were generated according to Section 3.4.3 [11]. The overall BER for each method is approximately the same and on average experiences one bit error for every 1.34 M symbol estimates. The maximum size burst sent has $NB_{max} = 2280$ symbols and only one out of every 587 generated fingerprints would be affected on average based on current BER. One bit error would affect the proper placement of three points into the proper subcluster grouping. It is determined that this small error rate will have a negligible effect on CB-DNA fingerprint generation. The effects of an increased BER on fingerprint statistics is left for future work.

Table 4.2. Comparison of Card Manufacturer BER for Previous Single Slope (SSLP) Estimation Method in [10] and the 2D Constellation Point (CP) Method [11].

Manufacturer	# Processed Bits in Billions	# Bit Errors		BER	
		SSLP	CB	SSLP	CB
D-Link (M1)	1,733	21	18	1.21E-08	1.04E-08
Intel (M2)	1,739	845	845	4.86E-07	4.86E-07
TRENDnET (M3)	1,740	8	389	4.59E-09	2.23E-07
StarTech (M4)	1,737	1260	3478	7.25E-07	2.00E-06
Totals	**6,949**	**2971**	**5186**	**4.28E-07**	**7.46E-07**

4.3 Device Chip-set Analysis

The chip-sets for the $N_C = 16$ Device Under Test (DUT)s that were used in this research were examined for similarities in the specific components used to manufacture these devices. The four different manufacturers were used with four devices from each manufacturer; the results of the chip-set visual examination are provided in Table 4.3. It is evident from this table that M1 and M3 devices have the same LAN transformer markings. The LAN transformer is the last component that conditions the signal prior to it being transferred to the PHY medium. The effects of the common LAN transformer markings will be discussed as needed in the future sections.

Table 4.3. An Expansion of Table 3.1 to Highlight the Chip-Set Markings for the 16 Devices Under Test (DUT)s [11, 12].

Manufacturer	Reference	MAC Address Last Four	LAN Transformer Markings		
D-Link	M1:D1	D966	Bi-Tek	IM-1178LLF	1247I
	M1:D2	DA06	Bi-Tek	IM-1178LLF	1247I
	M1:D3	DA07	Bi-Tek	IM-1178LLF	1247I
	M1:D4	60E0	Bi-Tek	IM-1178LLF	1247I
Intel	M2:D1	1586	BI	HS00-06037LF	1247
	M2:D2	1A93	BI	HS00-06037LF	1247
	M2:D3	1A59	BI	HS00-06037LF	1247
	M2:D4	1A9E	BI	HS00-06037LF	1247
TRENDnET	M3:D1	9B55	Bi-Tek	IM-1178LLF	1247I
	M3:D2	9334	Bi-Tek	IM-1178LLF	1247I
	M3:D3	9B54	Bi-Tek	IM-1178LLF	1247I
	M3:D4	9B56	Bi-Tek	IM-1178LLF	1247I
StarTech	M4:D1	32CB	FPE	G24102MK	1250a1
	M4:D2	32B4	FPE	G24102MK	1250a1
	M4:D3	96F4	FPE	G24102MK	1320G1
	M4:D4	3048	FPE	G24102MK	1250a1

4.4 Device Classification

This section provides results for the 1 vs. M "Looks Most Like?" classification assessment. For the remainder of the document, comparison is aided by presenting CB-DNA results to the left of, or above, RF-DNA results.

Classification results are based on the MDA/ML process outlined in Section 3.8, where classification represents a comparison between one device versus many (specifically, 1 vs. M). MDA/ML results are presented here for both Cross-Model Discrimination (CMD) and Like-Model Discrimination (LMD) (serial number discrimination) using the $N_C = 16$ devices listed in Table 3.1. Device fingerprint generation occurs using *identical* burst emissions per methods in Section 3.6 for RF-DNA and Section 3.7 for CB-DNA, with RF-DNA using only the burst preamble and CB-DNA using the entire burst response.

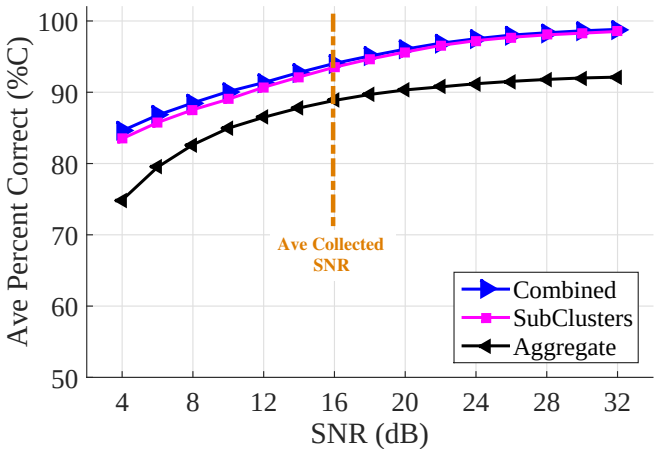
For classification assessments, a total of $N_{Col} = 1,000$ collected bursts ($N_{Tng} = 500$ for training and $N_{Tst} = 500$ for testing) are processed from each device with six like-filtered Additive White Gaussian Noise (AWGN) noise realizations added to each collected burst. This results in a total of $N_{Tng} = 500 \times 6 = 3,000$ training and $N_{Tst} = 500 \times 6 = 3,000$ testing fingerprints being used per device for classification training and testing assessments as described in Section 3.8. Two classification models are created, per Section 3.8, and used for discrimination assessment, with 1) CMD results being based on $N_{Tst} = 12,000$ testing fingerprints per device manufacturer, and 2) LMD results being based on $N_{Tst} = 3,000$ fingerprints per device. To stay consistent with prior related RF-DNA research, an arbitrary performance benchmark of $\%C = 90\%$ average cross-class correct classification performance is used for comparative assessment. Summary analysis and conclusions are based on $CI = 95\%$ binomial confidence intervals [44]. When results are presented for a large number of independent trials (e.g., Figure 4.2 and Figure 4.4), the resultant $CI = 95\%$ con-

fidence intervals are less than the vertical extent of data markers and omitted for visual clarity.

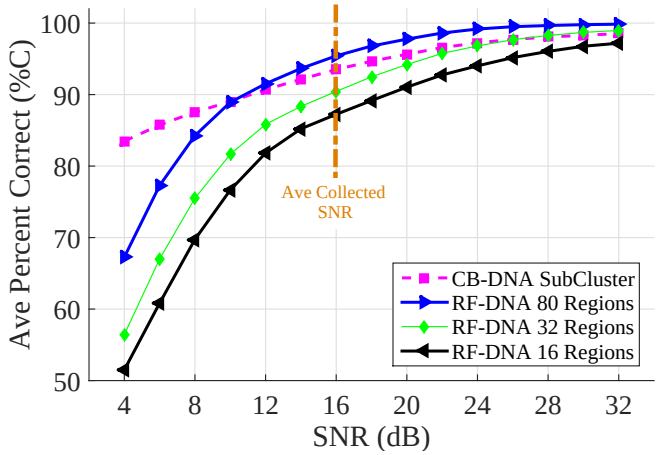
4.4.1 Cross-Model Discrimination (CMD).

Figure 4.2 shows average RF-DNA and CB-DNA classification performance for CMD discrimination. Results show that the $\%C = 90\%$ benchmark is achieved for both RF-DNA and CB-DNA at Signal-to-Noise Ratio $SNR \geq 12.0$ dB. However, RF-DNA requires $N_{Feat} = 720$ total features to achieve this. The CB-DNA approach achieves the benchmark utilizing only $N_{Feat} = 112$. With respect to CB-DNA $\%C$ results in Figure 4.2a, subclusters and combined fingerprints consistently outperform aggregated fingerprints by approximately 5% across all SNR values, where combined fingerprints consist of aggregate clusters and subclusters. With fingerprints generated from combined and subcluster regions having statistically the same performance in Figure 4.2a, only fingerprints based on subcluster points will be compared to RF-DNA; they consist of 28 less features relative to the number of features in combined fingerprints. Figure 4.2b provides RF-DNA performance and an overlay of CB-DNA subcluster results from Figure 4.2a. The RF-DNA results are equal or slightly better than CB-DNA results at $SNR = 10$ dB, but have worse performance at lower SNR values.

While CMD results in Figure 4.2 enable direct comparison of average cross-class $\%C$ performance for RF-DNA and CB-DNA Fingerprinting, they inherently hide class interaction and individual class performance. Individual class performance is more accurately analyzed using a conventional classification confusion matrix as described in Section 3.8. Confusion matrix results exist for all SNR in Figure 4.2 but are only presented here for two selected SNR to support general conclusions. The MDA/ML confusion matrices for CMD at $SNR = 12.0$ dB and $SNR = 30.0$ dB are presented in



(a) CB-DNA Fingerprinting $\%C$ vs. SNR for CMD using $N_C = 4$ Classes and $N_{CR} = 2$ Aggregate, 8 Subcluster, and 10 Combined Regions.



(b) RF-DNA Fingerprinting $\%C$ vs. SNR for CMD using $N_C = 4$ Classes and $N_R = 16$, 32, and 80 Subregions.

Figure 4.2. MDA/ML *Cross-Model Discrimination* (CMD) using (a) CB-DNA and (b) RF-DNA Fingerprinting [12].

Table 4.4 and Table 4.5, respectively. These matrices highlight correct classification (diagonal entries) and cross-class misclassification (off-diagonal entries) where matrix rows represent *Input Class* and matrix columns represent *Called Class*. The *Input Class* is defined as the ground truth for the input fingerprints. The *Called Class* is the results after classification. The table entries are presented as $\%C$ CB-DNA / $\%C$ RF-DNA with bold entries denoting best or equivalent performance.

CB-DNA CMD Fingerprinting benefits considerably with the introduction of subcluster DNA features. Improvement across the range of SNR considered includes an approximate: 1) 5% to 8% increase in $\%C$, and 2) 5 to 19 dB of "gain," measured as the reduction in required SNR relative to what is required for aggregate features to achieve the same $\%C$.

Historically, RF-DNA CMD *manufacturer* discrimination has been least challenging. Relative to best case RF-DNA performance, CB-DNA achieves 1) a marginally poorer 2% decrease in $\%C$ for $SNR > 12$ dB, and 2) up to 10% improvement in $\%C$ for $SNR < 12$ dB.

The CMD confusion matrices in Table 4.4 and Table 4.5 are nearly symmetric about the diagonal with *a majority* of the misclassification occurring between DLink (M1) and TRENDnET (M3) devices. This is attributable to DLink and TRENDnET devices using identical LAN transformers as indicated in Table 4.3. The diagonal correct classification entries show that CMD performance for both RF-DNA and CB-DNA are generally equivalent at each SNR presented. The resultant CMD averages for RF-DNA and CB-DNA are pursuant with Figure 4.2 at the corresponding SNR.

Table 4.4. Conventional CMD Classification Confusion Matrix (%) for $N_C = 4$ Classes at $SNR = 12$ dB [12]. Presented as %C CB-DNA / %C RF-DNA with Bold Entries Denoting Superior or Statistically Equivalent Performance.

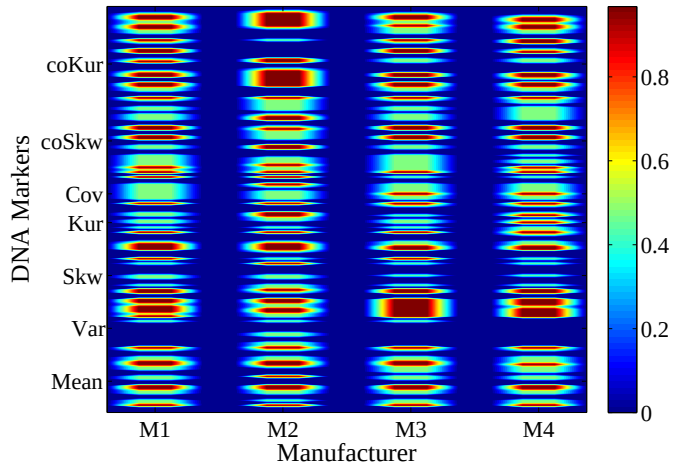
		Called Class			
		DLink	**Intel**	**TRENDnET**	**StarTech**
Input Class	**DLink**	83.76 / **87.30**	0.0 / 0.02	16.21 / 12.61	0.03 / 0.07
	Intel	0.0 / 0.03	**100 / 99.9**	0.0 / 0.07	0.0 / 0.0
	TRENDnET	18.31 / 20.98	0.0 /0.1	**81.67** / 78.92	0.02 / 0.0
	StarTech	0.0 / 0.02	0.0 / 0.0	0.0 / 0.03	**100 / 99.5**

The CMD DNA plots in Figure 4.3 were generated by averaging $N_{Tst} = 250$ fingerprints from each device within a given manufacturing group (a total of $N_{Tst} = 1,000$ fingerprints per manufacturer). The vertical DNA Marker (statistical features) shows

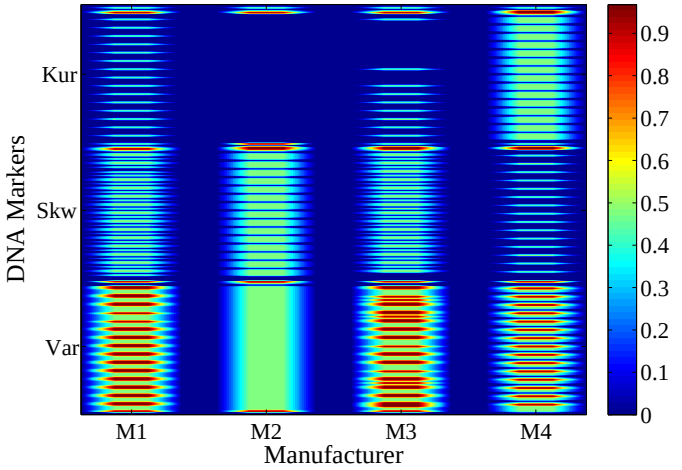
Table 4.5. Conventional CMD Classification Confusion Matrix (%) for $N_C = 4$ Classes at $SNR = 30$ dB [12]. Presented as %C CB-DNA / %C RF-DNA with Bold Entries Denoting Superior or Statistically Equivalent Performance.

		Called Class			
		DLink	**Intel**	**TRENDnET**	**StarTech**
Input Class	**DLink**	**97.11 / 99.50**	0.0 / 0.01	2.89 / 0.49	0.0 / 0.0
	Intel	0.0 / 0.0	**100 / 100**	0.0 / 0.0	0.0 / 0.0
	TRENDnET	2.63 / 0.38	0.0 /0.0	**97.37 / 99.62**	0.0 / 0.0
	StarTech	0.0 / 0.0	0.0 / 0.02	0.0 / 0.0	**100 / 99.98**

how device fingerprint features vary across the device fingerprints – note that the displayed value are normalized within each feature such that a maximum (red) value occurs for each statistic. The horizontal Manufacturer axis shows the device manufacturer identities in Table 3.1. Figure 4.3 provides a visual aide reflecting how device fingerprints generally differ. Of note here is that manufacturer M1 and M3 fingerprints appear mostly similar, with the greatest similarity reflected in the RF-DNA fingerprints. This is consistent with the higher level of cross-manufacturer misclassification occurring between M1 and M3 in the Table 4.4 and Table 4.5 confusion matrices.



(a) Average *CB-DNA* Features ($N_F = 140$)



(b) Average *RF-DNA* Features ($N_F = 720$)

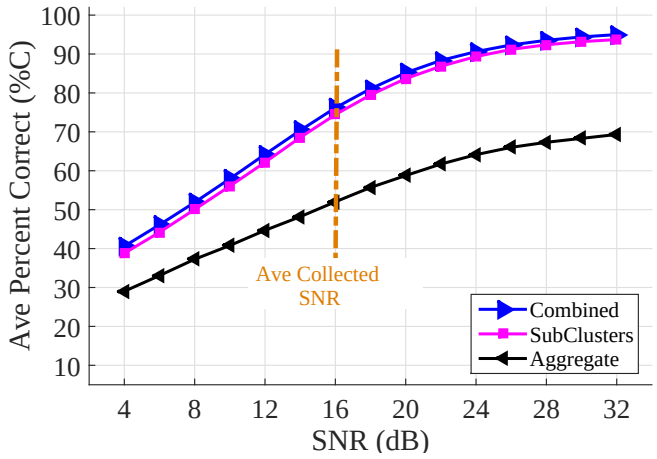
Figure 4.3. CMD CB-DNA and RF-DNA statistical fingerprint visualization with total number of features per fingerprint in parentheses.

