PHYSICAL-LAYER IDENTIFICATION OF POWER LINE COMMUNICATIONS USING WS-DNA FINGERPRINTING

THESIS

Brady P. Ross, Capt, USAF

AFIT-ENG-MS-17-M-067

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-17-M-067

PHYSICAL-LAYER IDENTIFICATION OF POWER LINE COMMUNICATIONS USING WS-DNA FINGERPRINTING

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Brady P. Ross, B.S. Mathematics, B.S.E.E.

Capt, USAF

March 2017

AFIT-ENG-MS-17-M-067

PHYSICAL-LAYER IDENTIFICATION OF POWER LINE COMMUNICATIONS USING WS-DNA FINGERPRINTING

THESIS

Brady P. Ross, B.S. Mathematics, B.S.E.E.
Capt, USAF

Committee Membership:

Maj Timothy J. Carbino, PhD
Chair

Dr. Michael A. Temple, PhD
Member

Maj Samuel J. Stone, PhD
Member

AFIT-ENG-MS-17-M-067

Abstract

Communication security concerns are growing and range from large scale automation and control systems to home automation networks. These security gaps are ever increasing and requirements are becoming stricter every year. Vulnerabilities in Supervisory Control and Data Acquisition (SCADA) system networks can leave critical infrastructure exposed to cyber attacks and short falls in home automation communication security permit similar attacks against government and military personnel within their homes. Power Line Communication (PLC) as a network communication method is a practical and cost effective solution supporting many of these systems and networks. PLC can utilize existing infrastructure eliminating the need for new physical communication frameworks making it extremely tempting for use in new and retrofitted industry and government systems. The PLC communication signals can propagate great distances without the need for repeaters and can utilize the zero crossing of the carrier phase of the power line for global synchronization. This synchronization can allow multiple interconnected devices to transmit repeated signals simultaneously which can increase operating range and reliability while boosting the total average received signal power. Using this simultaneous transmission of signals, a Simulcasting PLC Network (SPN) of multiple PLC devices can operate on a single power line circuit. PLC device and SPN discrimination using Wired Signal Distinct Native Attribute (WS-DNA) fingerprinting is investigated as a method for Physical-Layer (PHY) intrusion detection for PLC and SPN communication networks. This PHY intrusion detection method can provide an additional layer of protection that can supplement current vulnerable bit layer intrusion detection. Intentional PLC and SPN signals are captured and WS-DNA fingerprints created to be used in a Multiple

Discriminate Analysis Maximum Likelihood (MDA/ML) process to achieve discrimination. Discrimination is accomplished on three different categories of Device Under Test (DUT); 1) Single device DUT uses $N_{c_{IH}} = 6$ individual Insteon Hubs, 2) SPN DUT where the same 6 Insteon Hubs are integrated with 4 different Insteon On/Off Outlets creating $N_{c_{SPN}} = 24$ distinct SPNs, and 3) a subset of the SPN DUT with $N_{c_{SPN}} = 6$ where each SPN contains identical On/Off outlet configuration but exchanges the Insteon Hub devices. For single device DUT, an Average Cross-Class Percent Correct Classification (%C) of %C = 90% is achieved at Signal-to-Noise Ratio (SNR) of SNR $\geq$ 36 dB and %C = 99% at SNR $\geq$ 46 dB. Receiver Operating Characteristic (ROC) curves are used to illustrate rogue detection results with Equal Error Rate (EER) of EER = 10% achieved for all devices at SNR = 40 dB, i.e., 90% of unauthorized rogue devices are successfully rejected. For the SPN DUT, %C = 90% is achieved for SNR $\geq$ 50 dB with rogue detection resulting in a EER = 10% achieved at SNR = 50 dB. An average %C = 90% is not achieved for the entire set of SPN DUT and rogue detection results in a EER = 10% for only 4 out of 24 classes.

Acknowledgements

May you be strengthened with all power, according to his glorious might, for all endurance and patience with joy. -Colossians 1:11

I am grateful to my God for the good health and steadfastness required to complete this work, you are unfailing in your love, grace, and faithfulness.

I would like to thank my thesis advisor Major Timothy Carbino, PhD. The door to Prof. Carbino's office was always open whenever I had a question about my research or writing. He consistently allowed this paper to be my own work, but steered me in the right direction when I needed it.

Finally, I must express my very profound gratitude to my wife for providing me with unfailing support, prayers, and continuous encouragement throughout my studies and through the process of researching and writing this thesis. This accomplishment would not have been possible without you. Thank you.

Brady P. Ross

Table of Contents

Page

List of Figures

List of Tables

Acronyms

%C Average Cross-Class Percent Correct Classification.

AC Alternating Current.

AGL Airfield Ground Lighting.

AIEE American Institute of Electrical Engineers.

AM Amplitude Modulation.

AWGN Additive White Gaussian Noise.

BPL Broadband over Power Line.

BPSK Binary Phase Shift Keying.

CI Confidence Interval.

DUT Device Under Test.

EER Equal Error Rate.

EMI Electro-Magnetic Interference.

FAR False Accept Rate.

FRR False Reject Rate.

FSK Frequency Shift Keying.

FT Fourier Transform.

FVR Flase Verifiaction Rate.

GRLVQI Generalized Relevance Learning Vector Quantized-Improved.

GSM Global System for Mobile Communications.

GT Gabor Transform.

IEEE Institute of Electrical and Electronics Engineers.

IOT Internet of Things.

IPL Internet over Powerline.

LAN Local Area Network.

LDA Linear Discriminate Analysis.

MAC Media Access Control.

MDA Multiple Discriminate Analysis.

MDA/ML Multiple Discriminate Analysis Maximum Likelihood.

ML Maximum Likelihood.

PDF Probabilty Density Function.

PHY Physical-Layer.

PLC Power Line Communication.

PM Phase Modulation.

PMF Probabilty Mass Function.

PSD Power Spectral Densities.

RAR Rogue Accept Rate.

RF Radio Frequency.

RF-DNA Radio Frequency Distinct Native Attribute.

RFID Radio Frequency Identification.

ROC Receiver Operating Characteristic.

ROI Region of Interest.

RRR Rogue Reject Rate.

SCADA Supervisory Control and Data Acquisition.

SD Spectral Domain.

SNR Signal-to-Noise Ratio.

SPN Simulcasting PLC Network.

TAR True Accept Rate.

TD Time Domain.

TVR True Verifiaction Rate.

VT Variance Trajectory.

WS-DNA Wired Signal Distinct Native Attribute.

PHYSICAL-LAYER IDENTIFICATION OF POWER LINE COMMUNICATIONS USING WS-DNA FINGERPRINTING

I. Introduction

This research involves the investigation of the discrimination of Power Line Communication (PLC) signals through the exploitations of PLC emissions captured from a powerline. The result is the successful demonstration of the Wired Signal Distinct Native Attribute (WS-DNA) process applied to PLC signals. This chapter presents the operational motivation in Section 1.1, the technical motivation in Section 1.2, research contributions in Section 1.3, and the organization and structure of the document in Section 1.4.

1.1 Operational Motivation

As the connectivity of Internet of Things (IOT) devices expands and communication networks evolve and grow, the need for the security of these networks expands. The urgency for increased network security has been a concern that has ranged from broadcast Local Area Network (LAN) to wireless cellar phone networks [1, 2]. This proliferation of individual devices that can connect from one network to another introduces an ever growing problem of security for these networks, especially to those devoted to mission critical systems and Supervisory Control and Data Acquisition (SCADA) networks used to control large scale automation and control systems. These security risks also overflow into the vulnerability of home automation systems that can compromise individual personal security. PLC also presents a problem for institutional information control and security in that PLC can be used to move sensitive

information in a covert way over a potentially unmonitored power line serving additionally as a data network. PLC communications are used in home automation networks and are currently being investigated by industry as possible low cost solutions for large scale automation [3, 4].

The attraction of implementing PLC communication networks is that existing infrastructure can be harnessed and new communication lines do not need to be installed. By using existing powerlines as the communication medium, the costs associated with new network implementation is greatly reduced [3,5]. PLC signals can also travel up to 100 miles without having to be retransmitted and with retransmission the range can be drastically increased [6]. A current use for PLC is automatic meter reading by power companies for one way power monitoring and billing, however two-way PLC communication and control is being investigated [7]. PLC is also being considered for systems like Airfield Ground Lighting (AGL) at airports [3]. The allure of PLC for use in a AGL system is that the current power lines that provide power can also be used for communications that can result in more flexibility and control over the way AGL systems are used [3]. All of these are examples of possible large scale control and automation systems to include SCADA systems that can implement PLC communications to control the network. Network security concerns for critical infrastructure like theses and others are not new. Many of the concerns originate with the lack of security at the time of the system implementation and the subsequent patches and fixes to update the system with vulnerabilities possibly still present. These holes in critical infrastructure security has led to a dramatic increase in attacks on United States infrastructure between 2009 and 2011 with the Department of Homeland Security naming cyber attacks as a top threat [8, 9].

In addition to critical infrastructure and SCADA systems, PLC communication networks are used in home automation control and communication. Specifically, PLC

is implemented for use in Insteon devices and networks [10]. Home automation traditionally utilizes wireless communications like WiFi and Zigbee systems controlling and communicating with various devices around the home. These home automation systems have already shown to have vulnerabilities, with security issues being a "rich field of research problems" [11]. These security issues for individual home automation networks pose a potential threat to those that use these systems in their home. With PLC being implemented in some home automation networks, security of these communications are critical.

The movement of information via PLC also highlights a problem in information control for institutions and secure areas. The very nature of the powerline being used for communications presents PLC as an "unmonitored, possibly covert, communications network" [12]. Several steps have been taken to prevent unintentional transmission of information over powerlines but little is discussed about preventing intentional transmission of information via PLC [13].

PLC implemented in large scale command and control systems as well as in home automation networks presents itself as a technology that has grown faster than its own security. Current and possible PLC networks lack intrusion detection and in most cases are entirely unmonitored. Traditional Media Access Control (MAC) methods are used in some PLC networks as a single layer of unauthorized device protection, however this variety of authentication has been shown to be susceptible to spoofing [14]. An additional layer of Physical-Layer (PHY) authentication is proposed as a possibility to increase security and intrusion detection.

1.2 Technical Motivation

The use of the PHY in device discrimination is a well researched topic and a considerable amount of work has been conducted [15–52]. The majority of these works

have focused on the classification of devices, i.e. 1 vs many, predominantly in the areas of wireless communications including: Institute of Electrical and Electronics Engineers (IEEE) 802.11 WiFi [26–28, 31–33, 39, 40], Radio Frequency Identification (RFID) [17, 46], IEEE 802.16 WiMAX [34–36, 44], IEEE 802.15 Bluetooth [24], and Global System for Mobile Communications (GSM) cellular phones [38, 45]. Additional work has been conducted focused on wired signal Ethernet device classification [49, 50]. Most of the research as focused on intentional emissions of wired or wireless [26, 30, 44, 45, 53, 54], however some effort has been applied to fingerprinting unintentional emissions [51, 52, 55]. Generally, PHY features are extracted from 1) transient, or 2) invariant responses that are used to perform device discrimination [15]. The transient response method [24,42,47] focuses on the response to a change in steady state or equilibrium. This method is generally avoided due to the effects of outside environmental conditions that affect the response as well as the limited duration of the response [16]. The invariant response method [26, 27, 34, 44, 45, 48, 53] focuses on a specific Region of Interest (ROI) within a burst. The target ROI contains non-data modulation typically associated with a preamble, midamble, etc.

1.2.1 Wired Signal Distinct Native Attribute (WS-DNA).

Research into Radio Frequency Distinct Native Attribute (RF-DNA) is wide with a considerable knowledge base [34, 35, 44, 45, 53, 56] and RF-DNA techniques have been adapted to include wired signals via WS-DNA [57]. There is a need to extend these techniques and processes to be applied to PLC communication networks to improve network security and intrusion detection. PHY fingerprinting to include WS-DNA has not been used in the classification or verification of PLC networks or Simulcasting PLC Networks (SPNs). This research contribution will investigate and apply WS-DNA processes and techniques to PLC devices/networks and SPNs.

1.3 Research Contributions

Previously mentioned technical categories are summarized in Table 1.1 and can be used to relate previous work to the work conducted in this paper. Some abbreviations and acronyms that are previously undefined are as follows: Time Domain (TD), Spectral Domain (SD), Gabor Transform (GT), Multiple Discriminate Analysis Maximum Likelihood (MDA/ML), Generalized Relevance Learning Vector Quantized-Improved (GRLVQI), and Simulcasting PLC Network (SPN).

Table 1.1. Relation of Previous Technical Areas of Research and Current Contributions with X's Depicting Addressed Areas.

Technical Area	Previous Work		Current Research	
	Addressed	Ref #	Addressed	Ref #
TD Features	X	[30, 44, 45, 53, 54]	X	[12, 58]
SD Features	X	[34, 44, 56, 59]		
GT Features	X	[34, 53]		
Emission Type				
Intentional	X	[26, 30, 44, 45, 53, 54]	X	[12, 58]
Unintentional	X	[51, 55, 56, 59]		
Response Type				
Transient	X	[24, 42, 47]		
Invariant	X	[26, 27, 34, 44, 45, 48, 53]	X	[12, 58]
Classification/Verification Devices				
Wireless	X	[26, 30, 44, 45, 53, 54]		
Wired	X	[49, 50]	X	[12, 58]
Classification/Verification Process				
MDA/ML	X	[30, 44, 45, 51, 53–56, 59]	X	
GRLVQI	X	[30, 34, 53]		
Network Type				
PLC			X	[12]
SPN			X	[58]

1.4 Document Structure and Organization

The remaining portion of this document is arranged as follows. Chapter II presents applicable background information pertaining to subjects used for this research in-

cluding PLC, SPNs and WS-DNA. Chapter III highlights the experimental methodology used for emission collection, post-processing, WS-DNA implementation, and the subsequent classification and verification. Chapter IV provides classification and verification results. Chapter V presents research summary and conclusions with discussion on possible future work.

II. Background

2.1 Introduction

This chapter provides key background and conceptual knowledge in order to support the research methodology and results provided in in Chapters III and IV respectively. Section 2.2 introduces the reader to a brief history and concept of Power Line Communication (PLC), including information on home automation and Broadband over Power Line (BPL) protocols. Insteon is the subject of section 2.3 describing the target signal and its characteristics, simulcasting, and multiphase transmissions. Section 2.4 discusses Radio Frequency (RF) Fingerprinting including a description of Wired Signal Distinct Native Attribute (WS-DNA) fingerprinting. The final sections discuss device discrimination via Multiple Discriminate Analysis (MDA) and Maximum Likelihood (ML) classification as well as class verification.