4.4.2 Like-Model Discrimination (LMD).

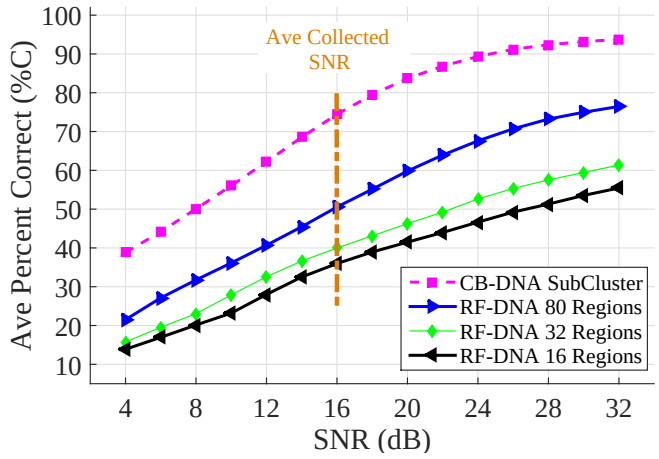
Historically, LMD has presented the greatest discrimination challenge for RF-DNA Fingerprinting given that the devices are assembled using identical components and may come off the assembly line in the same batch [16, 50]. LMD is also the most challenging case for CB-DNA when comparing the CMD results from Figure 4.2 with LMD results in Figure 4.4.

Average $\%C$ LMD results are presented in Figure 4.4 for RF-DNA and CB-DNA Fingerprinting. Results in Figure 4.4b show that the RF-DNA approach never achieves the $\%C = 90\%$ benchmark and yields maximum performance of $\%C \approx 78\%$ at $SNR = 32.0$ dB. The $\%C = 90\%$ performance benchmark is only achieved by CB-DNA for $SNR \geq 24.0$ dB for combined results and $SNR \geq 26.0$ dB for subcluster results.

The confidence interval $CI = 95\%$ contained within the data markers suggests that fingerprints based on combined and subcluster regions are statistically equivalent in Figure 4.4a. Therefore, as in the CMD case, comparisons with RF-DNA will be done with only subcluster regions at a reduced feature count of $N_{Feat} = 112$. The subcluster CB-DNA performance from Figure 4.4a is superimposed on RF-DNA performance results in Figure 4.4b for comparison. The comparison shows the best case RF-DNA performance ($N_R = 80$ regions) is $\%C \approx 78\%$ at $SNR = 32.0$ dB while CB-DNA reaches $\%C = 90\%$ at $SNR \approx 24.0$ dB. For the LMD case, RF-DNA is the inferior technique and is outperformed by CB-DNA by approximately 20% at the collected $SNR_C = 16.0$ dB.



(a) CB-DNA Fingerprinting $\%C$ vs. SNR for LMD using $N_C = 16$ Classes and $N_{CR} = 2$ Aggregate, 8 Subcluster, and 10 Combined Regions.



(b) RF-DNA Fingerprinting $\%C$ vs. SNR for LMD using $N_C = 16$ Classes and $N_R = 16$, 32, and 80 Subregions.

Figure 4.4. MDA/ML *Like-Model Discrimination* (LMD) using (a) CB-DNA and (b) RF-DNA Fingerprinting [12].

CB-DNA LMD Fingerprinting benefits considerably with the introduction of subcluster DNA features. Improvement across the range of SNR considered includes an approximate: 1) 5% to 22% increase in $\%C$, and 2) 5 to 19 dB of "gain," measured as the reduction in required SNR relative to what is required for aggregate features to achieve the same $\%C$.

Historically, RF-DNA LMD *serial number* discrimination has been most challenging. Relative to best case RF-DNA performance, CB-DNA is clearly superior and provides 1) nearly 22% of $\%C$ improvement at collected SNR=16 dB, and 2) 9 dB or more "gain" for $\%C \geq 70$, where gain is the reduction in SNR relative to what is required by RF-DNA to achieve the same $\%C$.

As with CMD results in Section 4.4.1, LMD results in Figure 4.4 do not enable direct comparison of average cross-class $\%C$ performance and inherently hide class interaction and individual class performance. Unlike CMD assessments which were based on $N_C = 4$ classes (manufacturers), LMD assessments were based on $N_C = 16$ classes (devices) with each class representing one of four devices from one of four manufacturers. Thus, a conventional LMD confusion matrix would generally contain 16 rows (one input class per row) and 16 columns (one called class per column). As an alternative, the $N_C = 16$ LMD class results are presented here using unconventional confusion matrices at $SNR = 12$ dB and $SNR = 30$ dB for consistency with previous CMD analysis. The unconventional confusion matrices are formed here by pooling results for all four classes (devices) within a given manufacturer, i.e., individual confusion matrix results for all classes (individual devices) for a given manufacturer are pooled into a manufacturer class and presented in a conventional 4-by-4 confusion matrix format. Table 4.6 and Table 4.7 show pooled LMD classification performance at $SNR = 12$ dB and $SNR = 30$ dB, respectively. In this case, diagonal entries represent that the device was correctly classified as belonging within its manufacturing group and off-diagonal terms represent all misclassifications attributable to the device being incorrectly associated with another manufacturer. The table entries are presented as $\%C$ CB-DNA / $\%C$ RF-DNA with bold entries denoting best or equivalent performance.

By comparison with prior CMD results in Table 4.4 ($SNR = 12$ dB) and Table 4.5 ($SNR = 30$ dB), the corresponding pooled LMD results in Table 4.6 and Table 4.7

Table 4.6. Unconventional Cross Manufacturer Classification Confusion Matrix (%) Based on LMD Results for $N_C = 16$ Classes at $SNR = 12$ dB [12]. Four Classes (Devices) Within Each Manufactured Pooled for Presentation. Presented as %C CB-DNA / %C RF-DNA with Bold Entries Denoting Superior or Statistically Equivalent Performance.

		Any Called Manufacturer			
		M1	**M2**	**M3**	**M4**
Any Input Manufacturer	**M1**	**84.07 / 81.61**	0.0 / 0.0	15.93 / 18.84	0.0 / 0.03
	M2	0.0 / 0.0	**100 / 99.99**	0.0 / 0.01	0.0 / 0.0
	M3	15.98 / 16.11	0.0 / 0.23	**84.02 / 83.89**	0.0 / 0.0
	M4	0.0 / 0.01	0.0 / 0.0	0.0 / 0.0	**100 / 99.99**

Table 4.7. Unconventional Cross Manufacturer Classification Confusion Matrix (%) Based on LMD Results for $N_C = 16$ Classes at $SNR = 30$ dB [12]. Four Classes (Devices) Within Each Manufactured Pooled for Presentation. Presented as %C CB-DNA / %C RF-DNA with Bold Entries Denoting Superior or Statistically Equivalent Performance.

		Any Called Manufacturer			
		M1	**M2**	**M3**	**M4**
Any Input Manufacturer	**M1**	**97.68 / 99.65**	0.0 / 0.0	2.32 / 0.35	0.0 / 0.0
	M2	0.0 / 0.0	**100 / 100**	0.0 / 0.0	0.0 / 0.0
	M3	1.69 / 0.25	0.0 / 0.0	**98.31 / 99.75**	0.0 / 0.0
	M4	0.0 / 0.0	0.0 / 0.0	0.0 / 0.0	**100 / 100**

reflect overall similar discrimination performance for both RF-DNA and CB-DNA Fingerprinting methods as the CMD results. This is consistent with expectations given that the misclassifications within the same manufacturing group are hidden within the diagonal entries of the confusion matrix.

The unconventional pooled confusion matrices in Table 4.6 and Table 4.7 do not show LMD misclassification occurring within the manufacturer groups. Thus, another unconventional confusion matrix representation is introduced to assess LMD performance within and across manufacturer groups. One such representation is provided in Table 4.8 and used to highlight like-manufacturer called class performance using all devices as input classes ($N_C = 16$). In this representation, the *Other Class* column

includes all results where input devices are misclassified as belonging to another manufacturer group (cross-manufacturer error). This confusion matrix representation is available for all SNR considered. However, representative results are presented here for $SNR = 26.0$ dB given that this is the lowest SNR at which CB-DNA performance in Figure 4.4a achieves the $\%C = 90\%$ benchmark. There are four miniature confusion matrices in Table 4.8 that represent the like-model confusion within a given manufacturer group. The four diagonal correct classification entries in Table 4.8 show that LMD performance for CB-DNA is statistically better than RF-DNA in all but one case (M3:D3) for the SNR presented. When excluding the M3:D3 case, the range of improvement of CB-DNA relative to RF-DNA is $\%C = 13\%$ to 52%. *Other Class* entries in Table 4.8 show that the only cross-manufacturer confusion occurs between DLink (M1) and TRENDnET (M3), which is also attributed to the fact that they have the same LAN transformer. As the table further shows, M2 and M4 only experienced misclassification within its own manufacturing group.

The high $\%C$ for device M3:D3 is attributable to the alignment jitter discussed in Section 4.1, where it was shown that Region of Interest (ROI) for this device had a higher standard deviation than the rest of the devices. With RF-DNA utilizing only the preamble, which is a much smaller ROI, the misalignment has a more positive impact on the RF-DNA results for this device. This would also affect the results for the CMD case. The positive effect on results will also be discussed in the verification section.

Figure 4.5 is used to visually show how similar/dissimilar like-model fingerprints are to one another and highlights the difficulty of the process when compared to CMD. The figure was generated by averaging 1,000 fingerprints from each device within manufacturer group M2 and was chosen because it had the highest %C of the 4 subtables when excluding M3 due to the alignment jitter in Table 4.8. Therefore,

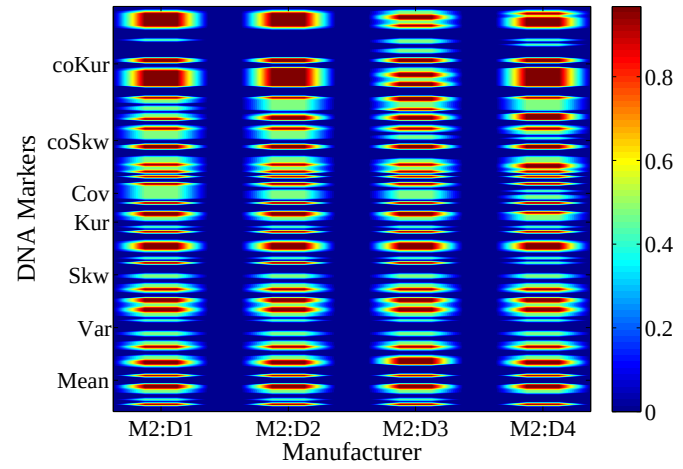
it should have the most dissimilar fingerprints. The Y-axis represents the location of a given statistic within a device fingerprint. The X-axis represents the device as described in Table 3.1.

Table 4.8. Unconventional LMD Classification Confusion Matrix Highlighting Like-Manufacture Confusion for $N_C = 16$ at $SNR = 26.0$ dB. Presented as %C CB-DNA / %C RF-DNA with Bold Entries Denoting Superior or Statistically Equivalent Performance [12].

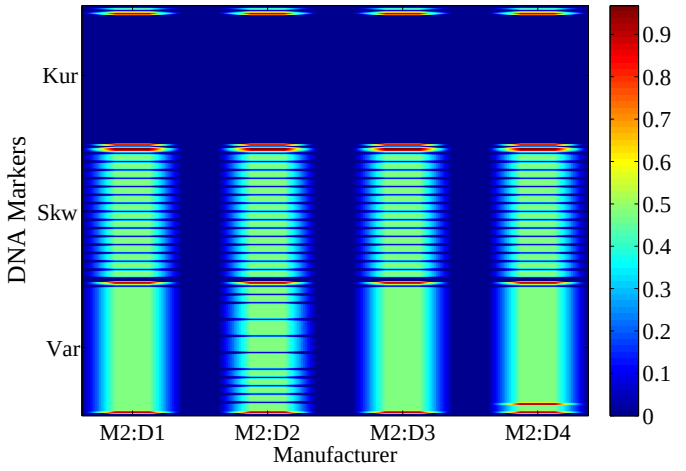
Input Class	Called Class				
	M1:D1	**M1:D2**	**M1:D3**	**M1:D4**	Other Class
M1:D1	**76.60** / 33.83	0.07 / 11.10	23.20 / 30.60	0.0 / 24.26	0.13 / 0.21
M1:D2	0.17 / 10.03	**95.57** / 70.10	2.20 / 8.23	0.87 / 9.63	1.19 / 2.01
M1:D3	9.90 / 9.13	0.83 /10.0	**87.97** / 57.17	0.53 / 22.70	0.77 / 1.0
M1:D4	0.37 / 7.40	1.17 / 13.70	0.70 / 25.13	**85.30** / 53.40	12.46/ 0.37
	M2:D1	**M2:D2**	**M2:D3**	**M2:D4**	Other Class
M2:D1	**91.63** / 86.53	3.97 / 6.40	3.03 / 1.37	0.70 / 1.17	0.0 / 0.0
M2:D2	5.27 / 6.70	**83.10** / 57.23	1.50 / 13.30	10.13/ 22.77	0.0 / 0.0
M2:D3	1.03 / 8.03	1.0 / 11.50	**97.73**/ 67.47	0.23/ 13.0	0.0 / 0.0
M2:D4	3.53/ 2.83	6.53/ 21.63	1.03 / 13.57	**88.90** / 61.97	0.0 / 0.0
	M3:D1	**M3:D2**	**M3:D3**	**M3:D4**	Other Class
M3:D1	**92.03** / 60.77	5.43 / 24.43	0.07 / 0.0	1.07 / 14.33	1.40/ 0.47
M3:D2	5.83 / 26.0	**91.10** / 59.57	0.17 / 0.0	2.10 / 13.60	0.08 / 0.83
M3:D3	0.03/ 0.0	0.13 / 0.0	**99.80 / 100**	0.0 / 0.0	0.04 / 0.0
M3:D4	2.26 / 11.87	1.93 / 9.80	0.0 / 0.0	**87.20** / 75.73	8.61 / 2.60
	M4:D1	**M4:D2**	**M4:D3**	**M4:D4**	Other Class
M4:D1	**83.50** / 71.93	3.80/ 0.33	4.60/ 5.84	8.10 / 21.90	0.0 / 0.0
M4:D2	2.90 / 1.33	**93.70** / 81.63	1.17 / 7.94	2.23 / 9.10	0.0 / 0.0
M4:D3	6.67/ 6.23	0.67/ 10.90	**87.37** / 73.20	5.30 / 9.67	0.0 / 0.0
M4:D4	3.37 / 11.17	3.13 / 8.43	5.40 / 9.43	**88.10** / 70.97	0.0 / 0.0

4.5 Device ID Verification

This section provides results for the 1 vs. 1 a "Look How Much Like?" verification assessments. As stated in Section 3.9, 256 different permutations for $N_A = 12$ autho-



(a) Average *CB-DNA* Features ($N_F = 140$)



(b) Average *RF-DNA* Features ($N_F = 720$)

Figure 4.5. LMD CB-DNA and RF-DNA statistical fingerprint visualization with total number of features per fingerprint in parentheses.

rized devices and $N_R = 4$ were created from the $N_C = 16$ devices in Table 4.3 with representative permutations provided in Table 3.3. Specific results are provided for Perm #29 to guide the discussion on ROC generation and raw test statistic presentation for both authorized and rogue devices. Perm #29 was chosen because it had the highest $\%C$ of the permutations listed in Table 3.3.

Euclidean distance was chosen as the similarity measure for device verification. The verification results presented in this section use only like-model verification and

utilize a total of $N_{Feat} = 140$ CB-DNA and $N_{Feat} = 720$ RF-DNA features per fingerprint but are available for fingerprints based on a reduced number of features. True Verification Rate (TVR) and False Verification Rate (FVR) for Authorized devices as described in Section 3.9 is based on $N_{Tst} = 3,000$ fingerprints per device. Rogue Accept Rate (RAR) and Rogue Reject Rate (RRR) for Rogue Devices are based on $N_{Tst} = 6,000$ fingerprints.

Verification is assessed using two network access methods, including 1) ROC curves for making *Binary Grant/Deny* (BGD) decisions using test statistic PMFs, and 2) stem plots of raw Euclidean distance test statistics (Z_V) for making Burst-by-Burst (BbB) decisions.

Assessment of Binary Grant/Deny (BGD) verification performance is accomplished using ROC curves, which are generated for authorized and rogue devices as TVR vs. FVR and TVR vs. RAR, respectively. The TVR vs. RAR presentation is a matter of convenience and enables 1) direct assessment of rogue performance for a given authorized device TVR (vertical displacement in Figure 4.6 and Figure 4.8 are identical), and 2) easy calculation of RRR=1-RAR in Figure 4.8. The PMFs used to generate Figures 4.6 and 4.8 ROCs are based on independent Z_V generated per Section 3.9 and include a total of $N_{Tst} = 3,000$ and $N_{Tst} = 6,000$ fingerprints per authorized and rogue device, respectively.

For ROC curves in Figure 4.6, BGD *success* is based on arbitrarily defined criteria, to stay consistent with other RF-DNA works, such that *Authorized Device* verification criteria is $TVR > 0.9$ and $FVR < 0.1$. The Authorized Accept Rate (AAR) metric is common to the TVR metric presented in previous RF-DNA publications as being the number of authorized access attempts satisfying this criteria divided by the total number of attempts for a given permutation [49, 50]. The common $TVR > 0.9$ benchmark is shown as a horizontal dotted line in Figure 4.6, with curves for successful

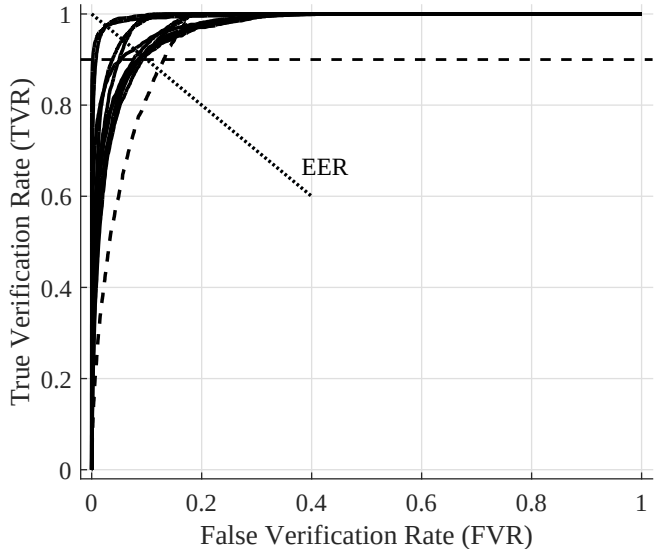
attempts denoted by solid lines and failures denoted by dashed curves.

The RF-DNA and CB-DNA ID verification authorized device ROC curves are displayed in Figure 4.6 for Perm #29 in Table 3.3 at $SNR = 20.0$ dB. The dashed ROC curves in Figure 4.6b for RF-DNA show that only five of the $N_A = 12$ authorized devices meet the arbitrary $TVR > 0.9$ and $FVR < 0.1$ criteria and are not granted network access ($AAR = 41.7\%$). In addition, there is one device in Figure 4.6b in the upper left corner; it is the M3:D3 device that had the higher alignment jitter. The solid ROC curves in Figure 4.6a for CB-DNA show that all but one of the $N_A = 12$ authorized devices meet or exceed the arbitrary $TVR < 0.9$ and $FVR < 0.1$ criteria and are granted network access ($AAR = 91.7\%$). The $t_V(d)$ verification threshold values are set according to the Equal Error Rate (EER) line in Figure 4.6.

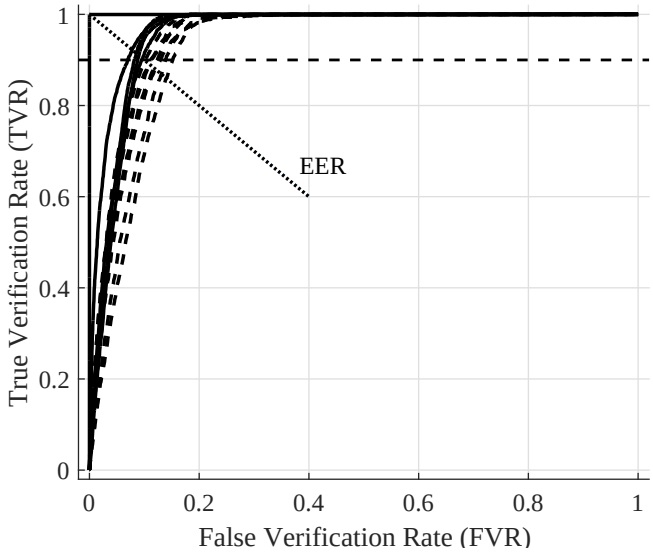
The BbB verification process for authorized devices is illustrated in Figure 4.7 which shows $N_{Tst} = 3,000$ Euclidean distance Z_V from all authorized devices (A1–A12). The device dependent verification thresholds $t_V(d)$ are indicated by a solid black horizontal line and correspond to EER operating points in Figure 4.6 ROC curves. The blue circles below the threshold value are device access attempts where the device was correctly granted network access and the red X's denote an erroneous rejection for that device.

For BbB verification assessment, TVR for the d^{th} authorized device is calculated as the number of $Z_V(d) \leq t_V(d)$ divided by the total number of $Z_V(d)$ with the percentages for each device being displayed in Table 4.9 along with the verification thresholds $t_V(d)$ for each device. The TVR for RF-DNA in Table 4.9 are $84.8\% \leq TVR \leq 100\%$ and CB-DNA are $88.4\% \leq TVR \leq 97.8\%$. Again, it is seen that M3:D3 (A9) is has the highest TVR due to the alignment jitter.

In the rogue device ROC curves in Figure 4.8, BGD *success* is based on arbitrarily defined criteria for *Rogue Device* verification of $TVR > 0.9$ and $RAR < 0.1$, with

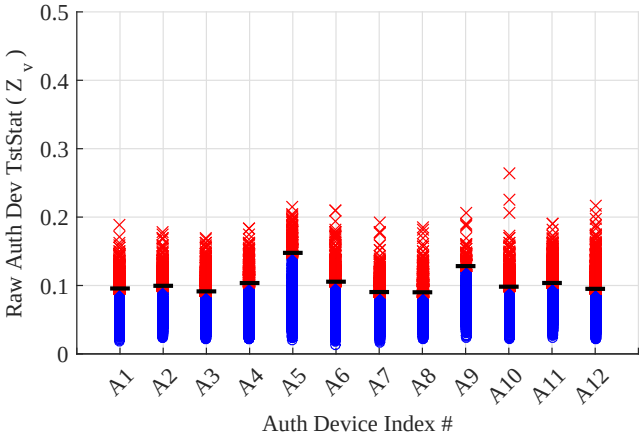


(a) CB-DNA

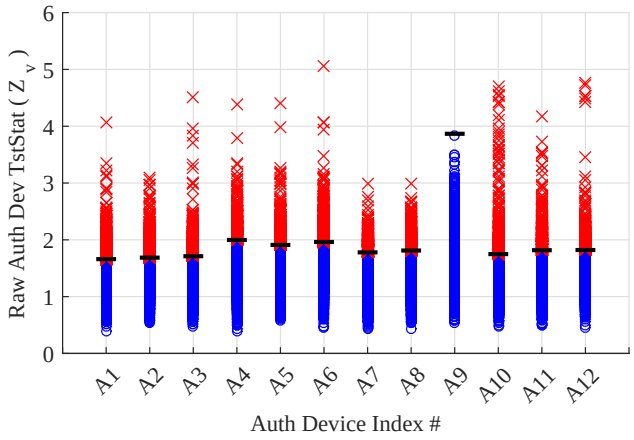


(b) RF-DNA

Figure 4.6. ID Verification ROC curves for Perm #29 at $SNR = 20$ dB using a Euclidean distance measure of similarity. Relative to Binary Grant/Deny (BGD) network access decisions CB-DNA authorized device success is $AAR = 91.7\%$ (11/12) and RF-DNA $AAR = 41.7\%$ (5/12) for $TVR > 0.9$ and $FVR < 0.1$ criteria.



(a) CB-DNA



(b) RF-DNA

Figure 4.7. Euclidean distance test statistics for Perm #29 devices at $SNR = 20$ dB. Solid horizontal lines are device dependent $t_V(d)$ thresholds corresponding to ROC EER in Figure 4.6. Authorized device (A1–A12) ID verification test statistics where blue circles indicate correct access granted and red X's indicate an incorrect access denied for N_{Tst}=3,000 testing fingerprints per authorized device.

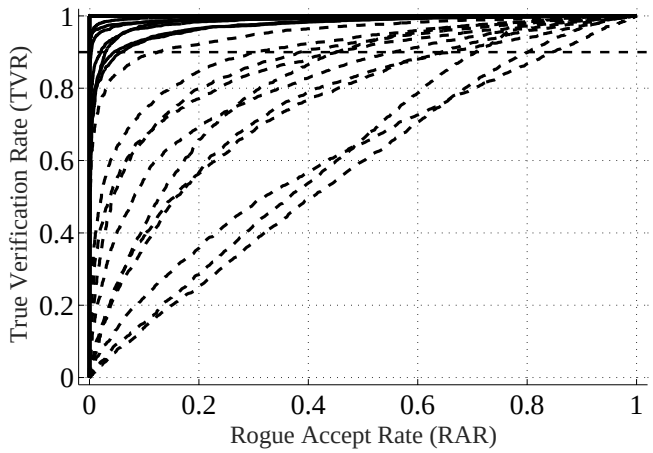
Table 4.9. CB-DNA and RF-DNA Authorized Device Dependent $T_V(d)$ Threshold and TVR Values for Perm #29 at $SNR = 20$ dB Corresponding to Figure 4.7 with Bold Entries Denoting Better Performance for TVR Results. Device Dependent $t_V(d)$ Thresholds Corresponding to ROC EER in Figure 4.6.

		Authorized Device Index (A#)											
		A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
CB-DNA	TVR	90.4	90.7	89.4	93.1	97.1	94.3	91.5	90.6	97.8	91.0	88.4	86.7
	$T_V(d)$	0.10	0.10	0.09	0.10	0.15	0.11	0.09	0.09	0.13	0.10	0.10	0.10
RF-DNA	TVR	85.4	85.2	84.8	91.4	87.5	86.6	89.3	89.4	100	86.2	85.7	86.9
	$T_V(d)$	1.66	1.69	1.71	2.00	1.91	1.96	1.78	1.81	3.87	1.75	1.82	1.82

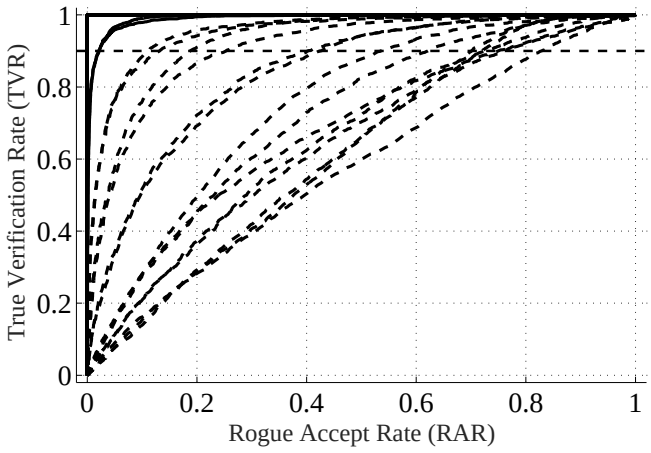
RRR being the number of rogue access attempts satisfying this criteria divided by the total number of attempts. The common $TVR > 0.9$ benchmark is shown as a horizontal dotted line and is the same as Figure 4.6, with curves for successful rejections denoted by solid lines and dashed curves denote when access is wrongly granted.

Rogue device ROC curves for RF-DNA and CB-DNA ID verification are provided in Figure 4.8 using Perm #29 devices in Table 3.3 at $SNR = 20.0$ dB. The solid RF-DNA ROC curves in Figure 4.8b show that $RRR = 34/48$ rogue device attempts met the $TVR > 0.9$ and $RAR < 0.1$ criteria and were successfully rejected (denied network access) at $RRR = 70\%$. The solid CB-DNA ROC curves in Figure 4.8a show that $RRR = 37/48$ rogue device attempts met the $TVR > 0.9$ and $RAR < 0.1$ criteria and were successfully rejected (denied network access) at $RRR = 77\%$. CB-DNA is marginally better and improved RRR by 7% over RF-DNA.

The BbB verification process for rogue devices is illustrated in Figure 4.9, which shows $N_{Tst} = 6,000$ Euclidean distance Z_V per Perm #29. There were a total of 48 rogue assessment scenarios for this permutation. For visual clarity, only results for 12 of the scenarios are presented and results for only $N_{R(3)} = R3$ are presented as falsely claiming each of the authorized device IDs (R3:A1, R3:A2,. . . , R3:A12) in Figure 4.7. The authorized devices $t_V(d)$ correspond to those in Table 4.10 and are used to make



(a) CB-DNA

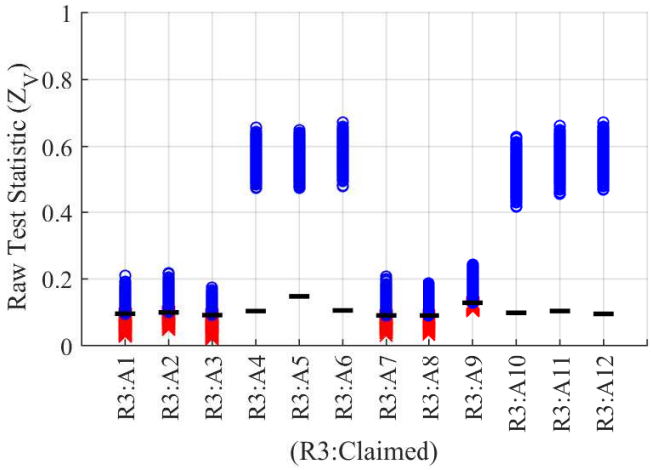


(b) RF-DNA

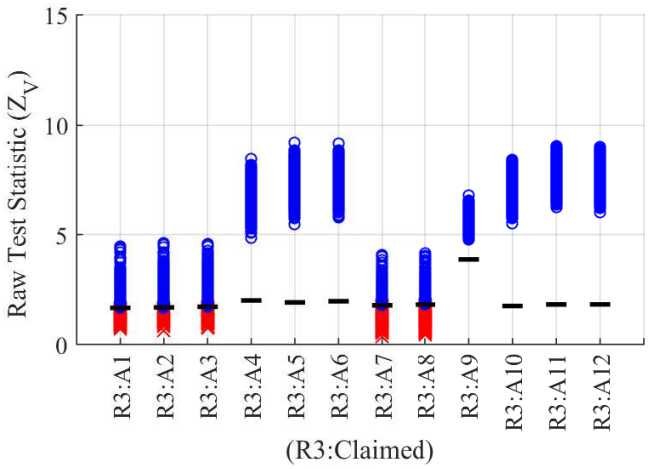
Figure 4.8. Rogue device ID verification ROC curves for Perm #29 in Table 3.3 at $SNR = 20$ dB using a Euclidean distance measure of similarity. Relative to Binary Grant/Deny (BGD) network access decisions CB-DNA rogue device R3 rejection is $RRR = 77\%$ (37/48) and RF-DNA $RRR = 70\%$ (34/48) for $TVR > 0.9$ and $RAR < 0.1$ criteria.

BbB grant/deny decisions.

The blue circles above the $t_V(d)$ threshold are rogue device rejections where the rogue device is correctly denied network access. The red X's below $t_V(d)$ are rogue device acceptances where the rogue is errantly granted network access. In this case, RRR for d^{th} claimed ID is calculated as the number of $Z_V(d) > t_V(d)$ divided by the total number of $Z_V(d)$. The $t_V(d)$ used for the rogue assessment are in Table 4.10 for RF-DNA and CB-DNA. Table 4.10 also provides RRR values for RF-DNA from



(a) CB-DNA



(b) RF-DNA

Figure 4.9. Euclidean distance test statistics for Perm #29 rogue devices at $SNR = 20$ dB. Solid horizontal lines are device dependent $t_V(d)$ thresholds corresponding to ROC EER in Figure 4.6. Rogue device (R3) verification test statistics where blue circles denote a rogue device being correctly denied access and red X's denote an incorrect grant access decision for $N_{Tst} = 6,000$ BbB testing fingerprints, with R3 presenting a false ID for each authorized device (R3:A1–R3:A12).

Table 4.10. CB-DNA and RF-DNA Device Dependent $T_V(d)$ Threshold and RRR Values for Perm #29 at $SNR = 20$ dB Corresponding to Figure 4.9 with Bold Entries Denoting Better or Equal Performance for RRR Results. Device Dependent $t_V(d)$ Thresholds Corresponding to ROC EER in Figure 4.6.