2.2 Power Line Communication (PLC)

PLC is a communication method utilizing a sinusoidal or DC power line as a carrier signal with a communication protocol modulated on it. Historically, the PLC communication protocol is implemented to use existing cable infrastructure as a cost savings over new installations [60]. This use as well as others were outlined in a 1954 publication by the American Institute of Electrical Engineers (AIEE) which was later updated in 1980 [61]. PLC has been used by power line workers historically as a simple communication method and is currently used a great deal by power companies in automatic meter reading [6] [62]. The main advantage of PLC networks being the aforementioned ability to use existing infrastructure, another advantage is the independence of the PLC communication network from other communication networks [60]. Disadvantages include relatively low data rates and harsh noise envi-

ronments. Utilizing Frequency Shift Keying (FSK) and spread-FSK industry standard data rates of 2.4 Kb/s can be achieved, however advanced features have be used to demonstrate rates of up to 500 Kb/s [63]. The noise environment of the PLC network can be notorious and spawns from thermal background noise, weather effects, and especially the various devices and appliances that utilize the network for power consumption. Poor weather can cause coronal ionization which can increase noise 20 - 30 dB higher than normal weather conditions [61]. Various household devices that operate simultaneously on the PLC network can be the source of the most troublesome and unpredictable sources of noise. For example, figure 2.1 displays the Power Spectral Densities (PSD) of various household appliances [60]. These noise sources can present unique hurdles for successful and robust PLC networks.

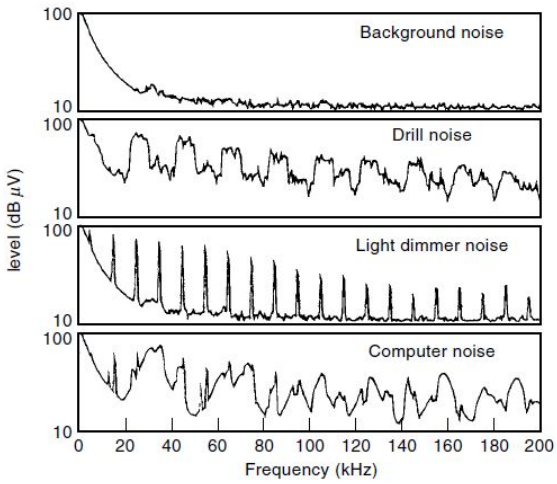


Figure 2.1. Experimental measurements of the Power Spectral Densities (PSD) of various noise sources on power lines [60].

2.2.1 Home Automation.

Traditional uses for PLC networks have expanded from commercial and industrial uses, to home automation. Utilizing the existing power line network as a cost effective home automation solution is gaining attention. Various home sensors and devices such

as locks, cameras, and motion sensors can communicate via a PLC network, sometimes in parallel with other RF communication networks. Thus, a wired independent communication network can be created without the installation of additional cable infrastructure. PLC as a means for home automation began with a company called Pico Electronics, in Glenrothes, Scotland with the invention of X10 [64]. X10 was the first PLC protocol to be widely implemented in home automation and continues to be the industry standard. The X10 protocol has a low data rate at 1 bit every 240 cycles of 120 KHz carrier frequency [65]. These low data rates are adequate for basic home automation messages but are insufficient for complex control systems.

2.2.2 Broadband over Power Line (BPL).

Another application of Power Line Communication (PLC) is BPL. BPL allows high speed broadband communication over power lines and is described by the Institute of Electrical and Electronics Engineers (IEEE) 1901 standard. BPL is an example of broadband PLC with much higher data rates in excess of 500 Mbps [66]. BPL is ubiquitous with Internet over Powerline (IPL) and is extensively used for relatively high data transmissions over a power line network over very short distances. This is primary used for home Internet or to extend the range of home Internet.

2.3 Insteon

Insteon is a family of home automation devices designed to be networked together via RF, PLC, or a combination of both [67]. The PLC modulated signals sent between Insteon devices will be the target of this research. The PLC protocol that is used by Insteon is proprietary and unique to the company, however it is closely related to X10 as mentioned in section 2.2.1. Insteon improved upon the data rate of X10 by a factor of 48 greatly increasing the data rate of the PLC protocol [67].

2.3.1 Signal Characteristics.

Insteon devices communicate via PLC by injecting the communication signal onto the Alternating Current (AC) power-line [65]. For the United States, the nominal voltage is roughly 120 V alternating at 60 Hz. The signal is modulated onto a carrier frequency of 131.65 KHz via Binary Phase Shift Keying (BPSK) with an average peak-to-peak voltage of 4.64 V [65]. Instead of 180 degree transitions between bit boundaries, Insteon PLC utilized a gradual phase shift by introducing 1.5 cycles of carrier at 1.5 times the carrier frequency between bit boundaries. Figure 2.2 displays the gradual phase shift [65].

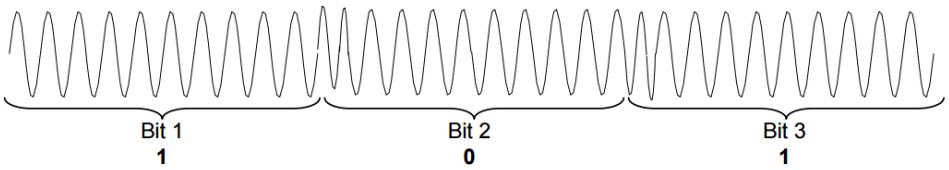


Figure 2.2. Binary Phase Shift Keying (BPSK) with gradual phase shift utilized by Insteon Power Line Communication (PLC) [65].

There are two types of PLC messages, standard messages and extended messages which are broken up into packets that contain 24 bits [65]. The standard message consists of 5 packets and the extended message consists of 11 packets [65]. Figure 2.3 shows the structure of the standard message.

INSTEON Standard-length Message – 10 Bytes				
3 Bytes	3 Bytes	1 Byte	2 Bytes	1 Byte
From Address	To Address	Flags	Command 1, 2	CRC[3]

Data		Bits	Contents
From Address		24	Message Originator's address
To Address		24	For Direct messages: Intended Recipient's address For Broadcast messages: Device Category, Subcategory For ALL-Link Broadcast messages: ALL-Link Group Number [0 - 255]
Message Flags	Message Type	1	Broadcast/NAK
		1	ALL-Link
		1	Acknowledgement
	Extended Msg Flag	1	**0 (Zero) for Standard-length messages**
	Hops Left	2	Counted down on each retransmission
	Max Hops	2	Maximum number of retransmissions allowed
Command 1		8	Command to execute
Command 2		8	
CRC[3]		8	Cyclic Redundancy Check

Figure 2.3. Standard message structure of Insteon Power Line Communication (PLC) message highlighting the required size for each piece of data and its expected contents [10].

A standard message contains a single start packet and 4 body packets for a total of 5 packets. An extended message contains a single start packet and 10 body packets for a total of 11 packets. For a start packet, the first $SP_{ssb} = 12$ bits are Start Packet-start/synchronization bits while the remaining $SP_{db} = 12$ bits are Start Packet-data bits. For a body packet, the first $BP_{ssb} = 6$ bits are Body Packet-start/synchronization bits while the remaining $BP_{db} = 18$ bits are Body Packet-data bits. The structure of start and body packets is presented in Figure 2.4 [65].

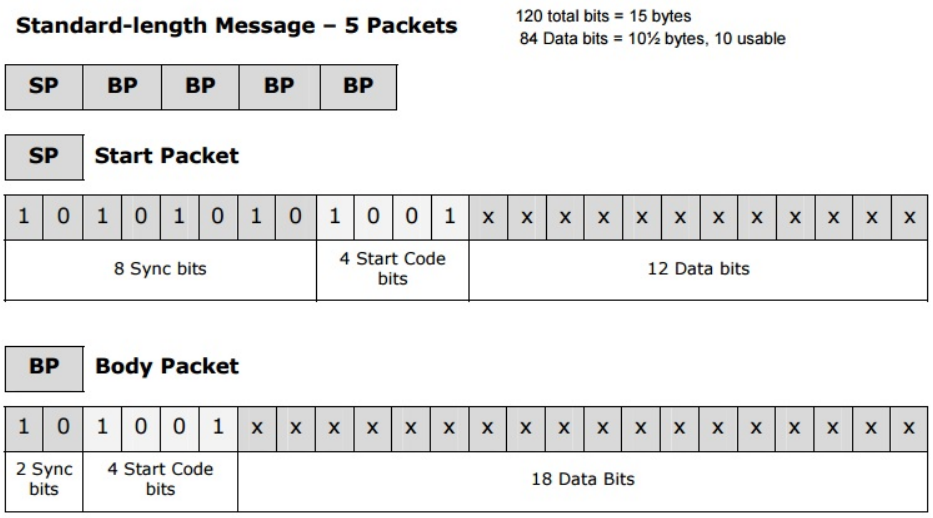


Figure 2.4. A standard message contains 5 packets, 1 start packet, and 4 body packets. Start packets contain 8 sync bits, 4 start bits and 12 data bits while body packets contain 2 sync bits, 4 start bits and 18 data bits [65].

Each packet has a duration of $T_{Pkt} = 1.823$ ms. The start of each packet is transmitted at $T_{PreZC} = 0.876$ ms prior to the zero crossing of the powerline signal and lasts until $T_{PostZC} = .947$ ms after the zero crossing. Each bit is transmitted at a rate of 1 bit every 10 cycles of the carrier frequency. Figure 2.5 displays the zero crossing transition details. Insteon messages are transmitted starting T_{Pkt} before the zero crossing with a frequency of 131.65 KHz.

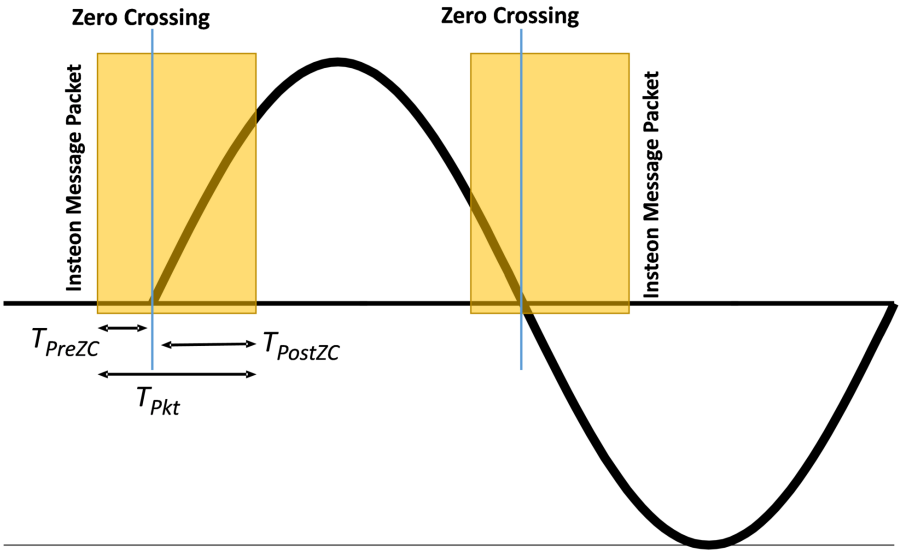


Figure 2.5. Powerline crossing timing illustrating the duration of Insteon messages about the zero crossing of the 60 Hz Alternating Current (AC) power signal [65] [12].

2.3.2 Message Repetition.

To improve reliability of PLC messages, Insteon uses two types of message repetitions: 1) message hopping, and 2) message retrying. These techniques are used individually or together to maximize the dependability of PLC messages sent via Insteon PLC devices.

2.3.2.1 Message Hopping.

Message hopping controls the number of message retransmissions that will occur. This enables the same message to be retransmitted a max number of three hops by the originating device [10]. Message hopping is achieved through *Message Retransmission Flags* that are contained in the message called *Max Hops* and *Hops Left*, an illustration of which can be seen in Figure 2.6 [10]. The *Max Hops* flag dictates that maximum number of hops and the *Hops Left* flag dictates the number of hops that are left.

Figure 2.6 illustrated how message hopping and retransmission works [10].

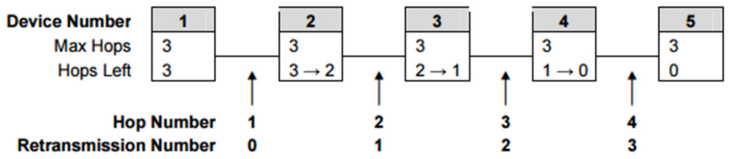


Figure 2.6. Message Retransmissions Illustration with Hops Left and Max Hops Displayed [10]. Hops left is decremented after each retransmission of the original message until it reaches zero.

Message hopping also allows Insteon PLC devices to relay and repeat an originator's message. This can extend the range of PLC messages and also improve the reliability of messages. Combining this with strict timeslot synchronization also allows the simultaneous transmission of messages called simulcasting [10]. Simulcasting will be further discussed in Section 2.3.3.

2.3.2.2 Message Retrying.

When an acknowledgment is not received by an originator it will automatically attempt to resend the message up to four additional times for a total of five transmissions [10]. This is different from message hopping in that a retry is an additional attempt to send a failed message rather than just an attempt to extend the range of the signal in the case of hopping. The *Acknowledgment* flag is used to inform the originator that the message was received. If there is no acknowledgment received by the originator then the message is retransmitted and the *Max Hops* incremented by one to a maximum of three [10]. Increasing *Max Hops* is in attempt to increase the range of the message. An illustration of message hopping and message retrying can be seen in Figure 2.7 [58].