	CB-DNA		RF-DNA	
Rogue : Claimed	RRR	$T_V(d)$	RRR	$T_V(d)$
R3:A1	42.0	0.096	**78.6**	1.660
R3:A2	79.9	0.100	**91.0**	1.686
R3:A3	14.7	0.091	**90.2**	1.711
R3:A4	**100**	0.104	**100**	1.998
R3:A5	**100**	0.148	**100**	1.910
R3:A6	**100**	0.106	**100**	1.962
R3:A7	**67.1**	0.090	24.8	1.779
R3:A8	**52.4**	0.090	22.7	1.812
R3:A9	96.8	0.128	**100**	3.867
R3:A10	**100**	0.098	**100**	1.749
R3:A11	**100**	0.104	**100**	1.817
R3:A12	**100**	0.095	**100**	1.821

$22.7\% \leq RRR \leq 100\%$ and CB-DNA ranging from $14.7\% \leq RRR \leq 100\%$. For RF-DNA and CB-DNA, it is clear in Figure 4.9 that R3 (an M3 device) is least similar to A4, A5, and A6 (M2 devices) and A10, A11, and A12 (M4 devices) given the corresponding Z_V are well above $t_V(d)$ for those devices. It is also evident that when the rogue device was granted access it was thought to be either an M1 or M3 manufacturer. There is one exception in Figure 4.9 for R3:A9 in that R3 was rejected every time for RF-DNA but gained network access 3.2% of time for CB-DNA. These results again show that the misalignment jitter impacts both RF-DNA and CB-DNA however the impact to RF-DNA is higher.

RF-DNA and CB-DNA results in Table 4.11 and Table 4.12 are presented as (#Successes / Total #Trials)×100 with bold entries denoting best or equivalent performance. For binary results, AAR is based on $N_A = 12$ authorized devices trials and

RRR is based on $(N_A = 12) \times (N_R = 4) = 48$ total trials. The BbB results are based on $(N_A = 12) \times (N_R = 4) \times (N_{Tst} = 6,000) = 288,000$ trials.

Table 4.11. Perm #29 Device ID Verification Performance: Binary Grant/Deny (BGD) Authorized Accept Rate (*AAR*) (12 attempts per *SNR*) and Rogue Reject Rate (*RRR*) for BGD (48 Attempts per *SNR*) and Burst-By-Burst (BbB) (288,000 Attempts per *SNR*) Assessments.

	CB-DNA			**RF-DNA**		
SNR (dB)	**BGD**		**BbB**	**BGD**		**BbB**
	AAR(%)	***RRR(%)***	***RRR(%)***	***AAR(%)***	***RRR(%)***	***RRR(%)***
8	**0**	**62.5**	**77.1**	**0**	60.4	74.8
10	0	62.5	**78.3**	**8.3**	**66.7**	76.5
12	**16.7**	62.5	**79.7**	8.3	**66.7**	78.2
14	**33.3**	64.6	**82.2**	8.3	**66.7**	80.0
16	**33.3**	**66.7**	**84.0**	8.3	**66.7**	82.0
18	**50.0**	**72.9**	**85.1**	25.0	70.8	83.8
20	**91.7**	**77.1**	**86.2**	41.7	70.8	85.4
22	**91.7**	**79.2**	**87.3**	58.3	75.0	86.5
24	**100**	**79.2**	**88.1**	75.0	**79.2**	87.3
26	**100**	**83.3**	**88.8**	83.3	79.2	87.8
28	**100**	**85.4**	**89.3**	91.7	79.2	88.5

Table 4.11 presents Perm #29 results for all SNR considered and highlights the direct relationship between SNR and the AAR and RRR for both RF-DNA and CB-DNA. In addition, Table 4.11 shows that $SNR = 24.0$ dB is the lowest SNR at which $AAR = 100\%$ for authorized devices. It is also evident in Table 4.11 that the BbB method consistently outperforms the binary accept/reject decision for both fingerprinting methods at all SNR. As indicted by bold entries in Table 4.11, RF-DNA results are inferior to CB-DNA for most SNR. The best BGD decision for RF-DNA is $RRR = 79.2\%$ at $SNR = 24.0$ dB, which is exceeded by CB-DNA at $SNR = 26.0$ dB. The confidence interval for these results was calculated to be $\pm 0.1\%$ with 95% confidence.

Table 4.12 provides results for the 10 Perms listed in Table 3.3 and the average

overall 12,288 rogue scenarios at $SNR = 20.0$ dB. This SNR is highlighted to stay consistent with the other results presented in this section. Binary Grant/Deny Access results collectively include $70\% < RRR < 79\%$ for RF-DNA and $72\% < RRR < 79\%$ for CB-DNA. Burst-by-Burst results jointly include $82\% < RRR < 88\%$ for RF-DNA and $82\% < RRR < 89\%$ for CB-DNA. As indicated by the bold entries, RF-DNA results are generally poorer than CB-DNA. Also of interest is that for the 10 Perms in Table 4.12, the permutations yielding highest RRR had correspondingly poorer %C than the permutations yielding lowest RRR – reflecting no direct relationship between classification and verification performance for both approaches.

Table 4.12. Device ID Verification Performance for 10 Selected Permutations at $SNR = 20$ dB for Binary Grant/Deny (BGD) AAR (12 attempts per Permutation), *RRR* (48 Attempts per Permutation) and Burst-By-Burst (BbB) *RRR* (288,000 Attempts per Permutation). All Permutations Averages Provided for BGD *RRR* (12,288 Attempts) and BbB *RRR* (Over 73,000,000 Attempts).

		CB-DNA			**RF-DNA**		
		BGD		**BbB**	**BGD**		**BbB**
	Perm#	***AAR(%)***	***RRR(%)***	***RRR(%)***	***AAR(%)***	***RRR(%)***	***RRR(%)***
Lowest %C	74	**33.3**	72.9	86.6	16.7	**79.2**	**87.9**
	105	**25.0**	75	**89.9**	8.3	79.2	88.1
	106	**25.0**	72.9	**89.6**	**25.0**	**79.2**	86.4
	107	**41.7**	72.9	**88.9**	25.0	**79.2**	86.4
	108	**41.7**	75.0	**88.4**	33.3	**79.2**	86.0
Highest %C	29	**91.7**	**77.1**	**86.2**	41.7	70.8	**85.4**
	32	**100**	**79.1**	**85.0**	66.7	70.8	83.3
	157	**91.7**	**72.9**	**84.7**	41.7	70.8	**84.5**
	159	**100**	**70.8**	**83.1**	50	**70.8**	**82.7**
	160	**91.7**	**72.9**	**82.5**	58.3	70.8	**82.3**
All Perms		**70.0**	72.4	**85.5**	42.6	75.1	**85.0**

The "All Perms" row in Table 4.12 shows that CB-DNA outperforms RF-DNA with average RRR of 72.4% and 85.5% for BGD and BbB, respectively. The improvement is $\approx 3\%$ for BGD and $\approx 1.5\%$ for BbB access decisions.

4.5.1 Alternate Verification Performance Metrics.

This section presents results using alternate verification metrics commonly employed in machine learning applications [38]. These metrics provide insight into individual device performance and are covered here for two purposes: 1) to enable comparison with other constellation-based works and results as found in [27, 28], and 2) to bridge the gap for researchers accustomed to different metrics. As introduced in Section 3.11, the alternate metrics include *Accuracy*, *Precision*, *Recall*, and *Specificity*. The results are only provided for CB-DNA as it has demonstrated superior performance to RF-DNA.

Numerical results are available for all four metrics. However, the focus of discussion here is on *Accuracy*. Refereed paper feedback suggests that this is the most "telling of the four metrics." The *Accuracy* metric for a given device reflects: 1) how reliably the device ID is self-validated and how network access is rightly granted (akin to TVR), and 2) how resistant the devices ID is to cross-validation error, whereby its credentials are stolen and used by a rogue device to wrongly gain network access (akin to RAR). Thus, an $Accuracy = 1$ for a particular device is desired and reflects that: 1) the device is appropriately granted access 100% of the time, and 2) rogues presenting its credentials are denied access 100% of the time.

Figure 4.10 and Table 4.13 contain information specific to Perm #29 and device $N_A = A2$ (M1:D3), which are used to link the effects of SNR on the accuracy metric and how it is related to traditional rogue Receiver Operating Characteristic (ROC) curves. The rogue ROC curves in Figure 4.10 contain a total of 8 rogue ROC curves with four for each of the two presented SNR values. Five of the eight curves are in the upper left hand corner and not visible suggesting at or near $RRR = 100\%$ while also achieving at or near $TVR = 100\%$. The EER line represents the chosen operating point.

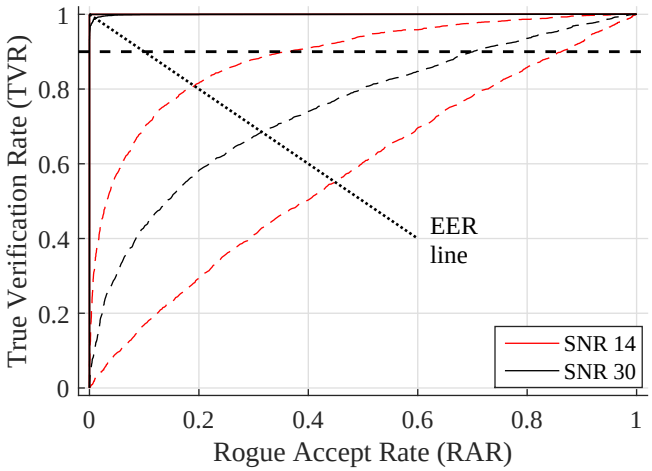


Figure 4.10. TVR and RAR for Device M1:M3 at $SNR = 14, 30$ dB. RAR shown for all rouge devices $N_R(i)$ = R1-R4.

Table 4.13 provides accuracy results across $N_A = 12$ devices for Perm #29 and highlights the effects of SNR variation on accuracy. The bold entries in this table correspond to the ROC curves in Figure 4.10 by accounting for all of the ROC curves for a given SNR value. More succinctly, an individual ROC curve provides metrics for network access attempts by a individual rogue device against one authorized device, whereas the accuracy metric accounts for all network access attempts across all rogue devices against one authorized device.

Table 4.13. Perm #29 Accuracy Performance for a Given Device with Each Metric based on 27,000 Tests per Device.

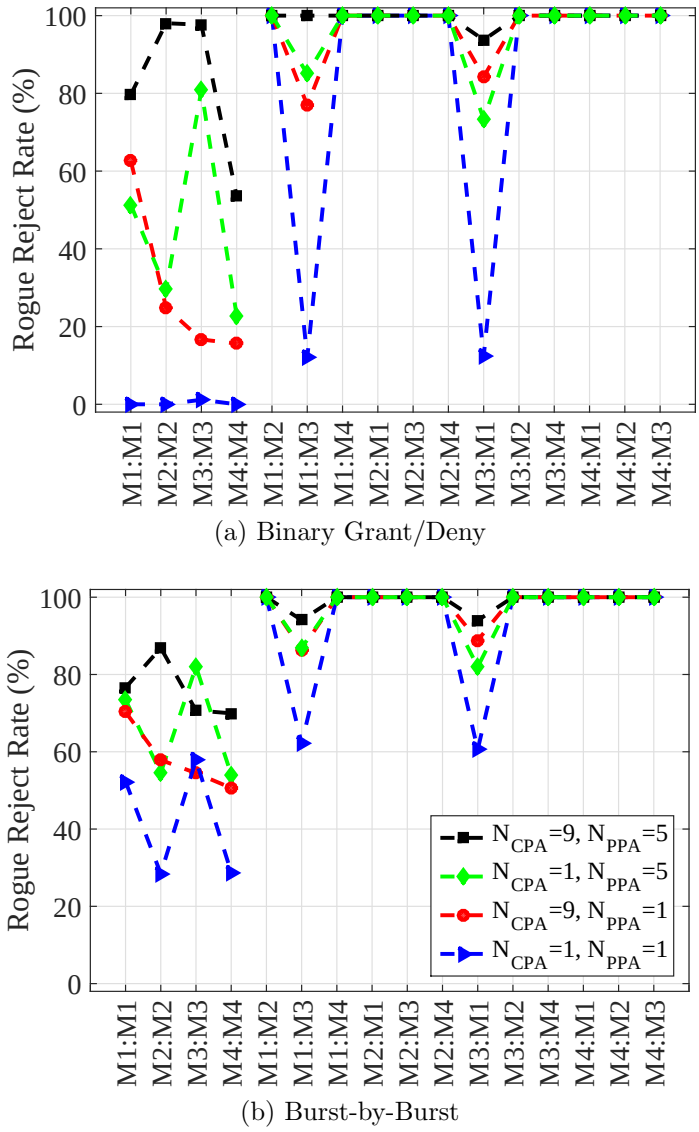
	SNR										
Device	10	12	14	16	18	20	22	24	26	28	30
M1:D2	0.731	0.763	0.807	0.836	0.843	0.856	0.867	0.886	0.911	0.927	0.935
M1:D3	0.735	0.739	**0.761**	0.770	0.773	0.782	0.799	0.809	0.815	0.817	**0.820**
M1:D4	0.735	0.735	0.758	0.767	0.777	0.784	0.788	0.789	0.789	0.790	0.790
M2:D1	0.795	0.797	0.801	0.804	0.807	0.811	0.820	0.826	0.833	0.836	0.836
M2:D3	0.842	0.872	0.904	0.937	0.959	0.974	0.984	0.988	0.990	0.991	0.991
M2:D4	0.798	0.799	0.801	0.803	0.803	0.805	0.804	0.804	0.801	0.801	0.800
M3:D1	0.779	0.792	0.822	0.852	0.880	0.905	0.924	0.941	0.953	0.962	0.967
M3:D2	0.777	0.778	0.819	0.850	0.866	0.883	0.908	0.926	0.945	0.955	0.967
M3:D3	0.819	0.858	0.911	0.947	0.973	0.988	0.996	0.998	0.999	0.999	0.999
M4:D2	0.837	0.855	0.869	0.875	0.882	0.892	0.909	0.923	0.934	0.948	0.958
M4:D3	0.804	0.817	0.829	0.839	0.845	0.856	0.863	0.864	0.870	0.875	0.877
M4:D4	0.808	0.826	0.842	0.861	0.871	0.883	0.891	0.897	0.901	0.905	0.908
Mean	**0.776**	**0.788**	**0.803**	**0.827**	**0.845**	**0.857**	**0.868**	**0.880**	**0.888**	**0.895**	**0.901**

4.6 CPA and PPA Enhancements

This section provides results for performance enhancements that include: 1) the pre-fingerprint generation CPA process developed under this research and described in Section 3.10.1, and 2) the post-MDA/ML PPA process adopted from prior research and described in Section 3.10.2. The goal is to improve overall device ID verification performance using CB-DNA. Results are presented for four different parameter values, including: 1)$N_{CPA} = 1$ representing no accumulation and $N_{CPA} = 9$ representing accumulation of constellation points from symbols in nine bursts, and 2) $N_{PPA} = 1$ representing no projection averaging, and $N_{PPA} = 5$ representing the averaging of five projection bursts in MDA/ML projection space.

Figure 4.11 provides four different *RRR* assessments for BGD and BbB decisions, with the blue triangles representing *No Enhancement* ($N_{CPA} = 1$ and $N_{PPA} = 1$), the red circles representing *CPA-Only Enhancement* ($N_{CPA} = 9$ and $N_{PPA} = 1$), the green diamonds representing *PPA-Only Enhancement* (N_{CPA}=1 and $N_{PPA} = 5$), and the black squares representing *Combined Enhancement* ($N_{CPA} = 9$ and $N_{PPA} = 5$). The vertical axis is $RRR(\%)$ and the horizontal axis is presented as Rogue Manufacturer ID:Claimed Manufacturer ID (M#:M#). For example, the first horizontal entry in Figure 3.21 is M1:M1 that represents all the times that a rogue device from manufacturing group M1 attempted to gain access as one of the other three authorized M1 devices. The results in Figure 4.11a, under BGD, are based on $(N_A = 3) \times (N_{Perms} = 256) \times (N_R = 1) = 768$ individual binary tests for all cases. Figure 4.11b under BbB results are composed of $(N_A = 3) \times (N_{Perms} = 256) \times (N_R = 1) \times (N_{Tst} = 6,000) \approx 4.6M$ raw test statistic comparisons with no PPA $(N_{PPA} = 1)$ and $(N_A = 3) \times (N_{Perms} = 256) \times (N_R = 1) \times (N_{Tst} = 6,000/5) \approx 92K$ raw test statistic with PPA $(N_{PPA} = 5)$ for each M#:M# in the x-axis.

The first four M#:M# entries in the horizontal axis of the individual subfigures



(a) Binary Grant/Deny

(b) Burst-by-Burst

Figure 4.11. Constellation Point Accumulation (CPA) and MDA/ML Projection Point Averaging (PPA) results. Average *RRR* presented as rogue manufacturer (M#) : claimed manufacturer (M#) for Binary Grant/Deny (BGD) and Burst-by-Burst (BbB) decisions across 256 permutations at *SNR* = 14. Results for no CPA (N_{CPA}=1) and no PPA (N_{PPA}=1), CPA ONLY (N_{CPA} = 9), PPA ONLY (N_{PPA} = 5),and both CPA (N_{CPA}=9) and PPA (N_{PPA}=5).

in Figure 4.11 show results for when a rogue device is from the same manufacturer as the authorized device it is pretending to be, and as expected, the worst *RRR* are in that section of each subfigure. The only other time CB-DNA has difficulty with a lower *RRR* is when an M1 device is pretending to be an M3 device and vice

versa. However, when enhancements due to CPA and PPA are used individually, verification for M1:M3 and M3:M1 improve $\approx$ 60% for the BGD Test and $\approx$ 22% for BbB. CPA and PPA enhancements see some mixed results when they are individually used for M1:M1 - M4:M4; however, when the two techniques are combined, an average increase in RRR over M1:M1 - M4:M4 is $58\% \leq RRR \leq 95\%$ for BGD Test and $11\% \leq RRR \leq 60\%$ for BbB. In general, RRR improve to over 78% when both CPA and PPA enhancements are used.

Also of note is that the BbB test has an average increase in performance of 13% over BGD test when the rogue device comes from the same manufacturer group. The BbB test also has an average increase in performance of $\approx 15\%$ and $\approx 11\%$ over BGD Test for M1:M3 and M3:M1 cases, respectfully. This advantage is eliminated when the CPA and PPA enhancements are taken into account and RRR becomes more similar for both methods.

The enhancements also provide increased performance in the accuracy metric discussed in Section 4.5.1. Individual device accuracy results without enhancements ($N_{CPA} = 1$, $N_{PPA} = 1$) are provided in Table 4.14. Table 4.15 provides individual device accuracy metrics with enhancements ($N_{CPA} = 9$, $N_{PPA} = 5$) with both tables showing SNR variations. Table 4.14, with no enhancements, has average results across all devices between $0.77 < Accuracy < 0.90$ and when enhancements are considered, as provided in Table 4.15, accuracy increases to $0.92 < Accuracy < 0.97$. These accuracy results suggest that the CB-DNA approach is able to, on average, reject more than 90% of the rogue attacks while correctly granting access to authorized devices more than 90% of time.

Table 4.14. Device Accuracy Across All Permutations with no Enhancements with Each Metric based on 5.1M+ Tests per Device.

	SNR										
Device	8	10	12	14	16	18	20	22	24	26	28
M1:D1	0.741	0.744	0.753	0.774	0.799	0.822	0.846	0.869	0.887	0.899	0.906
M1:D2	0.713	0.734	0.760	0.788	0.816	0.841	0.866	0.888	0.908	0.923	0.935
M1:D3	0.748	0.759	0.773	0.794	0.815	0.836	0.856	0.876	0.892	0.903	0.911
M1:D4	0.731	0.746	0.764	0.785	0.807	0.827	0.846	0.862	0.875	0.885	0.893
M2:D1	0.798	0.800	0.803	0.809	0.816	0.826	0.837	0.849	0.860	0.869	0.876
M2:D2	0.798	0.799	0.802	0.810	0.823	0.834	0.843	0.850	0.855	0.859	0.862
M2:D3	0.808	0.823	0.841	0.870	0.900	0.923	0.937	0.946	0.950	0.954	0.957
M2:D4	0.802	0.805	0.811	0.825	0.842	0.857	0.869	0.879	0.886	0.892	0.897
M3:D1	0.752	0.764	0.781	0.800	0.821	0.840	0.858	0.872	0.884	0.894	0.902
M3:D2	0.724	0.738	0.755	0.779	0.805	0.826	0.847	0.865	0.881	0.892	0.900
M3:D3	0.756	0.794	0.832	0.859	0.878	0.897	0.915	0.929	0.938	0.943	0.946
M3:D4	0.719	0.738	0.759	0.782	0.803	0.821	0.837	0.850	0.862	0.872	0.881
M4:D1	0.807	0.809	0.811	0.813	0.818	0.823	0.829	0.835	0.841	0.846	0.852
M4:D2	0.820	0.829	0.837	0.846	0.855	0.867	0.882	0.896	0.910	0.921	0.930
M4:D3	0.805	0.808	0.812	0.818	0.824	0.831	0.841	0.851	0.858	0.866	0.873
M4:D4	0.808	0.814	0.823	0.831	0.840	0.848	0.855	0.861	0.867	0.873	0.878
Mean	**0.771**	**0.781**	**0.795**	**0.811**	**0.829**	**0.845**	**0.860**	**0.874**	**0.885**	**0.893**	**0.900**

Table 4.15. Device Accuracy Across All Permutations with Enhancements for $N_{CPA} = 9$ and $N_{PPA} = 5$ Based on 1M+ Tests per Device.

	SNR										
Device	8	10	12	14	16	18	20	22	24	26	28
M1:D1	0.917	0.919	0.921	0.926	0.930	0.930	0.930	0.929	0.928	0.927	0.927
M1:D2	0.971	0.988	0.998	0.999	1.000	1.000	1.000	1.000	0.999	0.999	0.999
M1:D3	0.921	0.922	0.924	0.925	0.925	0.926	0.926	0.927	0.927	0.928	0.930
M1:D4	0.855	0.865	0.870	0.878	0.885	0.895	0.908	0.926	0.943	0.956	0.966
M2:D1	0.912	0.919	0.925	0.941	0.947	0.952	0.967	0.982	0.992	0.997	0.998
M2:D2	0.910	0.921	0.927	0.945	0.965	0.978	0.986	0.992	0.996	0.997	0.998
M2:D3	0.995	0.994	0.994	0.998	1.000	1.000	1.000	0.999	0.999	0.999	0.999
M2:D4	0.972	0.980	0.993	0.999	1.000	1.000	1.000	1.000	1.000	1.000	1.000
M3:D1	0.954	0.958	0.963	0.961	0.955	0.953	0.956	0.966	0.976	0.983	0.987
M3:D2	0.932	0.942	0.950	0.948	0.942	0.934	0.935	0.953	0.970	0.980	0.984
M3:D3	0.856	0.859	0.877	0.891	0.895	0.902	0.910	0.926	0.939	0.944	0.950
M3:D4	0.874	0.891	0.895	0.883	0.857	0.836	0.831	0.836	0.836	0.840	0.841
M4:D1	0.876	0.870	0.877	0.901	0.928	0.962	0.988	0.992	0.993	0.992	0.990
M4:D2	0.977	0.983	0.995	0.996	0.997	0.997	0.998	0.998	0.998	0.998	0.997
M4:D3	0.870	0.867	0.875	0.895	0.919	0.933	0.944	0.952	0.960	0.965	0.967
M4:D4	0.911	0.916	0.916	0.922	0.938	0.958	0.973	0.983	0.988	0.988	0.988
Mean	**0.919**	**0.925**	**0.931**	**0.938**	**0.943**	**0.947**	**0.953**	**0.960**	**0.965**	**0.968**	**0.970**

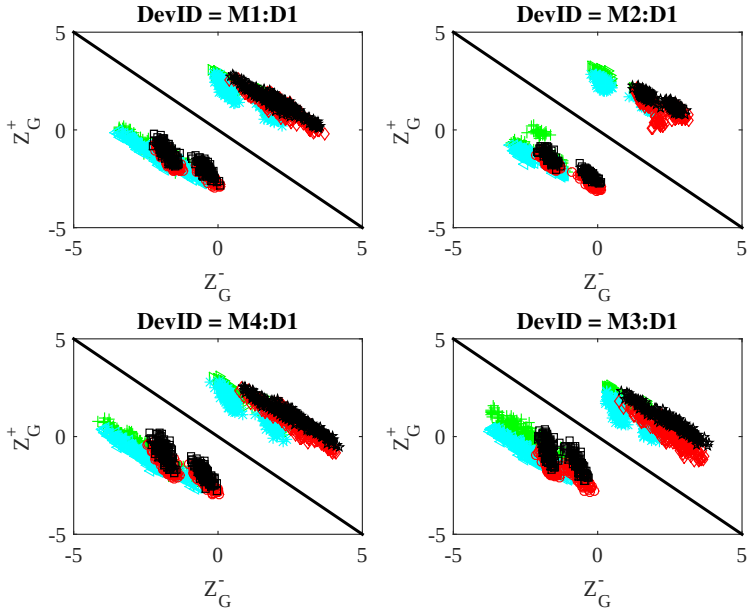
4.7 Sensitivity Analysis and Probe Placement

This section provides results for effects to projected constellation points (shapes of constellations), classification and verification results as the probe-to-card distance L_P increases from 2 to 98 m. It also validates Config #1 classification results for CMD and LMD from Section 4.4. Furthermore, verification results for Perm #29 Section 4.5 with Config #2 and probe-to-card distance of $L_P \approx 2\ m$ is also validated. The addition of Additive White Gaussian Noise (AWGN) to the collected signal is investigated to see if it provides accurate SNR variation on CMD and LMD results.

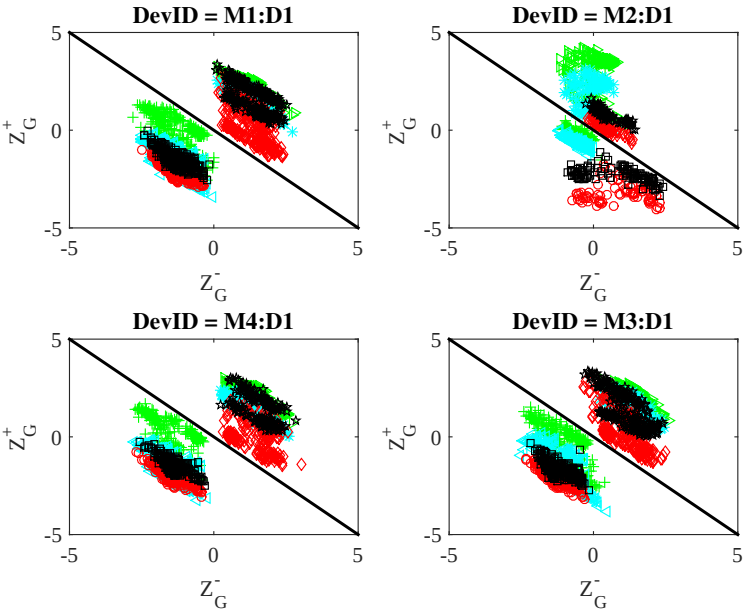
The projected device constellations in Figure 4.12 show how a representative device constellation changes from a card distance $L_P \approx 2\ m$ (Figure 4.12a) to $L_P \approx 98\ m$ (Figure 4.12b). A representative device (D1) is presented for each of the four manufacturers (M1-M4). The effects of an increase on L_P distance can be clearly seen in Figure 4.12 as the subclusters of the projected constellations are not as elongated when $L_P \approx 98\ m$. Receiver coloration has a potential to make some changes on the presentation of the projected symbols. This is seen when comparing Figure 3.15 and Figure 4.12a, which shows some slight movement in the projected subclusters but their relative shapes appear to be the same.

4.7.1 Sensitivity Analysis: Device Classification.

The effect of collection probe and Ethernet card separation distance on average cross-class $\%C$ performance was addressed, i.e., the variation in $\%C$ as the probe-to-card distance L_P increases. Config #2 with $L_P \approx 2\ m$ (Rx 2:Cable 2) was used to validate original results from Config #1 with $L_P \approx 2\ m$ (Rx 1:Cable 1). Config #2 was used to vary the probe-to-card distance for $L_P \approx 2\ m$ and $L_P \approx 98\ m$. Results are presented here for the maximum 10BASE-T cable length of $L_C = 100\ m$, as specified in IEEE 802 [1]. Figure 4.13 presents CMD (left) and LMD (right) results



(a) Config #2 with $L_P \approx 2\ m$

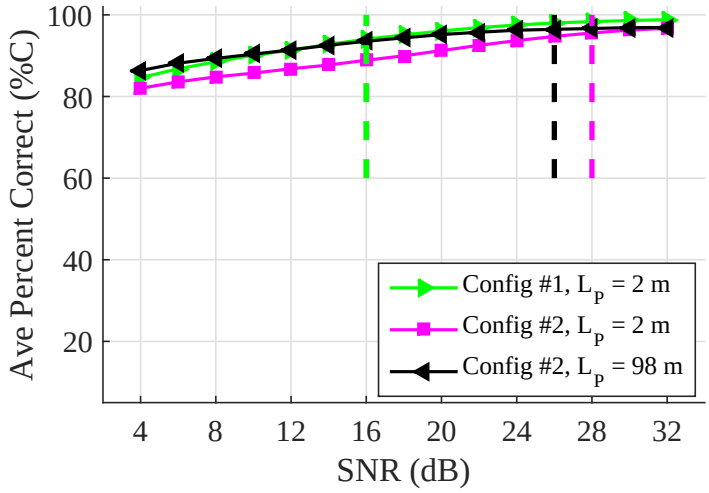


(b) Config #2 with $L_P \approx 98\ m$

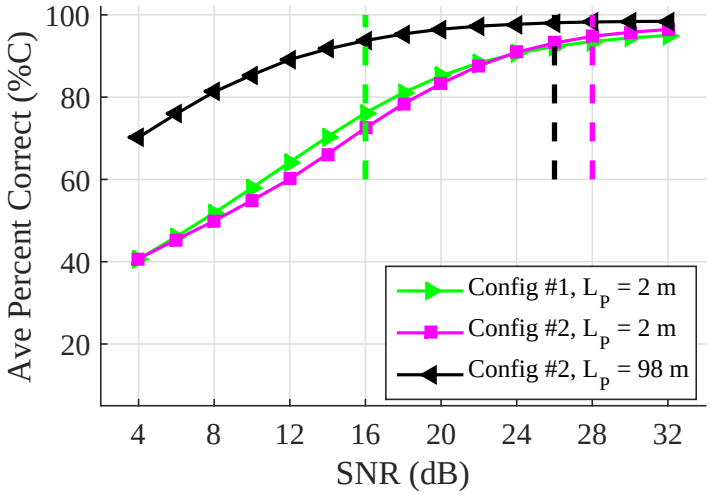
Figure 4.12. The effects of cable-to-probe linear distance on constellation shapes at $SNR = 26$ dB for both $L_P \approx 2\ m$ and $L_P \approx 98\ m$ collection points. Representative device (D1) is presented for each of the manufacturers (M1-M4).

for Config #1 at $L_P \approx 2\ m$, Config #2 at $L_P \approx 2\ m$, and $L_P \approx 98\ m$ with a theoretical variation of $SNR = \{2x | x \in, 2 < x < 32\}$ dB for both configurations. The vertical dashed lines in Figure 4.13 denote the collected SNR value for each

configuration and L_P combination with the same color as the $\%C$ curve it represents.



(a) CMD for Config #1 and Config #2



(b) LMD for Config #1 and Config #2

Figure 4.13. The effects of cable to probe linear distance on CMD and LMD for varying SNR values. Collected SNR values for each configuration and L_P combination denoted as a dashed vertical line with same color as $\%C$ curve.

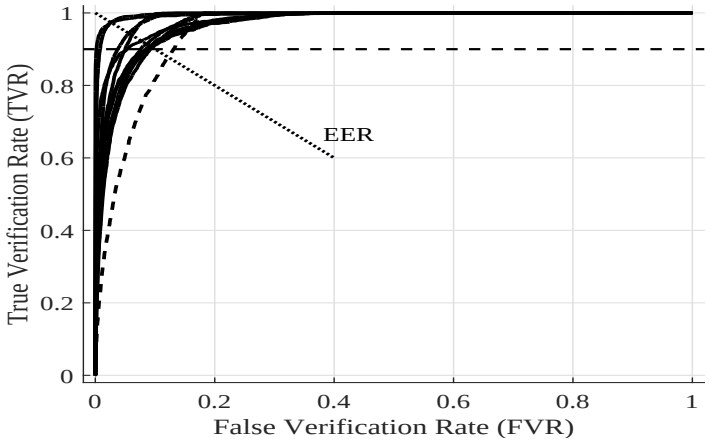
The CMD results for Config #1 and Config #2 at $L_P \approx 2\ m$ and $L_P \approx 98\ m$ are presented in Figure 4.13a and have similar $\%C$ classification across all SNRs, which provides evidence for validation of the CB-DNA process. The CMD results for Config #2 at $L_P \approx 2\ m$ and $L_P \approx 98\ m$ do not provide enough evidence to suggest that adding AWGN is a good indication of probe distance since both results

for Config #2 are statistically the same.