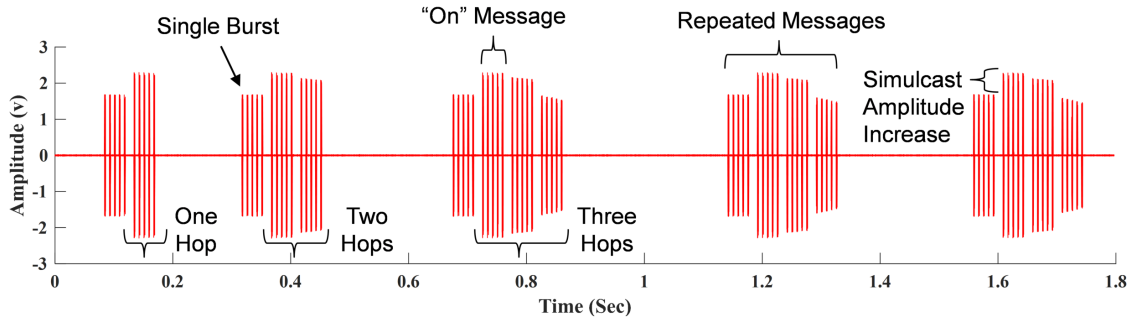


Figure 2.7. Typical time domain response of an Insteon Simulcasting PLC Network (SPN) On message transmission illustrating message responses, burst responses, repeated message responses, and amplitude increase resulting from simulcasting. The 5 retransmissions are highlighted in the On message response with an additional hop added to a max of 3 with no ACK flag from target device [65] [58].

2.3.3 Simulcasting.

Insteon's PLC protocol also includes simulcasting, which is the ability for devices to retransmit the same messages on top of each other [10]. Typical communication networks specifically prevent the simultaneous transmission of messages as this can inflict destructive interference and compromise the integrity of the transmissions. However, PLC networks that utilize the zero crossing of the AC power line as a global clock can use simultaneous transmissions and actually boost the power of the overall message. This increases the total power of transmitted messages and can greatly increase the range a network. An illustration of the zero crossing of an Insteon message can be seen in previous Figure 2.5. A PLC network with multiple devices that is using simulcasting will be referred to as a Simulcasting PLC Network (SPN).

2.4 WS-DNA Fingerprinting

RF fingerprinting is a general term used to describe the ability to extract unique characteristics from intentional or unintentional waveform emissions. These unique characteristics are used to create a digital fingerprint of the emission which then

can be used to discriminate between devices or a network of devices. The entropy of the manufacturing process causes components such as capacitors, amplifiers, oscillators, and inductors to have inherit minute variations in the otherwise identical components [16, 68–70]. These slight differences in the physical hardware introduce Physical-Layer (PHY) differences in device components [70]. The induced PHY differences can cause Amplitude Modulation (AM) -to- Phase Modulation (PM) alterations, change the observed center frequency, or alter symbol rates [70]. The same differences in PHY features and hardware components also apply to PLC devices. Therefore, even devices that are assumed to be identical will have slight variations which enables discrimination of devices [59]. The research presented will use the RF fingerprinting approach of WS-DNA which applies the techniques of Radio Frequency Distinct Native Attribute (RF-DNA) to a wired signal [57]. Section 2.4 provides background on the WS-DNA process and previous work.

Historically, the implementation of RF-DNA involved the extraction of non-data modulated signal burst responses [26,27,34,39,44,45,48,53,54,56,59]. These applications generate features from a Region of Interest (ROI) extracted from Time Domain (TD) [48], Spectral Domain (SD) [44], Fourier Transform (FT) [44], or Gabor Transform (GT) [34] domains.

Traditionally, RF-DNA research involved intentional RF emissions of wireless devices [34,39,44,45,48,54]. WS-DNA uses the same techniques as this but the signal of interest is captured from a wired source instead of a wireless RF source [12,57,58]. For this research, techniques described in [12,58] are used and explained in Chapter III for capturing intentional PLC communication signals created from Insteon PLC devices to produce WS-DNA fingerprints.

Like RF-DNA, WS-DNA uses the steady-state responses of a communication signal and extracts fingerprints based on the distinct features present in the signal typi-

cally extracted from some form of "amble" in the signal [34, 48, 53, 59]. This research will utilize WS-DNA fingerprinting techniques specifically for TD signals as explained in [53, 59]. An ROI is selected from the WS-DNA TD responses and then separated into smaller subregions. Instantaneous responses are then calculated for each subregion partition including: amplitude, phase, and frequency.

A real-valued discrete wired signal response, $ws(k)$, is acquired and WS-DNA fingerprints, F^{WS}, are created from N_k samples. A total of $N_{resp} = 3$ instantaneous TD responses are calculated consisting of amplitude $\{\bar{a}_c(k)\}$, phase $\{\bar{\phi}_c(k)\}$, and frequency $\{\bar{f}_c(k)\}$ where $k = 1, \ldots, N_k$ are provided in (2.1) - (2.3). Because $ws(k)$ is real-valued, it must be converted into I-Q samples before its instantaneous phase (2.2) and instantaneous frequency (2.3) can be calculated [71]. This is done through the Matlab© Hilbert transform function and results in $ws(k) = ws_Q(k) + ws_I(k)$ where

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

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

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

Consistent with previous work the TD responses are then normalized and centered (denoted by a bar and subscripted c respectively) as work seen in equations (2.4) - (2.6) [34, 39, 44]. The mean, $\mu(a)$, $\mu(\phi)$, and $\mu(f)$ is calculated for amplitude, phase, and frequency respectively across N_k samples:

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

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

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

The ROI contains a total of N_K samples and is broken up into N_R contiguous, equal duration subregions with the number of samples in each subregion, always an integer. Usually, the entire ROI is also assigned as an additional subregion for a total of $N_{TR} = N_R + 1$. For each of the centered and normalized instantaneous responses $N_{Resp} = 3$, statistical features $N_{Stat} = 4$ are calculated including: standard deviation (σ), variance (σ^2), skewess (γ), and kurtosis (κ). An illustration of this can be seen in Figure 2.8 [44].

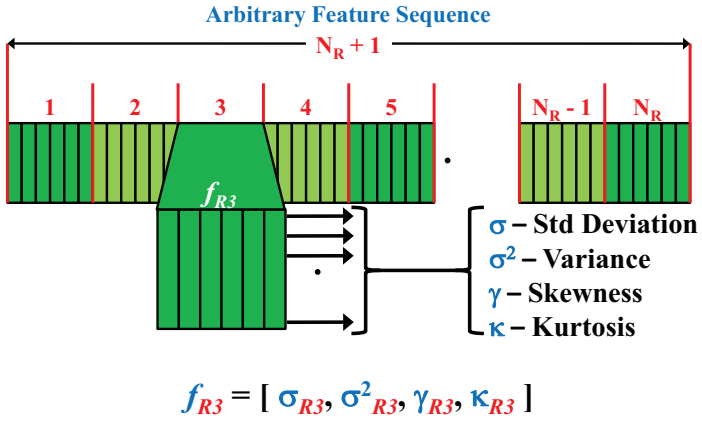


Figure 2.8. Typical Wired Signal Distinct Native Attribute (WS-DNA) fingerprint format with subregions, and individual features illustrated [44].

A regional fingerprint N_{R_i} is generated for each instantaneous response mentioned previously as seen in (2.7). The fingerprint is then concatenated to form (2.8) and the final composite fingerprint is generated from the individual TD feature vectors shown in equation (2.9):

$$F_{R_i}^{WS} = \begin{bmatrix} \sigma_{R_i} & \sigma_{R_i}^2 & \gamma_{R_i} & \kappa_{R_i} \end{bmatrix}_{1\times 4}, \tag{2.7}$$

$$\boldsymbol{F^{WS}}_{a,\phi,f} = \left[F_{R_1}^{WS} \;\vdots\; F_{R_2}^{WS} \;\vdots\; F_{R_3}^{WS} \;\; \ldots \;\; F_{R_{N_{TR}}}^{WS} \right]_{1\times 4(N_{TR})}, \tag{2.8}$$

$$\boldsymbol{F_C^{WS}} = \left[\boldsymbol{F^{WS}}_{a} \;\vdots\; \boldsymbol{F^{WS}}_{\phi} \;\vdots\; \boldsymbol{F^{WS}}_{f} \right]_{1\times 4(N_{TR})\times 3}. \tag{2.9}$$

The total number of features is contingent on the number of total subregions N_{TR}, instantaneous responses N_{Resp}, and statistical features N_{Stat} established. As an example, if $N_{TR} = 4 + 1 = 5$ subregions, $N_{Stat} = 4$ statistical features, and $N_{Resp} = 3$ instantaneous responses, the total number of features will be $N_{Feats} = 5 \times 4 \times 3 = 60$. The specific values for this research is discussed in Chapter III.

2.5 MDA/ML Discrimination

Device discrimination via Multiple Discriminate Analysis Maximum Likelihood (MDA/ML) achieved in this research is adapted from [53, 55]. These same techniques are also consistent with previous WS-DNA [57]/RF-DNA [34, 44, 45, 48, 53, 56, 59] fingerprinting research. This process will be implemented to produce results that are presented in Chapter IV.

The fingerprints of an unknown device are compared to known device fingerprints in what is commonly called classification or a 1 vs. M determination. The unknown device is compared with each of the known devices and a decision is made that will match the unknown device with the known device that most resembles it. This process is completed in two steps: 1) MDA model development and 2) comparison of the fingerprints via the ML classification technique. The MDA model expands Fisher's Linear Discriminate Analysis (LDA) model from a $N_c = 2$ class problem to a $N_c > 2$ class problem where N_c is the number of devices/classes [34]. MDA effectively decreases the number of feature dimensions from N_c to $N_c - 1$ while ensuring the distance between class means are maximized and the spread is minimized [34]. The ML process determines which class the unknown fingerprints resembles based

on the known class fingerprints utilizing the classification model. This is done for each N_c class and will return a the highest resemblance based on the rest of the class fingerprints [53, 55].

2.5.1 Multiple Discriminate Analysis (MDA).

MDA begins with the computation of the scatter matrices for the inter-class averages ($\mathbb{S}_b$) shown in equation (2.10) and intra-class spreads ($\mathbb{S}_w$) shown in equation (2.11) [72] shown as,

$$\mathbb{S}_b = \sum_{i=1}^{C} P_i \Sigma_i, \tag{2.10}$$

$$\mathbb{S}_w = \sum_{i=1}^{C} P_i (\mu_i - \mu_0)(\mu_i - \mu_0)^T, \tag{2.11}$$

where Σ_i is the covariance matrix, and P_i is the prior probability of class c_i while assuming equal cost and prior probabilities [34]. WS-DNA fingerprints are then projected into a $N_c - 1$ dimensional subspace via,

$$\boldsymbol{F}_i^{\mathbb{W}} = \mathbb{W}^T \boldsymbol{F}. \tag{2.12}$$

The projection matrix $\mathbb{W}$ is formed from equations (2.10) and (2.11) and the eigenvectors of $\mathbb{S}_w^{-1}\mathbb{S}_b$, which is the best ratio of intra-class spreads to inter-class mean distances [72]. $\mathbb{F}^{\mathbb{W}}$ is then created as a projected training matrix with N_{Tng} fingerprints per class as,

$$\mathbb{F}^{\mathbb{W}} = \left[\boldsymbol{F}_1^{\mathbb{W}}, \boldsymbol{F}_2^{\mathbb{W}}, \ldots, \boldsymbol{F}_{N_{Tng}}^{\mathbb{W}} \right]_{N_{Tng} \times (N_c - 1)}. \tag{2.13}$$

The mean vector $\hat{\mu}_i^{\mathbb{W}}$ and covariance matrix $\hat{\Sigma}_i^{\mathbb{W}}$ are calculated and a multivariate distribution is matched to the MDA projected data. The process then uses the results

of the projection matrix $\mathbb{W}$, the projected training matrix $\mathbb{F}^{\mathbb{W}}$, the mean vectors $\hat{\mu}_i^{\mathbb{W}}$, and covariance matrix $\hat{\Sigma}_i^{\mathbb{W}}$ for ML classification of testing fingerprints. This process is described in Section 2.5.2.

2.5.2 Maximum Likelihood (ML) Classification.

The outputs of previous Section 2.5.1 are used in ML classification. A similarity measure between unknown fingerprints and each known reference fingerprint is calculated and is described with Bayesian posterior probability while assuming uniform costs and equal prior probabilities [59]. The covariance matrices $\hat{\Sigma}_i^{\mathbb{W}}$ are pooled by:

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

where the total number of devices is denoted as N_C and the pooled covariances is denoted as $\hat{\Sigma}_P^{\mathbb{W}}$.

An unknown device's WS-DNA fingerprint $\hat{\mathbb{F}}$ is assigned to class w_i in accordance with:

$$P(w_i|\hat{\mathbb{F}}) > P(w_j|\hat{\mathbb{F}}) \forall j \neq i, \tag{2.15}$$

where i $\in \{1, 2, \ldots, N_C\}$ and $P(w_i|\hat{\mathbb{F}})$ is the conditional posterior probability that $\hat{\Sigma}_P^{\mathbb{W}}$ is in class w_i. Bayes' rule is then applied and the conditional probability is found by [73],

$$P(w_i|\hat{\mathbb{F}}) = \frac{P(\hat{\mathbb{F}}|w_i)P(w_i)}{P(\hat{\mathbb{F}})}. \tag{2.16}$$

When evaluating (2.16) $P(w_i)$ can be ignored by assuming equal cost and prior probabilities as stated in Section 2.5.1. Because the conditional probability is calculated for a given $\hat{F}$, the denominator $P(\hat{\mathbb{F}})$ will remain constant across all w_i and can subsequently be ignored. This effectively reduces (2.16) to simply $P(\hat{\mathbb{F}}|w_i)$. Reference templates are created by fitting each class with a multi-variate Gaussian distribu-

tion. These templates allow ML to be estimated from the likelihood values of the fingerprint $\hat{\mathbb{F}}$ by:

$$P(\hat{\mathbb{F}}|w_i) = \frac{1}{2\pi^{\frac{N_C-1}{2}}|\hat{\Sigma}|^{\frac{1}{2}}} \cdot \exp(\mathcal{F}_e), \tag{2.17}$$

with

$$\mathcal{F}_e = -\frac{1}{2}(\hat{\mathbb{F}} - \hat{\mu}_i)^T \hat{\Sigma}^{-1}(\hat{\mathbb{F}} - \hat{\mu}_i). \tag{2.18}$$

Average Cross-Class Percent Correct Classification (%C) is then calculated based on the number of fingerprints that are classified correctly divided by the total number or trails.

2.5.3 K-Fold Cross-Validation.

K-fold cross-validation is used to improve result reliability and ensure statistical significance. This is done by first dividing up the training fingerprints into $\frac{N_{Tng}}{K}$ equal size "blocks" of separate sections of fingerprints, where K are the number of blocks. Next, a single block is held out and the remaining $K-1$ blocks are used to create projection matrix $\mathbb{W}$ as described in Section 2.5.1. Finally, the held out block and $\mathbb{W}$ are used to validate the model and perform device classification described in Section 2.5.2 [74]. Ensuing MDA/ML testing is performed based on the $\mathbb{W}$ that had the highest average %C resulting from the training iteration. Consistent with previous works, a value of $K = 5$ is used for the cross-validation in this research [75]. Classification error results are analyzed with the use of a confusion matrix discussed in Chapter IV.

2.6 Class Verification

This section introduces how class verification is performed and explains the process. The techniques and processes described in this section are adopted from [53, 55]

and is consistent with previous WS-DNA works [34, 56, 59]. Class verification is a method to determine the similarity between the fingerprints of classes in a 1 to 1 basis. During verification a class asserts a claimed identity and is verified against a stored digital fingerprint at which point a decision is made as to the authenticity of the claimed identity and the class is either accepted or rejected. This process can be used to provide an additional layer of authentication for networked devices.

The results of class verification is binary where the class is appraised as authorized or unauthorized and if unauthorized, labeled as a rogue. More specifically, an authorized class presents its authorized fingerprint credentials and attempts to gain legitimate access, while a rogue class presents an authorized device's credentials to attempt unauthorized access. This binary decision can result in a class granted access truly or falsely, or rejected access truly or falsely. The binary decision is based on verification test statistic $P(N_c|\mathbb{F}^{\mathbb{W}})$ represented as,

$$P(N_c|\mathbb{F}^{\mathbb{W}}) \geq t, \tag{2.19}$$

where N_C is the claimed class, $\mathbb{F}$ is the observed fingerprint, and t is predetermined decision threshold [53]. The decision made in (2.19) is summarized in Table 2.1 below [53, 56, 59].

Table 2.1. Class Verification Decision Types

Class Verification Decisons		
Class	Authorized	Unauthorized
Authorized	True Accept	False Reject
Unauthorized	False Accept	True Reject

Based on Table 2.1, the decision defined in (2.19) can result in two different types of errors: 1) *True Reject* and 2) *False Accept*. A *True Reject* error results from an

authorized class being rejected from the outcome of (2.19). A *False Accept* results in an unauthorized class being accepted from the outcome of (2.19). *True Accept* and *False Reject* outcomes are non-errors and result when authorized classes are accepted or unauthorized classes are rejected respectively. The decision threshold t can be used to adjust the performance of verification decisions and either increase the rejection of devices, i.e. increased security, or increase the acceptance of devices, i.e. increase accessibility [53].

The performance of the verification decision is appraised with Receiver Operating Characteristic (ROC) curves and corresponding Equal Error Rate (EER) points. The EER point corresponds to the False Reject Rate (FRR) equaling the False Accept Rate (FAR). Each ROC curve is generated by varying t between [0,1] and plotting the True Accept Rate (TAR) vs the FAR [53].

III. Methodology

3.1 Introduction

This chapter presents the methodology used for creating results discussed in Chapter IV. This methodology will target two different focus areas: 1) single device and 2) Simulcasting PLC Network (SPN) and is consistent with previous work [12, 58]. Section 3.2 presents the experimental setup and collection of intentional wired Power Line Communication (PLC) signals originating from Insteon Hubs. Post collection processing with Region of Interest (ROI) definitions are discussed in Section 3.3. Section 3.4 presents how the collected Signal-to-Noise Ratio (SNR) is estimated and Section 3.5 covers the applied Wired Signal Distinct Native Attribute (WS-DNA) techniques used in generating WS-DNA fingerprints. Implemented Multiple Discriminate Analysis Maximum Likelihood (MDA/ML) discrimination technique is introduced in Section 3.6 for classification and class verification is presented in Section 3.7.

3.2 Experimental Hardware Setup

The experimental setup includes an HP© Laptop that is used in conjunction with an application called *Insteon for Hub*, to manually instruct Insteon Hub devices to send PLC messages. A series of two different in-line filters are used to prepare the PLC message for collection. The first being an OnFilter Plug-In Power Line Electro-Magnetic Interference (EMI) Filter that is used to isolate collection equipment from the 120 V voltage while also filtering the 60 Hz sinusoidal Alternating Current (AC) low frequency signal. The second being a $W_{BB} = 32$ MHz low pass anti-aliasing filter to remove any high frequency noise. A Lecroy WavePro 760Zi-A 6.0 GHz oscilloscope is used to digitally sample and store the conditioned PLC message as a discrete valued sequence. The oscilloscope's settings are as follows: 1) a time scale of 10.0 ms/div,

2) an amplitude scale of 2.00 V/Div, 3) a sample rate of 10 MSamp/Sec, and 4) a $t_{Off} = 0$ ms trigger offset. The sampled signal is then stored for post processing and fingerprint creation using MATLAB©.

All efforts are taken to reduce outside noise and influences due to other devices on the power line. The collections are taken on a weekend with all other devices near the collection setup powered down. This does not guarantee other sources of noise with different distribution, as mentioned in Section 2.2, are eliminated from the local power line. However, for this research it is assumed that the only noise present on the line is Additive White Gaussian Noise (AWGN). To further simulate varying channel effects, additional AWGN is introduced post collection and discussed later in Section 3.3.

3.2.1 Device Under Test (DUT).

This work will focus on two different Device Under Test (DUT) categories: 1) single device and 2) SPN. The single device category will focus on collections made from single Insteon Hub devices with no other PLC devices present. The SPN catagory will focus on an SPN comprised of a single Insteon Hub simulcasting with additional Insteon On/Off Outlets. Each DUT can be comprised of three different types of devices: *transmit device*, *peripheral device*, and *receive device*. A *transmit device* is the transmitting device and the originator of any PLC message. A *peripheral device* is an additional simulcasting PLC device or devices that will repeat PLC messages as described in Sections 2.3.2 and 2.3.3. A *receive device* is the target device of the *transmit device* message, i.e. an Insteon Hub (*transmit device*) sends an *On* message to an Insteon On/Off Outlet (*receive device*). For this research the *receive device* will be off network which will force the *transmit device* to use message hopping and message retrying in accordance with Section 2.3.2. The increase in message hops and

retrys reduces the time needed to collect an adequate number or packets for fingerprint generation. An illustration of these repeated messages can be seen in previous Figure 2.7 [58].

A test fixture is used to maintain conseistency between DUT collections and ensure configuration control, illustrated in Figure 3.1. The *transmit device* is located at D1 with any *peripheral devices* located at D2-D4. The EMI filter and collection point is located at D5.

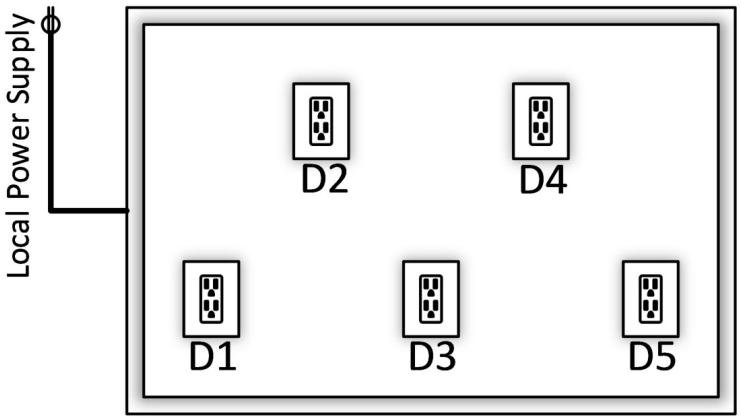


Figure 3.1. Illustration of test fixture used for configuration control. Electro-Magnetic Interference (EMI) filter is located at D5, exchanged transmit devices located at D1, and other peripheral devices located at D2-D4 [12].

3.2.1.1 Single Device DUT.

The single device DUT assessments include $N_{c_{IH}} = 6$ classes, each of which are comprised of a *transmit device* and a *receive device*. For each class a different Insteon Hub acts as the *transmit device* located at D1 on the test fixture transmitting an *On* PLC message targeted to an off network Insteon On/Off Outlet acting as the *receive device*. Collections are taken at D5 as mentioned in Section 3.2.1. Thus, each of the $N_{c_{IH}} = 6$ classes comprise of a different single Insteon Hub transmitting an *On* PLC message with no other PLC device present on the power line. Table 3.1 summarizes the single device DUT category with device addresses and estimated collected

SNR [12]. The estimation of the collected SNR is discussed later in Section 3.4.

Table 3.1. Single Device DUT with Device Addresses and Estimated Collected Signal-to-Noise Ratio (SNR) [12].

Transmit Devices			
N_{clH}	Device	Address	Collected SNR (dB)
1	Hub 1	39:30:05	45.2
2	Hub 2	39:32:86	45.1
3	Hub 3	39:21:82	44.8
4	Hub 4	39:20:DC	44.7
5	Hub 5	39:29:7F	44.9
6	Hub 6	39:17:E3	45.3
Receive Device			
	Insteon On/Off Outlet	39:A0:02	Off Network

Collections are made for each class and saved for post processing. Immediately following, the *transmit device* is replaced with the another device from Table 3.1 and the process is repeated. This is done until collections are made for each class. Each collection extracts 400 Insteon Hub PLC *On* standard messages [12]. As previously discussed in Section 2.3.1, each standard message contains 5 packets, or bursts. This equates to $N_{P_{IH}} = 2,000$ bursts/packets extracted for each class which will be used for fingerprint generation and individual Hub device discrimination.

3.2.1.2 Simulcasting PLC Network DUT.

The SPN DUT category includes $N_{c_{SPN}} = 24$ classes, each of which is comprised of a *transmit device*, *peripheral devices*, and a *receive device*. Each class contains one of $N_{TD} = 6$ Insteon Hubs which acts as the *transmit device* located at D1. A subset *peripheral devices* is created from $N_{PD} = 4$ *peripheral devices* contained in Table 3.2. Each of the $N_{PD_{ss}} = 4$ subsets contain 3 out of the $N_{PD} = 4$ *peripheral devices* with each subset denoted as $N_{\#\#\#}$ where # is taken as four-choose-three from the set of {1,2,3,4}. Table 3.2 summarizes these subsets.

Table 3.2. Subsets of Peripheral Devices with Device Addresses and Connection Positions.

Peripheral Devices		
Label	Device	Address
N_{P1}	On/Off Outlet 1	39:9F:FC
N_{P2}	On/Off Outlet 2	39:9C:9C
N_{P3}	On/Off Outlet 3	39:9E:28
N_{P4}	On/Off Outlet 4	39:9E:08
Subsets of Peripheral Devices		
Subset Label	Peripheral Devices in Subset	Connection Positions Respectively
N_{123}	N_{P1}, N_{P2}, N_{P3}	D2, D3, D4
N_{423}	N_{P4}, N_{P2}, N_{P3}	D2, D3, D4
N_{143}	N_{P1}, N_{P4}, N_{P3}	D2, D3, D4
N_{124}	N_{P1}, N_{P2}, N_{P4}	D2, D3, D4

Each of the *peripheral devices* are connected respectively to D2-D4 as shown in Table 3.2. Any given class contains one of $N_{TD} = 6$ *transmit device*, one of the $N_{P_s} = 4$ *peripheral device* subsets, and the same off network *receive device* which results in $N_{c_{SPN}} = N_{TD} \times N_{P_s} = 6 \times 4 = 24$ different classes. For example, the first class contains the first of the $N_{TD} = 6$ *transmit devices* targeting the same *receive device*. In addition, *peripheral devices* 1, 2, and 3 (at positions D2, D3, and D4 respectively) are present. This creates the first class of in the SPN DUT category. Table 3.3 displays all the SPN DUT classes collected on with the estimated collected SNR. The collected SNR estimation is explained in Section 3.4. Similar to Section 3.2.1.1 collection, for each class 1,000 *On* messages are collected. As discussed in Section 2.3.1 each message contains 1 start packet and 4 body packets. Thus, the collected messages contain $N_{P_{SPN}} = 1,000$ start packets per class that will be used for WS-DNA fingerprinting of SPN classes.

Table 3.3. All Simulcasting PLC Network (SPN) Device Under Test (DUT) Classes Collected On with Transmit Device Address and Collected Signal-to-Noise Ratio (SNR), Where N_{Ps} Can Be Found in Table 3.2.

SPN DUT			
N_{cSPN}	N_T with Address	N_{Ps}	Collected SNR (dB)
1	Hub 1 39:30:05	N_{123}	51.5
2		N_{423}	51.3
3		N_{143}	51.5
4		N_{124}	51.4
5	Hub 2 39:30:05	N_{123}	51.5
6		N_{423}	51.4
7		N_{143}	51.5
8		N_{124}	51.1
9	Hub 3 39:30:05	N_{123}	51.2
10		N_{423}	51.5
11		N_{143}	51.3
12		N_{124}	51.5
13	Hub 4 39:30:05	N_{123}	51.1
14		N_{423}	51.2
15		N_{143}	51.3
16		N_{124}	51.4
17	Hub 5 39:30:05	N_{123}	51.8
18		N_{423}	51.6
19		N_{143}	51.5
20		N_{124}	5.16
21	Hub 6 39:30:05	N_{123}	51.6
22		N_{423}	51.5
23		N_{143}	51.4
24		N_{124}	51.3

3.3 Post Collection Processing

This section presents information specific to post processing collections from both DUT categories in order to extract an ROI per response that are used in WS-DNA fingerprinting. This post processing is done exclusively in MATLAB© directly following signal collection described in Section 3.2. Post-collection processing for both categories include 1) digital filtering, 2) individual Variance Trajectory (VT) based burst detection and extraction consistent with [30, 53], 3) burst selection based on which DUT category was collected, 4) SNR scaling to achieve desired simulated channels effects, and 5) ROI selection. All collections have a duration of approximately $T_C \approx 1.8$ s and contain 17 messages with a total of 85 packets/bursts. A typical collection can be seen in Figure 3.2.