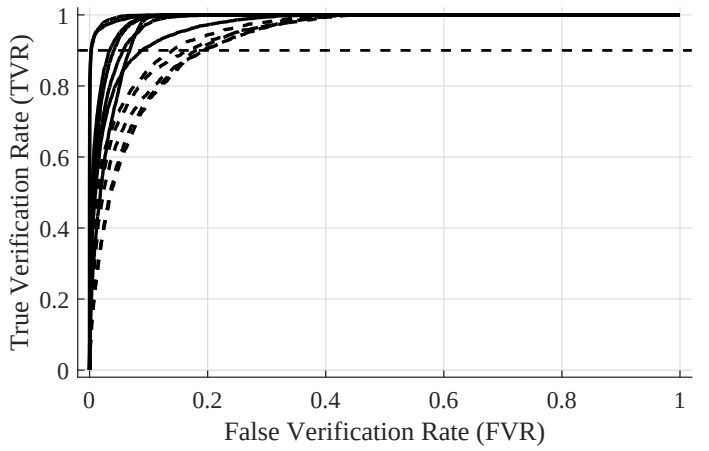
The LMD results for Config #1 and Config #2 at $L_P \approx 2\ m$ in Figure 4.13b provide additional evidence pointing towards validation of the process. An interesting observation in the LMD is that Config #2 at $L_P \approx 98\ m$ outperforms the other two at the collected SNR. This fact does not support the idea that adding AWGN to the collected signal at one collected SNR is representative of the actual performance at a lower SNR. However, Config #1 and Config #2 at $L_P \approx 2\ m$ have different collection SNR values of $SNR = 16$ dB and $SNR = 28$ dB, respectively. The predicted $\%C$ for Config #2 at $SNR = 16$ dB is very close to the actual collected SNR for Config #1 providing some evidence that adding AWGN at various powers does provide insight to classification performance at different collected SNRs. This suggests that the additions of AWGN is not tied to probe location and further study of this effect is required.

4.7.2 Sensitivity Analysis: Device ID Verification.

Verification was re-accomplished using Perm #29 at $L_P \approx 2\ m$ for Config #2 and the results are compared to Config #1 at $SNR = 26$ dB. From this point forward, results for Config #1 will be presented above Config #2 for all figures. The authorized device ROC curves for both configurations are in Figure 4.14 in which Config #1 has a higher BGD AAR of $AAR = 97.7\%$ versus Config #2 of $AAR = 58.3\%$. For Config #2, the five devices that did not meet the previously defined criteria of $TVR > 0.9$ and $FVR < 0.1$ were from manufacturing group M1 and M3. This is different from Config #1 where an M4 device was the sole manufacturer not meeting the criteria. It is expected that the use of different collection configurations will provide some variation in the results. However, Config #2 has similar alignment jitter for all devices, which removes the advantage of device (M3:D3) for Config #1.



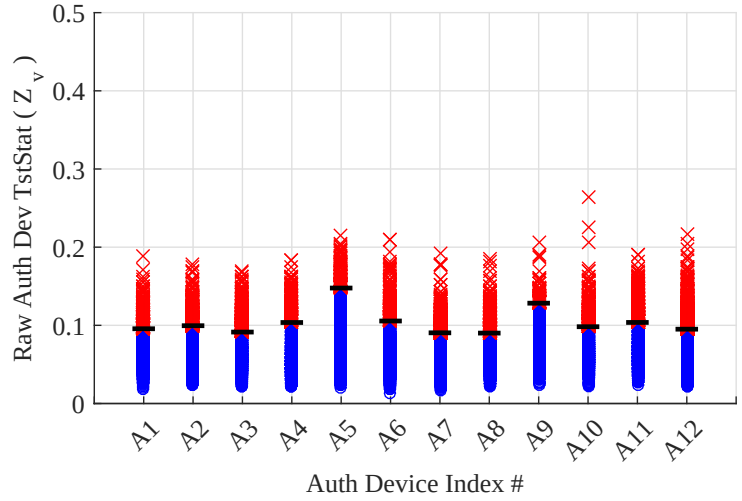
(a) Authorized ROC Curves Config #1



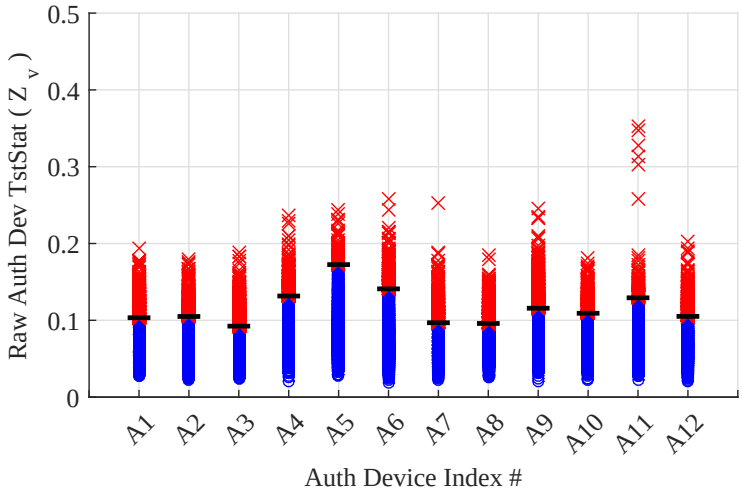
(b) Authorized ROC Curves Config #2

Figure 4.14. Config #1 and Config #2 validation at $L_P \approx 2\,m$ of CB-DNA ID verification ROC curves for Perm #29 in Table 3.3 at $SNR = 20$ dB using a Euclidean distance measure of similarity. Relative to Binary Grant/Deny (BGD) network access decisions Config #1 authorized device success is $AAR = 91.7\%$ (11/12) and Config #2 $AAR = 58.3\%$ (7/12) for $TVR > 0.9$ and $FVR < 0.1$ criteria.

The individual BbB test statistic for Config #1 and Config #2 for authorized devices is in Figure 4.15 with overall BbB percentage results and $T_v(d)$ threshold values corresponding the EER in Figure 4.14, which can be found in Table 4.16. Also summarized in Table 4.16 is the TVR results based on BbB comparisons. Config #1 and Config #2 BbB results presented in Figure 4.15 and Table 4.16 provide validation evidence on the CB-DNA approach for authorized device verification.



(a) Authorized Test Stats Config #1



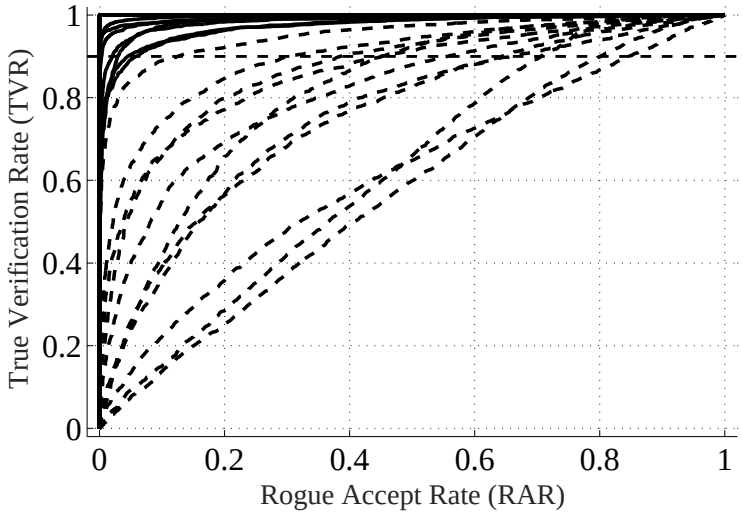
(b) Authorized Test Stats Config #2

Figure 4.15. Config #1 and Config #2 validation at $L_P \approx 2\ m$ of CB-DNA Euclidean distance test statistics for Perm #29 devices at $SNR = 20$ dB. Solid horizontal lines are device dependent $t_V(d)$ thresholds corresponding to ROC EER in Figure 4.14. Authorized Device (A1–A12) ID verification test statistics where blue circles indicate correct access granted and red X's indicate incorrect access denied for N_{Tst}=3,000 testing fingerprints per authorized device.

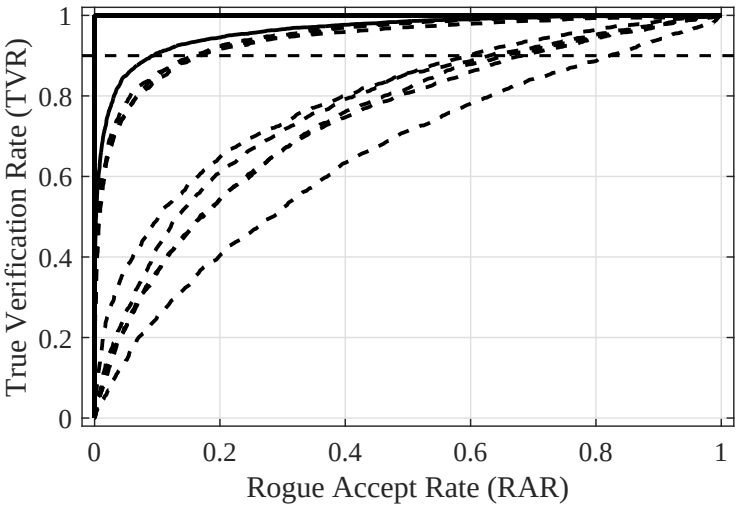
Table 4.16. CB-DNA Config #1 and Config #2 with $L_P = 2\ m$ Authorized Device Dependent $T_V(d)$ Threshold and TVR Values for Perm #29 at $SNR = 20$ dB Corresponding to Figure 4.15 with Bold Entries Denoting Better Performance for TVR Results. Device Dependent $t_V(d)$ Thresholds Corresponding to ROC EER in Figure 4.6.

	Config #1		Config #2	
	TVR	$T_V(d)$	TVR	$T_V(d)$
A1	**90.4**	0.096	84.5	0.103
A2	90.7	0.100	**91.5**	0.105
A3	**89.4**	0.091	82.2	0.092
A4	93.1	0.104	93.4	0.132
A5	97.1	0.148	**98.1**	0.172
A6	94.3	0.106	94.1	0.141
A7	**91.5**	0.090	85.1	0.097
A8	**90.6**	0.090	85.1	0.096
A9	**97.8**	0.128	85.0	0.116
A10	91.0	0.098	**92.7**	0.109
A11	88.4	0.104	**97.4**	0.129
A12	86.7	0.095	**91.0**	0.105
Mean	**91.8**		90.0	

The rogue device ROC curves show a different result than the authorized ROC curves in that the RRR, is based on the BGD access decision of $TVR > 0.9$ and $RAR < 0.1$. The results for Config #1, is lower than Config #2 at $RRR = 77\%$ and $RRR = 83.3\%$, respectively. These results provide additional rogue device evidence for the validation of the CB-DNA approach.



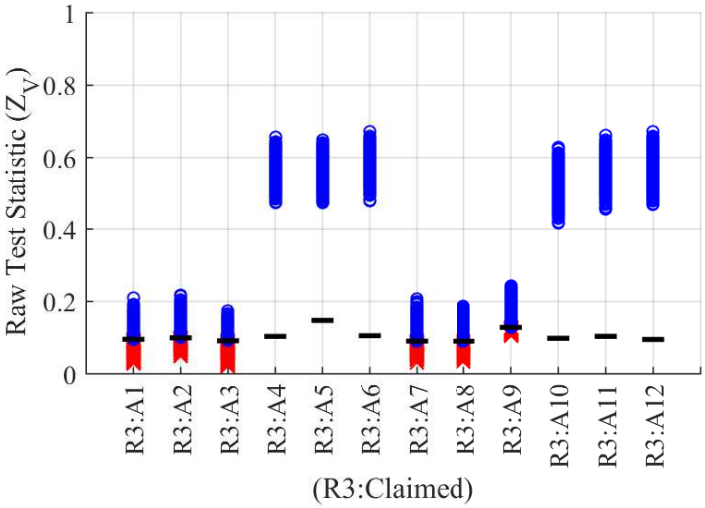
(a) Rogue ROC Curves Config #1



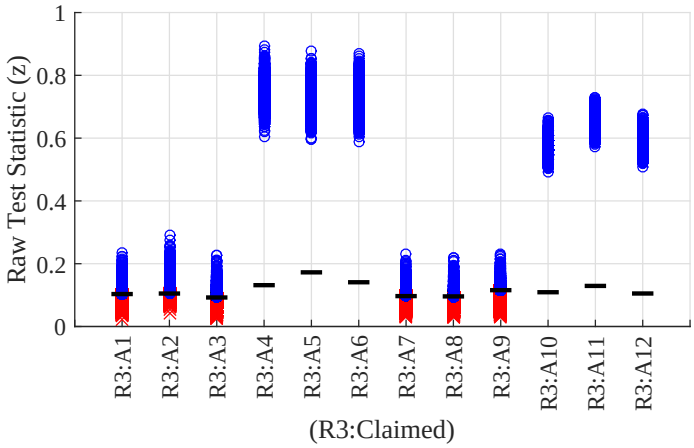
(b) Rogue ROC Curves Config #2

Figure 4.16. Config #1 and Config #2 validation at $L_P \approx 2\ m$ of rogue device ID verification ROC curves for Perm #29 in Table 3.3 at $SNR = 20$ dB using a Euclidean distance measure of similarity. Relative to Binary Grant/Deny (BGD) network access decisions Config #1 rogue device R3 rejection is $RRR = 77\%$ (37/48) and Config #2 $RRR = 83.3\%$ (40/48) for $TVR > 0.9$ and $RAR < 0.1$ criteria.

The BbB results presented in Figure 4.17 and Table 4.17 again show that the only confusion for rogue access is between manufacturer devices M1 and M3.



(a) Rogue Test Stats Config #1



(b) Rogue Test Stats Config #2

Figure 4.17. Config #1 and Config #2 validation at $L_P \approx 2\ m$ of CB-DNA Euclidean distance test statistics for Perm #29 rogue devices at $SNR = 20$ dB. Solid horizontal lines are device dependent $t_V(d)$ thresholds corresponding to ROC EER in Figure 4.14. Rogue device (R3) verification test statistics with blue circles denote a rogue device being correctly denied access and red X's denote an incorrectly granted access decision for $N_{Tst} = 6,000$ BbB testing fingerprints, with rogue device R3 presenting a false ID for each authorized device (R3:A1–R3:A12).

The individual BbB test statistic for Config #1 and Config #2 for rogue devices is in Figure 4.17 with overall BbB RRR percentage results and $T_v(d)$ threshold values corresponding the EER in Figure 4.14, which can be found in Table 4.17.

Table 4.17. CB-DNA Config #1 and Config #2 with $L_P = 2\ m$ Device Dependent $T_V(d)$ Threshold and RRR Values for Perm #29 at $SNR = 20$ dB Corresponding to Figure 4.14 with Bold Entries Denoting Better Performance. Device Dependent $t_V(d)$ Thresholds Corresponding to ROC EER in Figure 4.14.

	Config #1		Config #2	
(Rogue : Claimed)	RRR	$T_V(d)$	RRR	$T_V(d)$
R3:A1	42.0	0.096	**45.7**	0.103
R3:A2	79.9	0.100	**90.2**	0.105
R3:A3	14.7	0.091	**45.5**	0.092
R3:A4	100	0.104	100	0.132
R3:A5	100	0.148	100	0.172
R3:A6	100	0.106	100	0.141
R3:A7	**67.1**	0.090	50.1	0.097
R3:A8	**52.4**	0.090	41.6	0.096
R3:A9	**96.8**	0.128	24.3	0.116
R3:A10	100	0.098	100	0.109
R3:A11	100	0.104	100	0.129
R3:A12	100	0.095	100	0.105
Mean	79.4		74.8	

The general conclusions for AWGN show that the *experimental* $L_C = 100\ m$ assessment were not consistent with the theoretical assessment when using the same receiver and cable at different L_P values; however, the *experimental* assessment was consistent with the theoretical assessment at the same $L_P \approx 2\ m$ but utilizing different receivers and cables. The results for Config #2 were generally validated by the results from Config #1 at $L_P \approx 2\ m$.