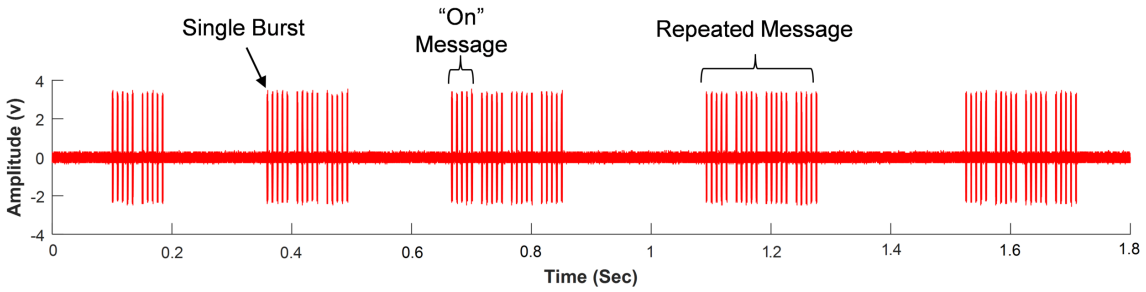


Figure 3.2. Typical Collection Illustration with Single Burst, Message, and Repeated Messages displayed.

3.3.1 Digital Filtering.

All collections are first filtered using a software implemented 16th order Butterworth filter centered at $f_c = 131.65KHz$ with bandwidth $W_{CBB} = 30KHz$. This removes the majority of noise from the modulated signal and Figure 3.3 shows the unfiltered Power Spectral Densities (PSD) and Figure 3.4 displays the PSD of the filtered signal with the impulse response of the filter.

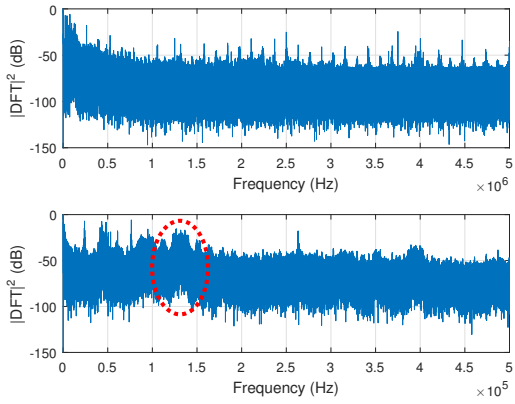


Figure 3.3. Unfiltered Signal Power Spectral Densities (PSD). Top illustrates a large portion of the PSD spectrum while the bottom shows expanded view with the target signal PSD highlighted with red dotted line.

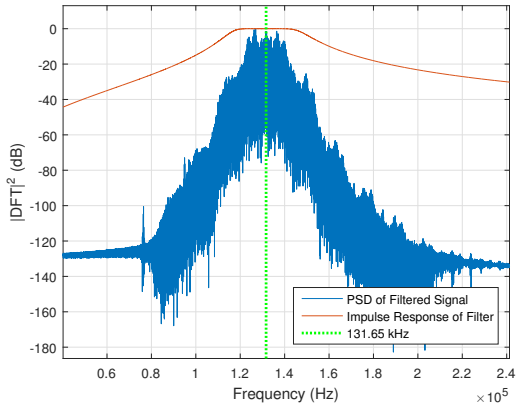


Figure 3.4. Filtered signal Power Spectral Densities (PSD) with impulse response and filter center frequency.

3.3.2 Burst Detection.

In order to detect and extract message packets or bursts from the total collection, amplitude-based VT is implemented as mentioned in Section 3.3. Using Equation (2.1) a VT sequence $VT_a(i)$ is created using,

$$VT_a(i) = |W_a(i) - W_a(i+1)|, \tag{3.1}$$

$$W_a(n) = \frac{1}{N_m} \sum_{i=1+(n-1)N_A}^{1+(n-1)N_A+N_m} (a(n) - \mu^2), \tag{3.2}$$

such that $i = 1, 2, \ldots, L_m - 1$, $m = 1, 2, \ldots, L_m$, $L_m = [(N_a - N_m)/N_s] + 1$, N_a is combined samples making up $a(i)$, N_m is the width of the window, and N_A is the number of samples that are advanced the window in between calculations [30, 53]. Because each burst will be approximately the same size, this results in coarse burst detection with all the bursts coarsely aligned with one another.

3.3.3 Burst Selection.

Immediately after burst detection, specific bursts are selected depending on which of the DUT categories are being collected. As described in Section 3.2.1 the two types of DUT categories are 1) single device and 2) SPN.

3.3.3.1 Single Device DUT.

When post processing for the single device DUT category, all packets/bursts are selected to be used. As mentioned is Section 3.2.1.1, this equates to $N_{P_{IH}} = 2,000$ packets/bursts that will be used in WS-DNA fingerprinting. The specific ROI used is further discussed in Section 3.3.5.

3.3.3.2 SPN DUT.

Unlike the single device DUT category, the SPN DUT category does not use all collected packet bursts. Only the simulcasted start packets are selected for WS-DNA fingerprinting resulting in $N_{P_{SPN}} = 1,000$ start packets. As discussed in Section 2.3.3, the first message in a series of repeated messages on a SPN is not simulcasted. Figure 3.5 illustrates an average of 0.7 V amplitude difference between single device packets and simulcasted packets.

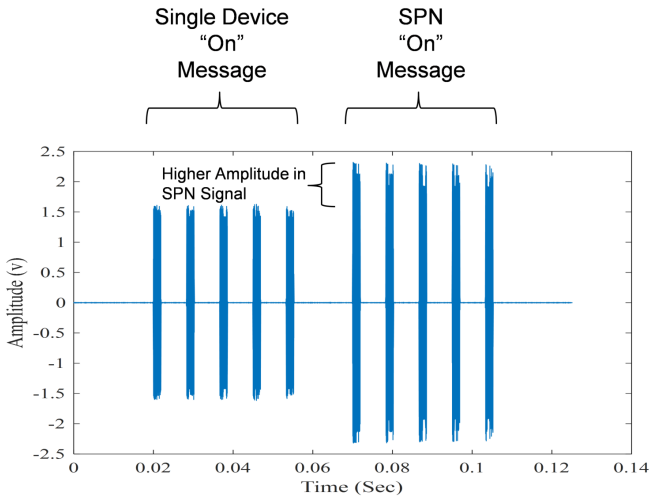


Figure 3.5. Simulcasting message compared to single device message illustrating an average amplitude difference of .7 V.

It is only the subsequent repeated messages in an SPN broadcast that are simulcasted. Thus, only start packets that have been simulcasted are selected for WS-DNA fingerprinting. Only start packets are used due to the larger steady state region available for fingerprinting, this is further explained in section 3.3.5.2. Simulcasted packets are isolated from non-simulcasted packets via a power metric P_{Thresh}. This is done by comparing the power of a known single device start packet signal with collected SPN start packets. A value of P_{Thresh} is selected and the SPN collected start packet P_{Col} is compared with the power of the known single device start packet P_{IH} using,

$$P_{Col} \geq P_{Thresh} \times P_{IH}. \tag{3.3}$$

Equation (3.3) results in a binary decision of either 1) the collected start packet power is less than the scaled known single device start packet power or 2) the collected start packet power is greater than or equal to the scaled known single device start packet power. A unit-less scaling factor of $P_{Thresh} = 1.4$ is empirically found to effectively discriminate single device start packets from simulcasted start packets greater than 3

standard deviations. The Probabilty Density Function (PDF) of the power of known single start packets are compared with the power from SPN collected start packets with a $P_{Thresh} = 1.4$ using Equation 3.3 over $N_{real} = 100$ realization. Figure 3.6 shows the PDFs of the power for the single device start packets and selected simulcasted packets when the equation (3.3) is used with $P_{Thresh} = 1.4$ along with three standard deviations for each PDF.

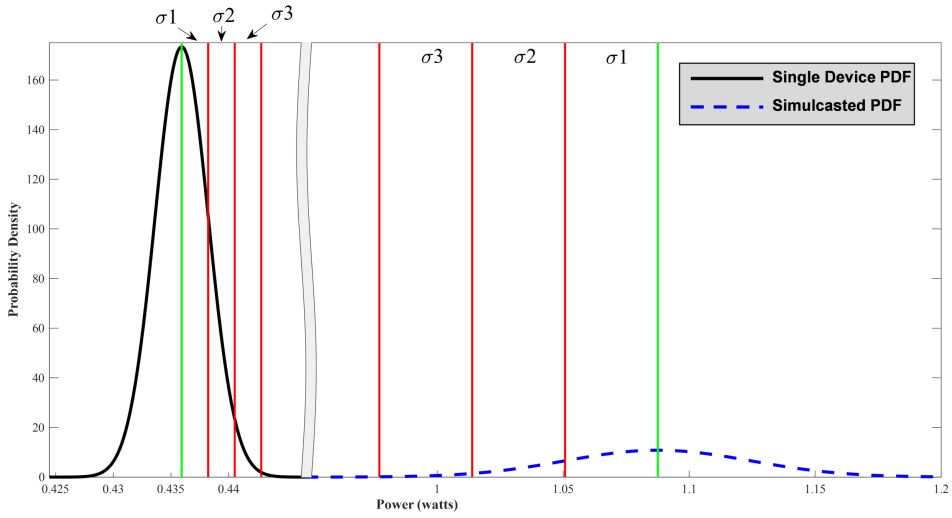


Figure 3.6. Power Probabilty Density Function (PDF) of single device start packets compared with collected Simulcasting PLC Network (SPN) start packets illustrating greater than 3 standard deviation separation.

This shows that a $P_{Thresh} = 1.4$ is adequate for at least 3σ to discriminate simulcasted start packets from single device packets.

3.3.4 SNR Scaling.

After burst detection and selection, the SNR of the PLC packets for the single device DUT categroy are approximately $SNR_{cIH} \approx 45$ dB and $SNR_{cSPN} \approx 51$ dB for the SPN DUT. The collected SNR for all classes can be found in Tables 3.1 and 3.3. These high collected SNR levels do not necessarily represent all channel conditions. Therefore, $N_{MCz} = 5$ independent power-scaled like-filtered Monte Carlo AWGN

realizations are added to simulate varying channel conditions to obtain $SNR_{aIH} = [-10 : 50]$ dB in 2 dB steps for the single device DUT category and $SNR_{aSPN} = [-10 : 54]$ dB in 2 dB steps for the SPN DUT category. Each AWGN realization was 1) randomly created from a Gaussian distribution, 2) filtered in the same manner as the collected message packets as mentioned in Section 3.3.1, and 3) power-scaled to achieved the desired SNR when added to the collected message packets. This is repeated for collected signals $N_{c_{IH}} = 2,000$ and $N_{cSPN} = 1,000$ to create a total of $N_{tIH} = N_{MCz} \times N_{c_{IH}} = 2,000 \times 5 = 10,000$ signal responses for the single device DUT category and $N_{tSPN} = N_{MCz} \times N_{cSPN} = 1,000 \times 5 = 5,000$ signal responses for the SPN DUT category.

3.3.5 ROI Selection.

The ROI is the area or areas of the steady state response that will be used during fingerprint generation. For this research a different ROI will be identified for each of the DUT categories, 1) single device and 2) SPN. Each DUT category targets different ROI regions, however for each category the same ROI will be targeted for all collections. This ensures that for each category, each ROI per collection will contain the same message information, i.e. the same start/sync symbols as described in Section 2.3.1.

3.3.5.1 Single Device ROI Selection.

In the single device DUT category all message packets are to be used for fingerprinting as mentioned in Section 3.3.3.1. The single device ROI_{IH} is chosen such that it contains the first 4 symbols that correspond to the first 4 bits transmitted along with a transient region prior to the first symbol. The first 4 symbols of start and body packets is the response which contains the same information regardless of

device or message sent as discussed in section 2.3.1. Figure 3.7 provides a visual representation of the collected packet response separated into the following section: 1) transient response region ($T_{IHtran} = 50\ \mu$s), 2) first 4 start/sync symbol region ($T_{IHSS} = 303\ \mu$s) 3) data symbol region ($T_{IHD} = 1519\ \mu$s) [12].

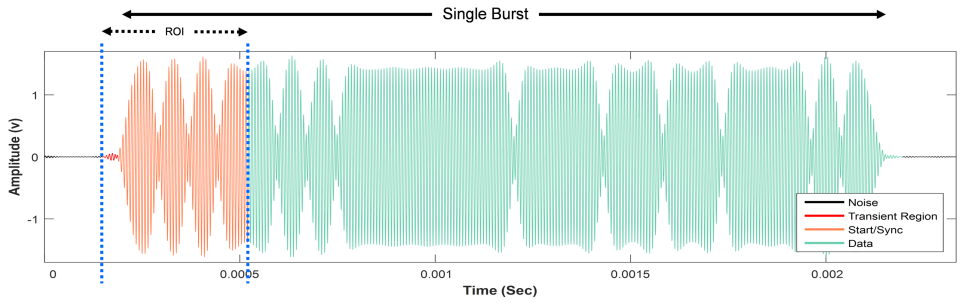


Figure 3.7. Single device packet illustrating the start/sync, data, transient, and noise regions. [12].

3.3.5.2 SPN ROI Selection.

In the SPN DUT category only message start packets are to be used for fingerprinting as mentioned in Section 3.3.3.2. Similar to the single device DUT a steady state like region will be chosen as the ROI_{SPN} containing the first 12 symbols along with a transient region prior to the first symbol. As mentioned before only start packets are used due to the larger region available due to more start/synchronization bits present in all start packets. Because there are more devices present in the SPN DUT category the larger ROI should provide more features for each fingerprint. The region that corresponds to the start/synchronization symbols will be used for each start packet. This corresponds to the fist 12 symbols/bits of any start packet of which the information in this region will not change between start packets despite the device that is transmitting or what message is sent. Figure 3.8 provides a visual representation of the collected packet response separated into the following section: 1) transient response region ($T_{SPNtran} = 50\ \mu$s), 2) first 12 start/sync symbol region

($T_{SPNSS} = 911\ \mu s$) 3) data symbol region ($T_{SPND} = 911\ \mu s$) [58].

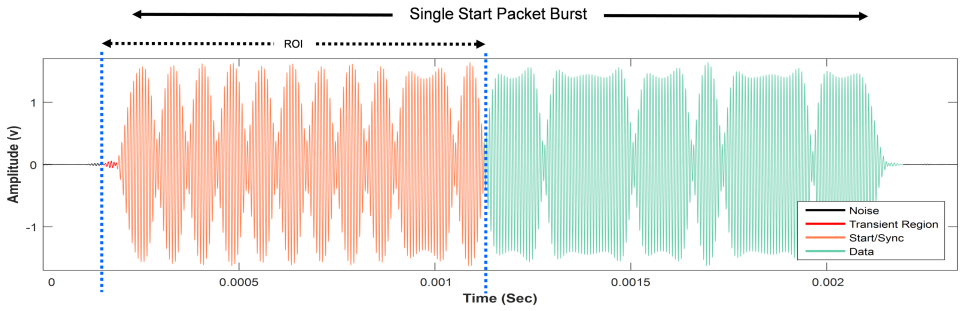


Figure 3.8. Simulcasting PLC Network (SPN) start packet illustrating the start/sync, data, transient, and noise regions. [58].