V. Summary and Conclusions

This chapter provides the summary and conclusions for the main research elements, results, as well as topic areas of focus for future research. Section 5.1.1 summarizes the Single Slope (SSLP) and Constellation Based (CB) symbol estimation processes. *Device Classification* as a 1 vs. M "Looks Most Like?" assessment, and *Device ID Verification* as a "Looks How Much Like?" assessment for authenticating bit-level credentials are addressed for Radio Frequency-Distinct Native Attribute (RF-DNA) and Constellation Based-Distinct Native Attribute (CB-DNA) Fingerprinting processes. Both fingerprinting processes were investigated over a range of Signal-to-Noise Ratio SNR values utilizing 16 devices from four manufacturers (DLink (M1), Intel (M2), TRENDnET (M3), and StarTech (M4)) with four devices from each manufacturer. The adopted RF-DNA process is covered in Section 5.1.2. Section 5.1.3 concludes the newly developed CB-DNA Fingerprinting process, and the impact of two process enhancements for Constellation Point Accumulation (CPA) and Projection Point Averaging (PPA) follows in Section 5.1.4. The summary of the comparison between the two approaches is provided in Section 5.1.5 prior to finishing with relevant future work in Section 5.2.

5.1 Research Summary

Cyber security threats are on the top 10 list of concerns for many security-minded enterprises as indicated by: 1) a 2014 survey of Fortune 1,000 companies which listed cyber as the number one concern during the previous five years [55], 2) the American Security Project considering cyber as its number two threat in 2015 [30], and 3) the United States Intelligence Office listing cyber as its number three concern [3].

Some of these same cyber security threats are also of concern within the Indus-

trial Control Systems (ICS) enterprise. One of the most concerning elements of these threats involves Supervisory Control and Data Acquisition (SCADA) and Process Control System (PCS) implementations that are migrating away from legacy Information Technology (IT) architectures to more modern Internet Protocol (IP)-based connections [29]. Modern IP-based connections (e.g., Modbus/TCP, Ethernet/IP and DNP3) are being used to provide critical communications to/from control devices [7, 61] and security vulnerabilities remain a concern of those connections. Common ICS vulnerabilities include critical platforms being inadequately protected which allow nonessential personnel direct access to equipment, as well as having open access to wireless and wired ports in common work areas [46, 58]. Many protocols and architectures built for ICS applications were designed without security measure concerns and include no means for verifying the authenticity of remote users or devices [46, 61]. These vulnerabilities make it easy for potential attackers to easily gain ICS network access and exploit hardware, operating systems, and/or executables [46].

Some of the ICS network security and control vulnerabilities can be addressed using the CB-DNA Fingerprinting method demonstrated under this research, with the envisioned implementation being used to augment bit-level mechanisms. CB-DNA Fingerprinting can also be used: 1) by asset owners to support ICS asset management by classifying devices, components, and performing sensor Identification (ID), 2) by compliance personnel to support ICS security audits through verifying device, component, and/or sensor status (unchanged or changed accidentally, intentionally, or maliciously), and 3) for post-incident event ICS triage to assess device, component, and/or sensor status to help determine if the cause of the incident is an incidental failure, intentional rogue activity, etc.

5.1.1 Symbol Estimation.

As developed under this research and documented in [10, 11], the technique for passive collection and exploitation of unintentional Ethernet cable emissions is effective and advances the body of knowledge on Side-Channel Analysis (SCA). Previous wired responses that were considered for SCA used signals that were extracted from field phone lines [24], RS-232 cables [56], power lines [21], and Ethernet cables [27,28]; these prior works focused on 1) monitor video reconstruction, 2) keystroke recognition, and 3) data extraction, versus communication symbol estimation as done under this research. The SSLP symbol estimation technique developed herein [10], uses unintentional emissions, and enables subsequent development of the CB symbol estimation process [11]. The resultant CB symbol estimation method not only provides a reliable, alternate method to perform symbol estimation, but the corresponding symbol constellation provides the basis for generating unique CB device fingerprints and development of the CB-DNA Fingerprinting approach.

The resultant Bit Error Rate (BER) for the two methods is $BER = 4.28\text{x}10^{-7}$ and $BER = 7.46\text{x}10^{-7}$ for SSLP and CB, respectively. These BERs are approximately the same and sufficient for Ethernet operation, as well as providing confidence in the fingerprint generation from the projected non-conventional constellations developed in this research.

5.1.2 RF-DNA Fingerprinting.

This work successfully implemented the RF-DNA approach in [17, 50] and the wired Ethernet results here are consistent with prior related wireless results in [31, 33, 51, 73, 74]. Results include RF-DNA Cross-Model Discrimination (CMD), where different manufactures were easily discernible with $\%C = 91.4\%$ at $SNR = 12$ dB and $\%C = 99.7\%$ at $SNR = 30$ dB. Like-Model Discrimination (LMD) was generally

poorer than other device discrimination results [48, 50] implementing the RF-DNA approach with results, here, being $\%C = 67.6\%$ at $SNR = 26$ dB.

Variation in standards between wired and wireless signaling characteristics, and many devices here share similar LAN transformer markings provide a couple of reasons for RF-DNAs generally poorer performance in LMD. Furthermore, the derivative effects of the probe on the transmitted burst can also hide some potential discriminating evidence in the preamble.

The RF-DNA device ID verification performance is also limited by the same effects that limit its classification performance and also results in generally poorer verification performance when comparing previously related work [47, 50].

5.1.3 CB-DNA Fingerprinting.

This work successfully collected and analyzed wired Ethernet emissions for the purpose of creating a non-conventional constellation in support of symbol estimation of cable emissions and device discrimination utilizing the developed CB-DNA approach herein. CB-DNA discrimination performance was investigated using two configurations: 1) Config #1 (oscope #1, cable #1 of length $L_C = 8\ m$), and 2) Config #2 (oscope #2, cable #2 of length $L_C = 100\ m$) where Config #2 was used to validate the CB-DNA results from Config #1 at $L_P \approx 2\ m$.

For experimental Config #1, CB-DNA CMD Fingerprinting benefits considerably with the introduction of subcluster DNA features. Improvement across the range of *SNR* considered includes an approximate: 1) 5% to 8% increase in *%C*, and 2) 5 to 19 dB of "gain," measured as the reduction in required *SNR* relative to what is required for aggregate features to achieve the same *%C*.

Historically, RF-DNA LMD *serial number* discrimination has been most challenging. Relative to best case RF-DNA performance, CB-DNA is clearly superior and

provides 1) nearly 22% of $\%C$ improvement at collected SNR=16 dB, and 2) 9 dB or more "gain" for $\%C \geq 70$, where gain is the reduction in SNR relative to what is required by RF-DNA to achieve the same $\%C$.

These results were revalidated by processing additional collections for CB-DNA with experimental Config #2, where similar results were achieved at a probe location $L_P = 2\ m$ from the transmitting Device Under Test (DUT). The sensitivity analysis conducted at $L_P = 98\ m$ showed improved performance across all SNR which is believed to be a result of fine burst alignment variations. Both configurations showed that the misclassification error for CMD occurred between DLink (M1) and TRENDnET (M3) devices near 100% of the time. The misclassification error appears to be directly tied to the fact that both manufacturers use the same LAN transformer [12]. For LMD there was some obvious confusion within a manufacturing group. However, any misclassification outside of a device's own manufacturer only occurred between DLink (M1) and TRENDnET (M3).

The like-model verification results provide adequate Rogue Reject Rate (RRR) and True Verification Rate (TVR) for network security implementation. The like-model verification results for CB-DNA utilizing the Binary Grant/Deny (BGD) decision are $65\% < RRR < 86\%$ at $SNR = 20$ dB and $25\% < TVR \leq 100\%$. The Burst-by-Burst (BbB) metric results at values of $81\% < RRR < 93\%$ and $88\% < TVR < 92\%$ at $SNR = 20$ dB are typically higher than BGD. The common LAN transformer also affects verification in much the same way as classification for manufacturers DLink (M1) and TRENDnET (M3). It was concluded that all network access attempts outside of a manufacturing group that resulted in Rogue Accepts (RA) are only between DLink (M1) and TRENDnET (M3). This suggests that LAN transformer RF characteristics influences fingerprint features and impact the ability to perform Ethernet card ID Verification across manufacturers.

Prior work that performs CB device discrimination primarily relies on symbol estimation errors to generate device signatures (i.e., fingerprints) [6, 8, 19, 25, 35]. Conducting a direct comparison of results between these prior works and the current research are difficult for multiple reasons: 1) incomplete methodologies, 2) terminology differences, 3) no SNR variations, 4) discrimination techniques variances, and 5) different devices. However, CB-DNA generally provides improved $TVR = 95\%$ relative to [6] which presents a $TVR \approx 90\%$. Another metric used by [6, 35] is accuracy, which is not defined in either document, but is reported as $accuracy \approx 99\%$ in both works. CB-DNA provides similar results by achieving $accuracy = 97\%$.

One last method for comparison is a correlation-based approach [27, 28] to exploit 10BASE-T Ethernet preambles and is most closely related to the research presented herein. The work in [27, 28] provides accuracy results over multiple methods that range from $90\% < accuarcy < 99\%$. The CB-DNA approach developed in this research provides consistent results ranging from $90\% < accuarcy < 97\%$. Benefits of the CB-DNA method herein include: 1) only requiring external cable access and not individual twisted wire pairs inside the cable, 2) using sample rates that can be 4 to 10 times lower, and 3) operating at lower SNR while still achieving desirable Authorized Accept Rate (AAR) and RRR.

5.1.3.1 Conditional Constellation Features.

This research introduces conditional constellation features as a means to exploit additional information contained in *aggregate* CB non-conventional constellation clusters, i.e., the two projected clusters representing Binary 1 and one Binary 0 transmissions. Conditional assignment of symbol projections to multiple *subclusters* forming the *aggregate* clusters was introduced here using a sequence of three consecutive symbols (bits), including the concatenation of 1) the prior estimated bit value, 2) the

current bit being assigned, and 3) the subsequent estimated bit value; a total of four possible prior/subsequent estimated bit combinations and four subclusters per binary aggregate cluster. None of the prior related RF-DNA or CB-DNA works address fingerprinting devices using conditional symbol features. CB-DNA Fingerprinting using conditional subcluster to create dependent features proved to be very effective and improved $\%C$ by 5% (CMD) and 25% (LMD) relative to using features based only on binary aggregate clusters. The performance increase of $\%C_i = 25\%$ for LMD provides evidence that the conditional subcluster features helped alleviate confusion of DLink (M1) and TRENDnET (M3) devices which share a common LAN transformer. Providing further evidence is when *aggregate* clusters and *subclusters* are combined for LMD, the performance increase is only $\%C_i < 2\%$ relative to just *subcluster* performance and is within the $CI = 95\%$ confidence interval. Even though the *aggregate* subclusters do provide decent classification results, the true power of the CB-DNA technique lies within the *subclusters* and the generation of dependent features introduced in this research.

The novel discovery of the dependent features generated from conditional subclusters allows the CB-DNA technique the ability to achieve performance for LMD that was previously only achievable when performing CMD.

5.1.4 CPA and PPA Enhancements.

Two types of performance enhancements were considered, including: 1) CPA where projected constellation points were accumulated for a specific number of bursts prior to fingerprint feature generation, and 2) PPA where fingerprints projections in the MDA/ML Fisher space are averaged prior to test statistic generation. CPA is a new method developed under this research for CB-DNA and not implementable in RF-DNA. PPA was previously considered for use in the Air Force Institute of

Technology (AFIT) RFINT program.

The utilization of CPA method for CB-DNA provides a Rogue rejection performance increase of $RRR_i = 19.7\%$ for BbB and $RRR_i = 42.5\%$ for BGD decisions relative to no CPA. The PPA method also experiences improvement in Rogue rejection performance results with an increase of $RRR_i = 23.8\%$ for BbB and $RRR_i = 52.9\%$ for BGD decisions relative to no PPA. The highest increase in Rogue rejection performance occurs when both techniques were combined resulting in an increase of $RRR_i = 33.3\%$ for BbB and $RRR_i = 82.9\%$ for BGD decisions relative to no CPA and no PPA. The results for combined CPA and PPA enhancements show an increase in rogue rejection to $RRR \approx 98\%$ between DLink (M1) and TRENDnET (M3) devices. It is evident that both enhancements helped alleviate confusion between DLink (M1) and TRENDnET (M3) devices due to their common LAN transformers. The increased ID Verification performance gains by CPA and PPA provide the potential for a more stringent device verification threshold.

5.1.5 RF-DNA vs. CB-DNA.

This work is the only known work to consider a direct comparison of RF-DNA and CB-DNA methods using *identical* collected emissions. A benefit of performing comparative device discrimination assessments using *identical* collected emissions is that it enables a direct comparison between approaches. Comparison of results for two techniques based on different emissions, collected with different hardware configurations and equipment, can induce potential biases and errantly sway conclusions.

The RF-DNA performance used here for unintentional Ethernet emissions are consistent with prior works [31,33,51,73,74] for other signals and show that LMD is more challenging than CMD. LMD was also more challenging than CMD for CB-DNA, however CB-DNA managed to achieve the $\%C > 90\%$ benchmark highlighting its

superior classification ability for this type of response. Device ID Verification results were more similar between the two approaches. It is believed that the RF-DNA approach had an advantage over CB-DNA because misalignment affects $N_R = 1$ subregion and consequently affects $N_{Feat} = 9$ features. The effect of one projected symbol error for CB-DNA fingerprinting only affects at most $N_{CR} = 3$ subcluster regions, and the $N_{Sym} = 80+$ symbols within each subcluster help to mitigate the misalignment effects. No one feature is based solely on the misaligned region as it is with RF-DNA. Evaluating the amount of the advantage RF-DNA experiences for this data set would require identifying the most relevant features for classification which Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) is not capable of doing.

CB-DNA is more applicable to an operational transition [50] due to the smaller feature set required for better performance. This assessment is based on the performance of both techniques and the number of features needed to achieve their respective performance (CB-DNA, $N_{feats} = 112$ vs. RF-DNA, $N_{feats} = 720$).

5.2 Future Research Topic Areas

This section outlines potential future work that could be accomplished either as a natural progression for extending CB-DNA Fingerprinting applicability or to addresses specific peculiarities discovered during development and warranting further consideration.

5.2.1 Conventional Constellation CB-DNA Fingerprinting.

The collected emissions and received constellation space used here to develop and demonstrate conditional CB-DNA Fingerprinting were not based on a conventional communication signaling constellation. However, this *does not* limit conditional

CB-DNA applicability. The natural progression of the research is to consider conventional higher-order constellations such as Phase Shift Keying (PSK), Phase Amplitude Modulation (PAM), and Quadrature Amplitude Modulation (QAM). There is community interest in pursuing this extension, as the results would enable more direct comparison with previous CB device discrimination work in [6, 8, 19, 25, 35], which did not utilize conditional features. The additional work could also consider an alternative projection space for the higher-order modulations such that were done here for the non-conventional binary constellation using waveform slope in/near symbol transition boundaries.

5.2.2 Probe Placement Analysis.

Collection probe placement along the Ethernet cable was done entirely through oscilloscope observations, with an "acceptable" location being one that produced a near-maximum amplitude response. It was experimentally observed that varying the probe orientation (linear translation and rotation) along the cable affected collected SNR levels and that pressure variation impacted the signal responses, as well. The effects of these variations on CB-DNA Fingerprinting performance requires further study and a non-visual approach to probe placement should be considered.

5.2.3 Ethernet Traffic Load Effects.

Only one of four Twisted Wire Pair (TWP) in the Ethernet cable were active to support DUT operation for this research. This benign environment was sufficient for initial proof-of-concept demonstration. Additional cable traffic loading should be considered for future studies. The cross-TWP interference effects in a more malign environment with higher traffic loads is expected to have some effect on both BER and CB-DNA device discrimination performance. The degree of degradation in a malign

environment remains to be determined. Further study is warranted to characterize performance for higher traffic rates occurring across multiple TWP.

5.2.4 Bit Error Rate (BER) Effects.

The effects of BER on conditional constellation projection assignment were deemed insignificant given that there was, on average, only one bit error occurring for every $N_F \approx 500$ processed fingerprints. As noted in Section 5.2.3, an increase in Ethernet traffic on other TWP is expected to increase BER and likely result in more projected symbols being incorrectly assigned to constellation subregions. The resultant effect may be similar to increasing SNR which results in degraded device discrimination performance. A follow-on study is suggested to assess the impact of increasing BER on conditional CB-DNA Fingerprinting performance.