3.4 Collected SNR Estimation

In order to determine the performance of WS-DNA discrimination, the collected SNR of the modulated PLC message is estimated. The results of this estimation are displayed in Tables 3.1 and 3.3. The PLC SNR is estimated by extracting a portion of the transmitted PLC modulated signal that falls between packets which contains the same number of samples as the collected message packets. This extracted portion only contains noise and is post preprocessed through the same software implemented Butterworth filter as previously mentioned. The power of this like-filtered noise sample is compared with that of the power of the post processed message packets to determine the estimated collected SNR. This results in a close estimation of the collected SNR that is actually slight higher than the true collected SNR as some small amount of noise is still present in the collected message packets.

3.5 WS-DNA Fingerprinting

The ROIs selected for each of the DUTs are used for WS-DNA implementation as highlighted in Figures 3.7 and 3.8. Each ROI is separated into N_R equal length, contiguous subregions in order to extract unique WS-DNA fingerprints. The ROI_{IH}

response shown in Figure 3.9 containing $N_{IHsamp} = 3530$ discrete time samples is divided into $N_{RIH} = 30$ subregions with each N_{RIH} subregion containing $N_{Sreg} = 117$ equal discrete time samples.

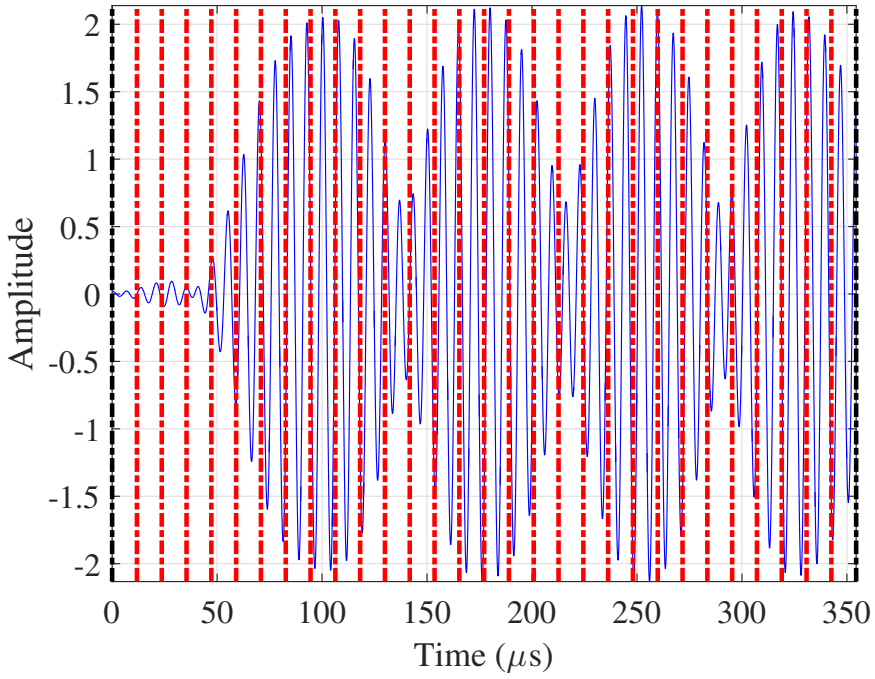


Figure 3.9. Representative Region of Interest (ROI) for single device Device Under Test (DUT) for Wired Signal Distinct Native Attribute (WS-DNA) and used for fingerprint generation. The ROI_{IH} contains $N_{IHsamp} = 3530$ discrete time samples divided into $N_{RIH} = 30$ subregions [12].

Figure 3.10 displays the ROI_{SPN} response with $N_{SPNsamp} = 9610$ discrete time samples that is divided into $N_{RSPN} = 43$ subregions, with each N_{RSPN} subregion containing $N_{Sreg} = 223$ equal discrete time samples. Note that $N_{Sreg} = 223$ may not be equal between DUT categories.

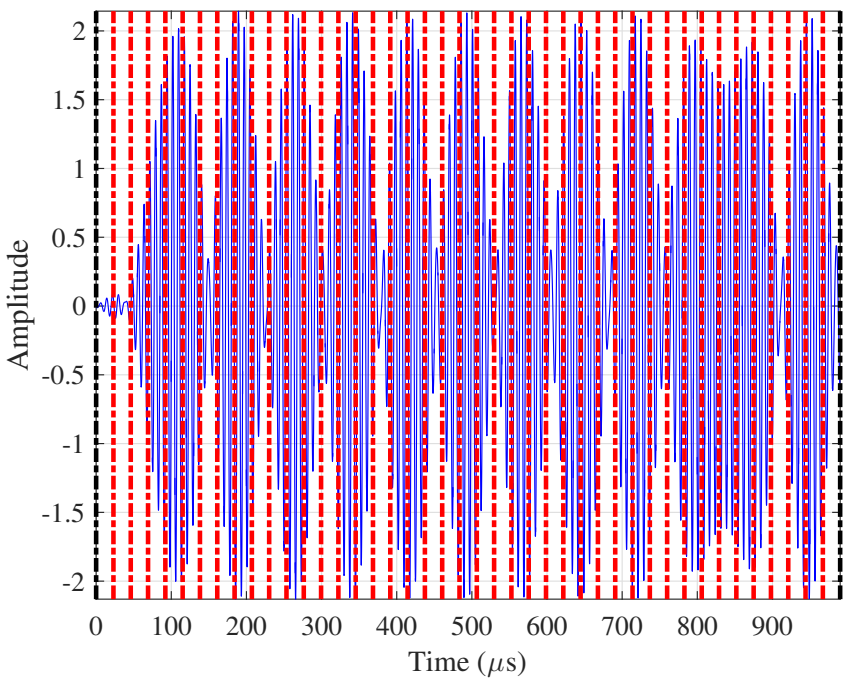


Figure 3.10. Representative Region of Interest (ROI) for Simulcasting PLC Network (SPN) Device Under Test (DUT) for Wired Signal Distinct Native Attribute (WS-DNA) and used for fingerprint generation. The ROI_{SPN} contains $N_{SPNsamp} = 9610$ discrete time samples divided into $N_{RSPN} = 43$ subregions [12].

As described in Section 2.4, composite WS-DNA fingerprints $\boldsymbol{F_C^{WS}}$ (2.9) are created for each Time Domain (TD) ROI by: 1) calculating, centering, and normalizing instantaneous amplitude $a(i)$, phase $\phi(i)$, and frequency $f(i)$, 2) forming regional fingerprints $F_{R_i}^{WS}$, (2.7) from calculating standard deviation (σ), variance (σ^2), skewness (γ), and kurtosis (κ) for each TD ROI sequence, 3) concatenating regional fingerprints to form instantaneous response vectors $\boldsymbol{F^{WS}}_{a,\phi,f}$ (2.8), and 4) concatenating the instantaneous response vectors $\boldsymbol{F^{WS}}_{a,\phi,f}$ into a single composite WS-DNA fingerprint $\boldsymbol{F_C^{WS}}$ [44, 56, 59].

The total number of features present in the final composite WS-DNA fingerprint depend on the number of subregions N_R, which instantaneous TD responses N_{Resp} are calculated, and which statistical features N_{Stat} are calculated. For both DUT

categories ROI, $N_{Resp} = 3$ instantaneous TD responses $a(i)$, $\phi(i)$, and $f(i)$ are calculated along with $N_{Stat} = 4$ statistical features (σ), (σ^2), (γ), and (κ). For the single device DUT category using ROI_{IH}, $N_{RIH} = 30$ subregions are used resulting in $N_{IH_{Feats}} = N_{Resp} \times N_{Stat} \times (N_{RIH} + 1) = 3 \times 4 \times 31 = 372$ features [12]. In the SPN category over ROI_{SPN}, $N_{RSPN} = 43$ subregions are used resulting in $N_{IH_{Feats}} = N_{Resp} \times N_{Stat} \times (N_{RIH} + 1) = 3 \times 4 \times 44 = 528$ features [58].

3.6 Training and Classification

With the single device DUT category a total of $N_{P_{IH}} = 2,000$ collected emissions per class were used in generating WS-DNA fingerprints. Under the SPN DUT category, $N_{P_{SPN}} = 1,000$ collected emissions per class were used in fingerprinting. In an effort to improve the robustness and reliability of model development, $M_{MCz} = 5$ Monte Carlo AWGN realizations were created at each desired $SNR_{aIH} \in [-10\ 50]$ dB and $SNR_{aSPN} \in [-10\ 54]$ dB, as mentioned in Section 3.3.4. This equates to a total of $N_{F_{IH}} = 10,000$ and $N_{F_{SPN}} = 5,000$ total fingerprints. Half of each category of fingerprints were used to create *Training* fingerprints $N_{Trn_{IH}} = 5,000$ and $N_{Trn_{SPN}} = 2,500$, with the other half used to generate *Testing* fingerprints $N_{Tst_{IH}} = 5,000$ and $N_{Tst_{SPN}} = 2,500$. The *Training* fingerprints were chosen, such that every other fingerprint is selected for *Training* with the remaining selected for *Testing*. The *Training* fingerprints $N_{Trn_{IH}}$ and $N_{Trn_{SPN}}$ will be used for model development. The *Testing* fingerprints $N_{Tst_{IH}}$ and $N_{Tst_{SPN}}$ fingerprints are not used in model development consistent with traditional assessment of classifiers.

To further increase reliability, K-fold classification validation is used in training as described in 2.5.3. A value of $K = 5$ is used and is consistent with common statistical methods [75]. This technique is used to validate the classifier model such that the set of *Training* of fingerprints is divided into K equally sized subsets.

$K-1$ subsets are used to perform classifier *Training* and the withheld subset used for validation of the model. This process is repeated K times until all subsets have been withheld and used for model testing. The average Average Cross-Class Percent Correct Classification (%C) performance is calculated for each K trial and the highest performing classification model is chosen.

MDA/ML classification is implemented as previously presented in Section 2.5 [53]. Both DUT categories are considered using $N_{c_{IH}} = 6$ and $N_{c_{SPN}} = 24$ classes respectively along with a 6 class subset of the SPN DUT such that the *peripherals* devices and their positions are identical in each SPN with the exception that each configuration includes the exchange of the 6 Insteon Hub devices. To further clarify this, the 6 class SPN DUT subset includes classes $N_{cSPN} = 1, 5, 9, 13, 17, 21$ with reference to Table 3.3 in Section 3.2.1.2. The number of *Training* fingerprints being $N_{Trn_{IH}} = 5,000, N_{Trn_{SPN}} = 2,500$ and the number of *Testing* fingerprints being $N_{Tst_{IH}} = 5,000, N_{Tst_{SPN}} = 2,500$ per SNR level respective to the two DUT categories.

Average %C versus SNR is plotted for each DUT category and used to display classification performance. Confusion matrices consistent with [50] are also used to emphasize %C performance at specific SNR levels that display the correct classification in diagonal slots with any misclassification appearing in non-diagonal slots. The non-diagonal slots highlight specific classes that are more commonly misclassified with other classes.

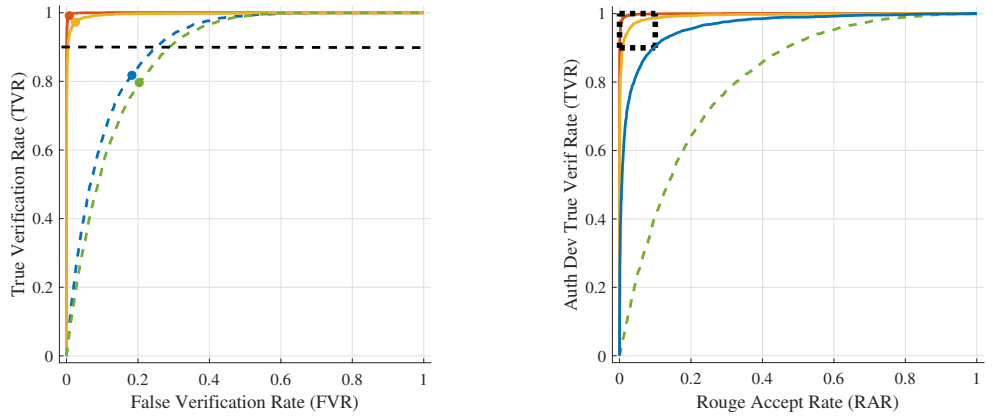
3.7 Class Verification

This Section describes how class verification is implemented as presented in Section 2.6. After model development outlined in Section 3.5 is used, euclidean distance is implemented to determine similarity between devices for verification. A key aspect of device ID verification is the choosing of a rogue class and testing how well the

model performs at accepting or rejecting the rogue class. This is done by selecting a single authorized class from the pool of authorized classes for each DUT category and labeling that class as rogue. Thus, $N_{R_{IH}} = 1$ rogue class is chosen such that $N_{R_{IH}} \in N_{c_{IH}}$ and $N_{R_{SPN}} = 1$ rogue class is chosen such that $N_{R_{SPN}} \in N_{c_{SPN}}$. The rogue class' *Testing* fingerprints are then used to assess rogue class accept/reject performance. In addition, the same rogue detection process is also performed on the SPN DUT subset as a 6 class problem instead of 24 class problem.

3.7.1 Device ID Verification Assessment.

To determine how well an authorized device can gain access to a PLC network, test statistics Z_v are calculated for *Training* and *Testing* fingerprints of authorized devices or each DUT category. These test statistics are used to create a Probabilty Mass Function (PMF) for each *Training* and *Testing* set. These PMFs in turn are used to create Receiver Operating Characteristic (ROC) curves. As discussed in Section 2.6, the ROC curves are used to determine verification performance. Figure 3.11 displays example ROC curves that will be used to present verification results in Chapter IV.



(a) True Verifiaction Rate (TVR) vs Flase Verifiaction Rate (FVR)

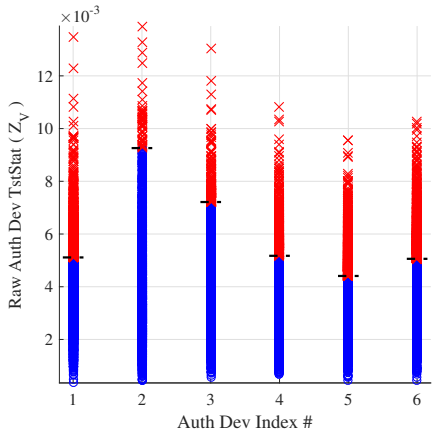
(b) TVR vs Rogue Accept Rate (RAR)

Figure 3.11. Typical Receiver Operating Characteristic (ROC) curves for (a) True Verifiaction Rate (TVR) vs Flase Verifiaction Rate (FVR) plot with dashed line representing 90% TVR and solid dots as the Equal Error Rate (EER) for each class and (b) TVR vs Rogue Accept Rate (RAR) with dashed block representing the Equal Error Rate (EER) of 10%. Both curves have solid curves (Accepted) and dashed curves (Rejected).

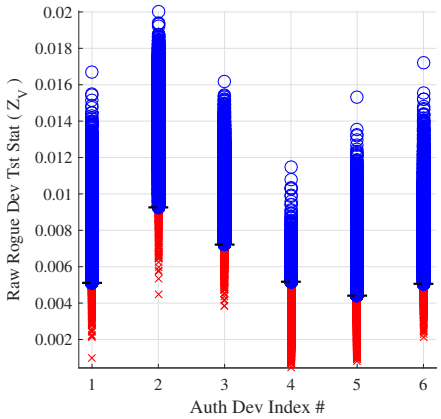
An arbitrary benchmark of EER = 10% is chosen as the criteria for a genuine class to gain access to a PLC or SPN network based on TVR and FVR such that $FVR < 0.1$ and $TVR > 0.9$. The same $EER = 10\%$ benchmark is used in determining how well a rogue class can access a PLC or SPN network based on TVR and RAR such that $RAR > 0.1$ and $TVR > 0.9$. With respect to the ROC curves, they result in the class being accepted or rejected. Solid curves are either authorized classes that have been accepted or rogue classes that have been rejected and dashed curves represent authorized classes that have been rejected or rogue classes that have been accepted. In summary, the solid curves represent a positive, or "True" outcome, whereas the dashed curves represent a negative, or "False" outcome.

An alternative view of a ROC curve can be seen in Figure 3.12. These euclidean distance test statistics charts are created by plotting the test statistics that make up the ROC curve's PMF. Figure 3.12a shows a chart for authorized class test statis-

tics with circles representing an authorized class acceptance and X's representing an authorized class rejection. Figure 3.12b shows a chart for rogue class test statistics with circles representing a rogue class rejection and X's representing a rogue class acceptance.



(a) Authorized Class Euclidian Distance Test Statistics



(b) Rogue Class Euclidian Distance Test Statistics

Figure 3.12. Euclidean distance test statistics for (a) authorized class test statistics with blue circles representing acceptance and X's representing rejection and (b) rogue class test statistics with circles representing rejection and X's representing acceptance. Dashed lines for each represents the threshold value corresponding the Receiver Operating Characteristic (ROC) curve's Equal Error Rate (EER).

IV. Results

4.1 Introduction

This chapter present results for classification and verification of Wired Signal Distinct Native Attribute (WS-DNA) fingerprinting based on the single device and Simulcasting PLC Network (SPN) Device Under Test (DUT) categories with the techniques described in Chapter III. The WS-DNA results created are consistent with previous work [34, 56] as described in Section 3.5. Classification results are presented in Section 4.2 followed by verification in Section 4.3 for single device DUT and SPN DUT categories. Classification results from Multiple Discriminate Analysis Maximum Likelihood (MDA/ML) discrimination are based on the methodology described in Section 3.6 for both $N_{c_{IH}} = 6$ and $N_{c_{SPN}} = 24$ authorized class model DUT categories as well as the SPN DUT subset. Rogue class verification is presented for both DUT categories and subset, with $N_{c_{IH}} = 6$ and $N_{c_{SPN}} = 24$ authorized classes and $N_{R_{IH}} = 1$ and $N_{R_{SPN}} = 1$ rogue classes as described in Section 3.7.

4.2 Classification

This section provides classification results for both single device and SPN DUT categories. Average $\%C = 90\%$ is achieved at 36 dB for single device category and at 50 dB for the SPN category subset. Average $\%C = 90\%$ is not achieved for the entire set in the SPN category with the highest achieved being $\%C = 56\%$ at 54 dB.

4.2.1 Single Device DUT.

Single device DUT category classification results are created for $N_{c_{IH}} = 6$ classes with $N_{F_{IH}} = 10,000$ total fingerprints utilized. These total fingerprints are equally

split with $N_{Trn_{IH}} = 5,000$ fingerprints used for *Training* and $N_{Tst_{IH}} = 5,000$ fingerprints used for *Testing*. The results are presented with a plot of Average Cross-Class Percent Correct Classification (%C) versus Signal-to-Noise Ratio (SNR) and a confusion matrix at $SNR = [30, 40]$ dB levels. Figure 4.1 shows a plot of %C versus SNR for the single device DUT category and with average $\%C = 90\%$ achieved at 36 dB and all six classes achieving 90% correct classification at 40 dB [12]. An average of %C = 99% is acahved at SNR $\geq$ 46 dB [12]. Confidence Intervals (CIs) were used to access statistical relevance based on $CI = 95\%$. At $SNR \geq 26$ dB the %C results were statistically different for each device based on $CI = 95\%$ and are omitted from the figure for clarity.

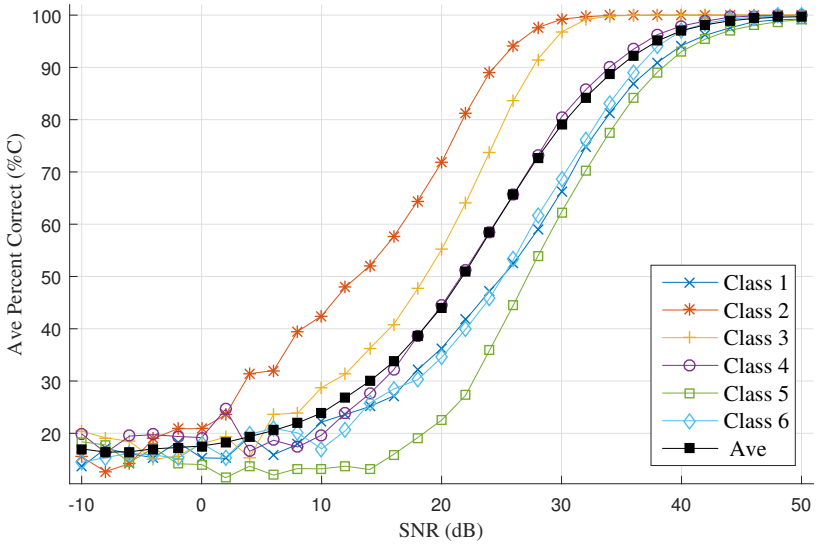


Figure 4.1. Single device Average Cross-Class Percent Correct Classification (%C) vs Signal-to-Noise Ratio (SNR) [12]. At $SNR \geq 26$ dB the Average Cross-Class Percent Correct Classification (%C) results were statistically different for each device based on Confidence Interval (CI) = 95% and are omitted from the figure for clarity.

Table 4.1 displays the confusion matrix for $SNR = [30, 40]$ dB levels presented as %C at 40 dB/30 dB [12]. This highlights that classes 1, 5, and 6 are more often misclassified as with one another than 2, 3, and 4. This can be caused by similarities

in the components of the devices that cause features to be more alike. After experimental collections were completed the individual Hub devices were dissembled and the visible components inspected. No distinguishable dissimilarities were found, each visible component was marked with the same manufacturer number, however nothing pertaining to a lot number could be found. Thus, even though each component within each device has the same model, the lot number may vary slightly between components with devices 1, 5, and 6 having more similar lot numbers than the others. This would mean that features present in the fingerprints of 1, 5, and 6 are more similar and thus more confused with one another due to more similar components [51].

Table 4.1. Single Device DUT Confusion Matrix for $SNR = 40/30$ dB with 5,000 Trials Per Class. Presented as Average Cross-Class Percent Correct Classification (%C) at 40 dB/30 dB [12].

$N_{C_{SD}}$	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6
Class 1	94.19/66.31	0.0/0.0	0.0/.20	0.0/.16	3.47/17.19	2.34/16.14
Class 2	0.0/0.0	100/99.24	0.0/.40	0.0/.36	0.0/0.0	0.0/0.0
Class 3	0.0/.02	.02/.90	99.98/96.78	0.0/.85	0.0/.87	0.0/.58
Class 4	0.0/.32	0.0/.98	0.0/.95	97.93/80.52	2.07/17.01	0.0/.22
Class 5	3.34/11.14	0.0/0.0	0.0/.86	2.25/15.48	93.04/62.33	1.37/10.19
Class 6	1.85/14.95	0.0/0.0	0.0/.56	0.0/14	1.12/15.60	97.03/68.75

4.2.2 SPN DUT.

SPN DUT category classification results are created for $N_{c_{IH}} = 24$ classes as well as the 6 class subset fo the SPN DUT with $N_{F_{SPN}} = 5,000$ total fingerprints utilized. These total fingerprints are equally split with $N_{Trn_{SPN}} = 2,500$ fingerprints used for *Training* and $N_{Tst_{SPN}} = 2,500$ fingerprints used for *Testing*. Results for all 24 classes are presented along with results for a subset that contains only classes 1, 5, 9, 13, 17, and 21. Referring to Table 3.3 this subset of classes contain the same *peripheral* devices for each class with only the *transmit* device changing. The results are presented with a plot of %C versus SNR and a confusion matrix at $SNR = 50$ dB. Figure 4.2 shows a plot of %C versus SNR for the subset of the SPN DUT category

with average $\%C = 90\%$ achieved at 50 dB [58]. CIs were used to access statistical relevance based on $CI = 95\%$. At $SNR \geq 30$ dB the %C results were statistically different for each device based on $CI = 95\%$ and are omitted from the figure for clarity.

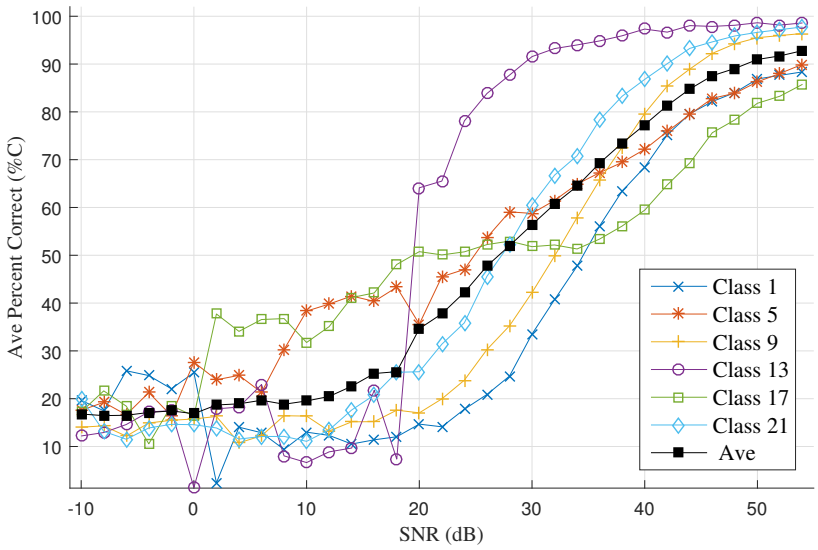


Figure 4.2. Simulcasting PLC Network (SPN) Device Under Test (DUT) Subest Average Cross-Class Percent Correct Classification (%C) vs Signal-to-Noise Ratio (SNR) [12]. At $SNR \geq 30$ dB the Average Cross-Class Percent Correct Classification (%C) results were statistically different for each device based on Confidence Interval (CI) $= 95\%$ and are omitted from the figure for clarity.

Table 4.2 displays the confusion matrix for $SNR = 50$ dB [58]. This shows that class 1 and class 17 are most often misclassified as one another with 1 misclassified as 17 7.32% of the time and 17 misclassified as 1 9.20% of the time. Class 1 and 17 of the SPN DUT category contain the same single Hub devices that were used in class 1 and 5 respectively of the single device DUT category. Thus, the higher confusion of these classes is consistent with the single device DUT category. This presents the idea that the *transmit* device in a SPN is a greater source of fingerprint features used in discrimination.

Table 4.2. SPN Confusion Matrix Subset for $SNR = 50$ dB [58].

$N_{C_{SPN}}$	Class 1	Class 5	Class 9	Class 13	Class 17	Class 21
Class 1	89.60	2.24	0.28	0.32	7.32	0.24
Class 5	4.72	90.80	2.56	1.16	0.76	0
Class 9	0.16	2.28	96.20	0.16	1.16	0.04
Class 13	0	0.12	0.40	98.56	0.52	0.40
Class 17	9.20	0.88	0.32	0.68	85.44	3.48
Class 21	0.20	0	0	0.12	2.36	97.32

Figure 4.3 displays a plot of %C versus SNR for all 24 classes of the SPN DUT category with $\%C = 90\%$ not being achieved. This can be mostly attributed to the shear number of categories. CIs were again used to access statistical relevance based on $CI = 95\%$. At $SNR \geq 48$ dB the %C results were statistically different for each device based on $CI = 95\%$ and are omitted from the figure for clarity.