5.2.5 Expansion to 100BASE-T.

The CB-DNA Fingerprinting approach was developed herein using 10BASE-T Ethernet cable emissions. Potential applicability to higher Ethernet speeds, such as 100BASE-T, is of interest. The lower speed of 10BASE-T is not a limiting factor for ICS applications given that a majority of ICS implementations are/will be using 10BASAE-T [7,61]. However, support for higher speeds is essential, and the CB-DNA approach should be expanded to address higher Ethernet speeds. This expansion is similar to what has been historically done for RF-DNA Fingerprinting using multiple wireless protocols, e.g., Zigbee [48], WiMAX [50], and WiFi [37].

5.2.6 Alternate Classifiers.

The MDA/ML classification technique used here has an inherent limitation of not being able to discern which of the input features are most relevant to the final

classification decision [50]. It is recommended that additional CB-DNA Fingerprinting demonstrations be conducted using an alternate classifier to identify the most relevant features. This resultant feature relevance ranking can then be used to select the best, reduced dimensional, subset of features and enhance operational transition opportunity. Two other potential classifiers that support post-classification feature relevance ranking are Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) [50] and Support Vector Machine (SVM) [6]. Even if these classifiers do not produce adequate classification performance, their relevance ranking will be useful for selecting reduced dimensional subsets for MDA/ML processing.

Bibliography

1. IEEE Standard for Ethernet 802.3. `https://standards.ieee.org/findstds/standard/802.3-2012.html`, 2012.

2. Agilent Technologies. *An Overview of the Eletrical Validation of 10BASE-T, 100BASE-T, and 1000BASE-T Devices.*, 2011.

3. Alexander, Keith, G. Statement of General Keith B. Alexander Before Sentate Committee on Armed Services.

4. Barbeau, M., Hall, J., and Kranakis, E. Detection of rogue devices in bluetooth networks using radio frequency fingerprinting. In *Proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, CCN* (2006), Citeseer, pp. 4–6.

5. Branch, P., Pavlicic, A., and Armitage, G. Using mac addresses in the lawful interception of ip traffic. In *Proc Australlian Telecommunications Networks & Applications Conference (ATNAC), Sydney, Australla* (2004), pp. 9–11.

6. Brik, V., Banerjee, S., Gruteser, M., and Oh, S. Wireless Device Identification with Radiometric Signatures. In *Proc of the 14th ACM Int'l Conf on Mobile Computing and Networking* (2008), ACM, pp. 116–127.

7. Cai, N., Wang, J., and Yu, X. Scada system security: Complexity, history and new developments. In *6th IEEE International Conference on Industrial Informatics, INDIN 2008.* (July 2008), pp. 569–574.

8. Candore, A., Kocabas, O., and Koushanfar, F. Robust Stable Radiometric Fingerprinting for Wireless Devices. In *Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE Int'l Workshop on*, pp. 43–49.

9. Caplan, N. Cyber war: the challenge to national security. *Global Security Studies 4*, 1 (2013).

10. Carbino, T. J., and Baldwin, R. O. Side Channel Analysis of Ethernet Network Cable Emissions. In *9th Int'l Conf on Cyber Warfare and Security* (ICCWS-2014).

11. Carbino, T. J., Temple, M. A., and Bihl, T. J. Ethernet Card Discrimination Using Unintentional Cable Emissions and Constellation-Based Fingerprints. In *2015 Int'l Workshop on Computing, Networking and Communications (IWCNC)* (2015).

12. Carbino, T. J., Temple, M. A., and Lopez Jr, J. A Comparison of PHY-Based Fingerprinting Methods Used to Enhance Network Access Control. In *ICT Systems Security and Privacy Protection* (2015), Springer, pp. 204–217.

13. Casado, M., Freedman, M. J., Pettit, J., Luo, J., McKeown, N., and Shenker, S. Ethane: Taking control of the enterprise. In *ACM SIGCOMM Computer Communication Review* (2007), vol. 37, ACM, pp. 1–12.

14. Chen, S., Wang, R., Wang, X., and Zhang, K. Side-channel leaks in web applications: A reality today, a challenge tomorrow. In *2010 IEEE Symp on Security and Privacy (SP)* (2010), IEEE, pp. 191–206.

15. Cobb, W. E. *"Exploitation of Unintentional Information Leakage from Integrated Circuits"*. Ph.D. dissertation, ECE, AFIT, Wright-Patt AFB, OH, 2011.

16. Cobb, W. E., Garcia, E. W., Temple, M. A., Baldwin, R. O., and Kim, Y. C. Physical Layer Identification of Embedded Devices using RF-DNA Fingerprinting. In *MILITARY COMMUNICATIONS Conf, 2010 - MILCOM 2010* (Oct 2010), pp. 2168–2173.

17. Cobb, W. E., Laspe, E. D., Baldwin, R. O., Temple, M. A., and Kim, Y. C. Intrinsic Physical-Layer Authentication of Integrated Circuits. *Information Forensics and Security, IEEE Trans on 7*, 1 (2012), 14–24.

18. Convery, S. Hacking layer 2: Fun with ethernet switches. *Blackhat [Online Document]* (2002).

19. Danev, B., Luecken, H., Capkun, S., and El Defrawy, K. Attacks on Physical-Layer Identification. In *Proc of the third ACM Conf on Wireless network security* (2010), ACM, pp. 89–98.

20. Danev, B., Zanetti, D., and Capkun, S. On Physical-Layer Identification of Wireless Devices. *ACM Computing Surveys (CSUR) 45*, 1 (2012), 6.

21. Du, Y.-L., Lu, Y.-H., and Zhang, J.-L. Novel method to detect and recover the keystrokes of ps/2 keyboard. *Progress In Electromagnetics Research C 41* (2013), 151–161.

22. Du, Y.-l., Lu, Y.-h., Zhang, J.-l., and Cui, Q. Estimation of eavesdropping distance from conducted emission on network cable of a pc. In *Environmental Electromagnetics (CEEM), 2012 6th Asia-Pacific Conf on* (2012), IEEE, pp. 347–350.

23. Duda, R. O., Hart, P. E., and Stork, D. G. *Pattern Classification*. John Wiley & Sons, 2012.

24. Dürmuth, M. *Novel classes of side channels and covert channels*. Ph.D. thesis, Nat. Sci. and Tec., Saarland Univ., Germany, 2009.

25. Edman, M., and Yener, B. Active Attacks Against Modulation-Based Radiometric Identification. *Rensselaer Institute of Technology, Technical report* (2009), 09–02.

26. Frankland, R., and Offences, A. Side channels, compromising emanations and surveillance: Current and future technologies., 2011.

27. Gerdes, R. M., Daniels, T. E., Mina, M., and Russell, S. F. Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach. In *NDSS* (2006).

28. Gerdes, R. M., Mina, M., Russell, S. F., and Daniels, T. E. Physical-Layer Identification of Wired Ethernet Devices. *IEEE Trans on Information Forensics and Security 7*, 4 (2012), 1339–1353.

29. Gold, S. The scada challenge: securing critical infrastructure. *Network Security 2009*, 8 (2009), 18–20.

30. Hamill, P. "10 Key National Security Challenges in 2015", 2015.

31. Harmer, P., Williams, M., and Temple, M. A. Using de-optimized lfs processing to enhance 4g communication security. In *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)* (July 2011), pp. 1–8.

32. Harmer, P. K., Reising, D. R., and Temple, M. A. Classifier Selection for Physical Layer Security Augmentation in Cognitive Radio Networks. In *IEEE Int'l Conf on Communications (ICC)* (June 2013), pp. 2846–2851.

33. Harmer, P. K., Temple, M. A., Buckner, M. A., and Farquahar, E. Using differential evolution to optimize 'learning from signals' and enhance network security. In *Proceedings of the 13th Annual Conference on Genetic and Evolutionary Computation* (New York, NY, USA, 2011), GECCO '11, ACM, pp. 1811–1818.

34. Hongxin, Z., Yuewang, H., Jianxin, W., Yinghua, L., and Jinling, Z. Recognition of electro-magnetic leakage information from computer radiation with svm. *Computers & Security 28*, 1 (2009), 72–76.

35. Huang, Y., and Zheng, H. Radio Frequency Fingerprinting Based on the Constellation Errors. In *2012 18th Asia-Pacific Conf on Communications (APCC)* (2012), IEEE, pp. 900–905.

36. II, W. C. S., Temple, M. A., Mendenhall, M. J., and Mills, R. F. Radio frequency fingerprinting commercial communication devices to enhance electronic security. *Int. J. Electron. Secur. Digit. Forensic 1*, 3 (Oct. 2008), 301–322.

37. Klein, R., Temple, M., Mendenhall, M., and Reising, D. Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance. In *IEEE International Conference on Communications, ICC '09.* (June 2009), pp. 1–5.

38. Kohavi, R., and Provost, F. Glossary of terms. *Machine Learning 30*, 2-3 (1998), 271–274.

39. Kuhn, M. G., and Anderson, R. J. Soft tempest: Hidden data transmission using electromagnetic emanations. In *Information Hiding* (1998), Springer, pp. 124–142.

40. Lawton, S. Cyber warfare: The next cold war. *SC Magazine April* (2012), 187–209.

41. Ling, Z., Luo, J., Zhang, Y., Yang, M., Fu, X., and Yu, W. A novel network delay based side-channel attack: Modeling and defense. In *INFOCOM, 2012 Proc IEEE* (2012), IEEE, pp. 2390–2398.

42. Marple, S.L., J. Computing the discrete-time ldquo;analytic rdquo; signal via fft. *IEEE Transactions on Signal Processing 47*, 9 (Sep 1999), 2600–2603.

43. Mathworks. *Numerical Gradient Calculation.*, Website.

44. Morisette, J. T., and Khorram, S. Exact Binomial Confidence Interval for Proportions. *Photogrammetric engineering and remote sensing 64*, 4 (1998), 281–282.

45. OConnell, M. E. Cyber security without cyber war. *Journal of Conflict and Security Law 17*, 2 (2012), 187–209.

46. Okhravi, H., and Nicol, D. Applying trusted network technology to process control systems. In *Critical Infrastructure Protection II*. Springer, 2008, pp. 57–70.

47. Ramsey, B. W. *"Improved Wireless Security through Physical Layer Protocol Manipulation and Radio Frequency Fingerprinting"*. Ph.D. dissertation, ECE, AFIT, Wright-Patt AFB, OH, 2014.

48. Ramsey, B. W., Temple, M. A., and Mullins, B. E. PHY Foundation for Multi-Factor ZigBee Node Authentication. In *Global Communications Conf (GLOBECOM), 2012 IEEE* (Dec 2012), pp. 795–800.

49. Reising, D., Temple, M., and Jackson, J. Authorized and rogue device discrimination using dimensionally reduced rf-dna fingerprints. *IEEE Transactions on Information Forensics and Security 10*, 6 (June 2015), 1180–1192.

50. Reising, D. R. *"Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing"*. Ph.D. dissertation, ECE, AFIT, Wright-Patt AFB, OH, 2012.

51. Reising, D. R., Temple, M. A., and Oxley, M. E. Gabor-Based RF-DNA Fingerprinting for Classifying 802.16e WiMAX Mobile Subscribers. In *Int'l Conf on Computing, Networking and Communications (ICNC)* (2012), IEEE, pp. 7–13.

52. Sanger, D., and Schmitt, E. Rise is seen in cyberattacks targeting us infrastructure. *The New York Times 26* (2012).

53. Sanou, B. The World in 2013: ICT Facts and Figures. *Int'l Telecommunications Union* (2013).

54. Sckinger, E. *Appendix A: Eye Diagrams*. John Wiley & Sons, Inc., 2005.

55. Securitas. "Top Security Threats and Management Issues Facing Corporate America", 2014.

56. Smulders, P. The threat of information theft by reception of electromagnetic radiation from rs-232 cables. *Computers & Security 9*, 1 (1990), 53–58.

57. Spurgeon, C. E. *Ethernet: the definitive guide*. O'Reilly, 2009.

58. Stamp, J., Dillinger, J., Young, W., and DePoy, J. Common vulnerabilities in critical infrastructure control systems. *SAND2003-1772C. Sandia National Laboratories* (2003).

59. Stone, S. J. Radio frequency based programmable logic controller anomaly detection. Tech. rep., DTIC Document, 2013.

60. Stone, S. J., Temple, M. A., and Baldwin, R. O. RF-Based PLC IC Design Verification. In *2012 DMSMS & Stand Conf. (DMSMS12)* (Invited Paper Aug 2012).

61. Stouffer, K., Falco, J., and Scarfone, K. Guide to industrial control systems (ics) security. *NIST special publication* (2011), 800–82.

62. Surman, G. Understanding security using the osi model. *SANS Institute InfoSec Reading Room* (2002).

63. Suski, W., Temple, M. A., Mendenhall, M. J., and Mills, R. Using spectral fingerprints to improve wireless network security. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (Nov 2008), pp. 1–5.

64. Tanaka, H. Information leakage via electromagnetic emanation and effectiveness of averaging technique. In *Int'l Conf on Information Security and Assurance, ISA* (2008), IEEE, pp. 98–101.

65. Tech-FAQ. OSI reference model, http://www.tech-faq.com/osi-model.html August 2015.

66. Theodoridis, S., and Koutroumbas, K. *Pattern Recognition*. China Machine Press, 2009.

67. Tipler, P. A. *Physics for Scientists and Engineers*. W.H. Freeman, 1999.

68. Toonstra, J., and Kinsner, W. A radio transmitter fingerprinting system odo-1. In *Canadian Conference on Electrical and Computer Engineering* (1996), vol. 1, IEEE, pp. 60–63.

69. Tzu, S. *The art of war*. e-artnow, 2012.

70. Ureten, O., and Serinken, N. Wireless security through rf fingerprinting. *Canadian Journal of Electrical and Computer Engineering 32*, 1 (2007), 27–33.

71. Van Eck, W. Electromagnetic radiation from video display units: an eavesdropping risk? *Computers & Security 4*, 4 (1985), 269–286.

72. Vuagnoux, M., and Pasini, S. An improved technique to discover compromising electromagnetic emanations. In *IEEE Int'l Symp on Electromagnetic Compatibility (EMC)* (2010), IEEE, pp. 121–126.

73. Williams, M. D., Munns, S. A., Temple, M. A., and Mendenhall, M. J. RF-DNA Fingerprinting for Airport WiMax Communications Security. In *4th Int'l Conf on Network and System Security (NSS)* (Sept 2010), pp. 32–39.

74. Williams, M. D., Temple, M. A., and Reising, D. R. Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting. In *Global Telecommunications Conf (GLOBECOM 2010), 2010 IEEE* (Dec 2010), pp. 1–6.

75. Wright, B. PLC Hardware Discrimination using RF-DNA Fingerprinting. Tech. rep., DTIC Document, 2014.

76. Wyglinski, A., and Pu, D. *Digital Communication Systems Engineering with Software-Defined Radio*. Artech House mobile communications library. Artech House, Incorporated, 2013.

77. Zander, S., Armitage, G., and Branch, P. A survey of covert channels and countermeasures in computer network protocols. *Communications Surveys Tutorials, IEEE 9*, 3 (Third 2007), 44–57.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
09–17–2015	Doctoral Dissertation	Sept 2012 — Sep 2015

4. TITLE AND SUBTITLE

Exploitation of Unintentional Ethernet Cable Emissions Using Constellation Based-Distinct Native Attribute (CB-DNA) Fingerprints to Enhance Network Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Carbino, Timothy J., Capt, USAF

5d. PROJECT NUMBER

N/A

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-DS-15-S-008

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

Air Force Research Laboratory, AFMC
Attn: AFRL/RYWE (Dr. Vasu Chakravarthy)
2241 Avionics Circle, Bldg 620
WPAFB OH 45433-7734
DSN 798-8269, COMM 937-528-8269
Email: vasu.chakravarthy@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYWE

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

This material has been declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

This research contributed to the AFIT's Radio Frequency Intelligence (RFINT) program by developing a new device discrimination technique called Constellation-Based Distinct Native Attribute (CB-DNA) Fingerprinting. This is of great interest to the Air Force Research Lab (AFRL), Sensor Directorate, who supported the research and now have new method for improving network security. CB-DNA fingerprints are used to authenticate wired network device identities, thwart unauthorized access, and augment traditional bit-level security measures that area easily bypassed by skilled hackers. Similar to human fingerprint features that uniquely identify individuals, CB-DNA uniquely identifies communication devices and improves the rate at which unauthorized rogue devices are granted network access.

15. SUBJECT TERMS

Device Discrimination, Ethernet Emissions, Distinct Native Attribute, Network Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Michael A. Temple, AFIT/ENG
U	U	U	U	154	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x4279; michael.temple@afit.edu