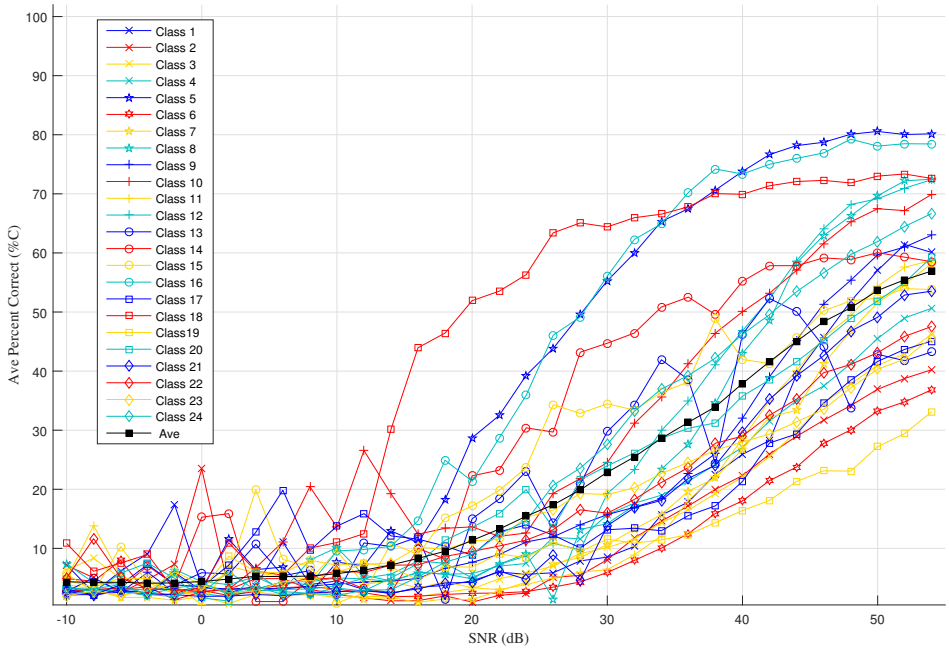


Figure 4.3. Simulcasting PLC Network (SPN) Device Under Test (DUT) Average Cross-Class Percent Correct Classification (%C) vs Signal-to-Noise Ratio (SNR). At $SNR \geq 48$ dB the Average Cross-Class Percent Correct Classification (%C) results were statistically different for each device based on Confidence Interval (CI) $= 95\%$ and are omitted from the figure for clarity.

Table 4.3 displays the confusion matrix for $SNR = 50$ dB for all 24 classes of the SPN DUT category. The results shown in the Table 4.3 demonstrate that the classes are less discriminable in the configurations where the *transmit* device is held constant as the control and the *peripheral* devices serve as the variable. This implies that the *transmit* device features contain more device-to-device unique attributes contributing to discriminability than the *peripheral* devices. Also, the SPNs that contain Hubs 1 and 5 are more often confused with one another than SPN that contain other Hubs. This is consistent with single device DUT results. This is consistent with results from the SPN DUT category subset. SPNs 21, 22, 23, and 24 have a higher confusion rate with SPN 18, however the inverse is not true. SPN 18 does not have a higher confusion rate with SPNs 21, 22, 23, and 24. This suggests that there is something that the classifiers have used that allows the model to confuse the classes with each other one way, but not confusing them the other way. This could be caused by human error or some other anomaly that appeared during the collection of theses classes.

Table 4.3. SPN DUT Confusion Matrix. Dark Green Diagonal Is Correct with Non-Diagonal Misclassification. Shading Ranges From Less Misclassification (Light Green) to More Misclassified (Red).

	Hub #		Hub 1				Hub 2				Hub 3				Hub 4				Hub 5				Hub 6			
Hub #		N_{Ps}	N_{123}	N_{423}	N_{143}	N_{124}	N_{123}	N_{423}	N_{143}	N_{124}	N_{123}	N_{423}	N_{143}	N_{124}	N_{123}	N_{423}	N_{143}	N_{124}	N_{123}	N_{423}	N_{143}	N_{124}	N_{123}	N_{423}	N_{143}	N_{124}
	N_{Ps}	N_{cSPN}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Hub 1	N_{123}	1	57.64	0.36	16.52	0.88	5.72	0.20	0.08	0.00	0.24	0.00	0.04	0.16	0.08	0.28	0.04	0.00	12.68	3.96	0.36	0.28	0.08	0.16	0.04	0.20
	N_{423}	2	0.60	43.64	8.44	6.88	0.12	1.84	1.24	2.28	0.20	0.16	0.28	1.52	0.20	0.56	0.00	0.00	0.84	20.60	0.84	8.28	0.24	1.04	0.04	0.16
	N_{143}	3	11.76	4.16	45.12	5.32	1.16	0.60	0.20	0.04	0.20	0.00	0.00	0.20	0.16	0.08	0.04	0.00	8.28	13.44	3.44	5.64	0.04	0.04	0.04	0.04
	N_{124}	4	0.56	5.20	13.00	48.92	0.00	0.08	1.40	2.60	0.08	0.04	0.00	1.20	1.12	0.68	0.00	0.00	0.96	7.64	0.88	14.08	0.16	0.08	0.16	1.16
Hub 2	N_{123}	5	5.92	0.04	1.96	0.28	81.72	1.72	1.96	1.28	1.00	0.28	0.48	0.56	0.48	0.32	0.00	0.72	0.32	0.88	0.00	0.00	0.00	0.00	0.08	0.00
	N_{423}	6	0.44	4.36	1.04	0.56	15.44	35.36	22.96	9.80	1.60	0.32	4.72	0.96	0.20	0.04	0.04	0.36	0.04	1.52	0.00	0.00	0.04	0.20	0.00	0.00
	N_{143}	7	0.88	1.16	1.12	0.84	6.36	6.00	53.96	22.92	1.08	0.08	1.28	1.16	0.08	0.04	0.00	0.16	0.00	2.52	0.32	0.04	0.00	0.00	0.00	0.00
	N_{124}	8	0.00	1.32	0.00	3.84	4.36	2.16	9.80	73.08	0.00	0.20	0.32	1.76	0.32	0.04	0.00	0.00	0.00	2.56	0.00	0.24	0.00	0.00	0.00	0.00
Hub 3	N_{123}	9	0.12	0.12	1.00	0.24	2.08	1.24	0.20	0.00	66.92	7.76	8.88	9.32	0.08	0.20	0.04	0.00	0.52	1.20	0.04	0.00	0.04	0.00	0.00	0.00
	N_{423}	10	0.24	1.28	0.12	0.44	0.28	0.92	0.16	0.32	7.20	64.60	18.68	4.88	0.00	0.28	0.04	0.32	0.00	0.20	0.04	0.00	0.00	0.00	0.00	0.00
	N_{143}	11	0.04	1.24	0.24	0.52	1.84	1.52	1.20	0.72	4.48	9.44	61.24	16.16	0.48	0.20	0.36	0.00	0.08	0.24	0.00	0.00	0.00	0.00	0.00	0.00
	N_{124}	12	0.00	1.20	0.28	0.80	0.72	0.20	0.88	1.96	2.04	4.52	16.12	69.92	0.52	0.04	0.04	0.04	0.00	0.72	0.00	0.00	0.00	0.00	0.00	0.00
Hub 4	N_{123}	13	0.04	0.44	0.12	0.88	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	63.80	6.12	12.28	16.12	0.04	0.00	0.08	0.00	0.00	0.00	0.00	0.08
	N_{423}	14	0.00	0.16	0.08	0.00	0.04	0.00	0.00	0.00	0.16	0.04	0.00	0.00	10.00	60.52	7.60	21.16	0.16	0.00	0.04	0.00	0.00	0.00	0.04	0.00
	N_{143}	15	0.12	0.04	0.12	0.04	0.12	0.16	0.00	0.00	0.00	0.24	0.12	0.04	13.44	9.56	53.36	22.40	0.12	0.00	0.12	0.00	0.00	0.00	0.00	0.00
	N_{124}	16	0.08	0.04	0.00	0.04	0.56	0.16	0.00	0.00	0.56	0.20	0.00	0.00	5.12	6.88	5.12	81.04	0.16	0.00	0.04	0.00	0.00	0.00	0.00	0.00
Hub 5	N_{123}	17	7.56	0.52	4.88	0.60	1.80	0.08	0.00	0.00	0.08	0.00	0.00	0.08	0.08	0.56	0.08	0.00	44.36	30.56	5.40	2.16	0.64	0.36	0.04	0.16
	N_{423}	18	0.44	4.76	0.44	0.00	0.48	0.04	0.20	0.48	0.16	0.00	0.20	0.08	0.00	0.00	0.00	0.00	4.80	78.32	2.60	4.60	0.68	1.00	0.08	0.64
	N_{143}	19	1.28	2.12	5.64	1.48	0.00	0.04	0.20	0.00	0.04	0.08	0.00	0.04	0.12	0.12	0.00	0.04	8.12	40.56	31.36	5.80	0.88	1.16	0.48	0.44
	N_{124}	20	0.00	1.60	2.64	2.28	0.00	0.00	0.00	0.20	0.04	0.00	0.00	0.12	0.00	0.00	0.00	0.00	0.48	35.04	1.52	54.16	0.04	0.56	0.24	1.08
Hub 6	N_{123}	21	0.12	0.16	0.04	0.00	0.12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.20	11.92	0.24	0.20	54.32	13.48	10.04	8.16
	N_{423}	22	0.04	0.96	0.04	0.04	0.00	0.00	0.16	0.00	0.00	0.00	0.00	0.00	0.04	0.00	0.00	0.00	0.32	20.72	1.76	1.16	18.96	46.04	7.08	2.68
	N_{143}	23	0.04	0.32	0.24	0.36	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.08	0.00	0.00	0.00	0.92	19.72	0.44	2.16	20.36	8.76	40.04	6.56
	N_{124}	24	0.12	0.28	1.00	0.48	0.00	0.04	0.00	0.00	0.00	0.00	0.00	0.00	0.60	0.04	0.00	0.00	0.04	13.36	0.32	1.44	13.08	2.28	4.12	62.80

Figure 4.4 displays the average %C for each DUT category as well as the 6 class subset of the SPN subset. Performance between the single device and SPN subset where the *peripheral* device remain constant and the *transmit* device are exchanged show performance drop of approximately 10% in average %C at $SNR = 50$ dB. This drop in average %C is associated to the *peripheral* device present on the Power Line Communication (PLC) network acting simply as an additional "noise" source. This increase in "noise" will degrade average %C performance just as traditional noise sources like Additive White Gaussian Noise (AWGN) thermal noise will degrade performance.

The full set of classes in the SPN DUT category has an approximate 35% decrease in average %C performance from SPN DUT subset curve at $SNR = 50$ dB when compared to the 6 class configuration. This drop is associated to the larger number of classes present in the discrimination.

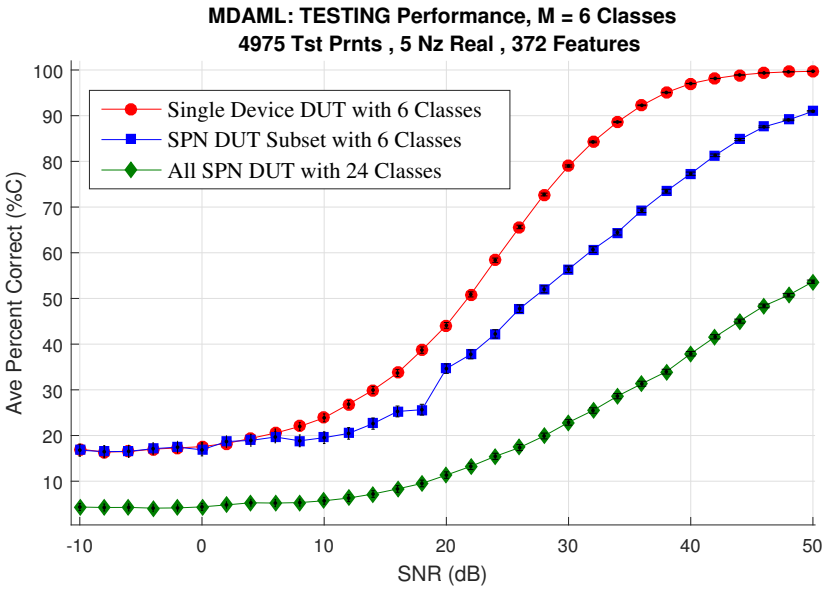


Figure 4.4. Average Cross-Class Percent Correct Classification (%C) vs Signal-to-Noise Ratio (SNR) averages for single device and Simulcasting PLC Network (SPN) Device Under Test (DUT) categories. Statistical relevance was determined with Confidence Interval (CI) = 95% shown as error bars.

4.3 Verification

This section provides verification results for both single device and SPN DUT categories. For the single device DUT category all classes achieve 90% True Verifiaction Rate (TVR) for verification and a Equal Error Rate (EER) = 10% for rouge detection at 40 dB. In the subset of the SPN DUT category classes 5, 9, 13, and 21 achieve 90% TVR for verification and all classes have a EER = 10% in rouge detection at 50 dB. For the entire set in the SPN DUT category only classes 13, 15, and 16 achieve 90% TVR in verification and classes 13, 14, 15, and 16 achieve a EER = 10% in rouge detection at 50 dB.

4.3.1 Single Device DUT.

Single device DUT category verification results are created for $N_{c_{IH}} = 6$ classes with $N_{F_{IH}} = 10,000$ total fingerprints utilized. These total fingerprints are equally split with $N_{Trn_{IH}} = 5,000$ fingerprints used for *Training* and $N_{Tst_{IH}} = 5,000$ fingerprints used for *Testing*. The results are presented with Receiver Operating Characteristic (ROC) curves and euclidean distance test statistic charts at $SNR = [30, 40]$ dB levels. Figure 4.5 shows a ROC curve of TVR vs Flase Verifiaction Rate (FVR) at 30 dB SNR for the single device DUT category [58]. Classes 2 and 3 achieve 90% TVR versus 10% FVR with the rest falling short. Figure 4.6 displays the alternate view in the form of euclidean distance test statistic. At a simulated SNR of approximately 15 dB less than the average collected SNR of 45 dB, a third of the devices achieve 90% TVR with room for improvement as the simulated SNR increases.

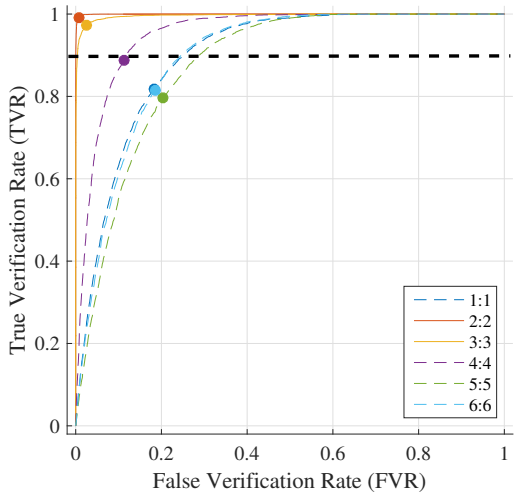
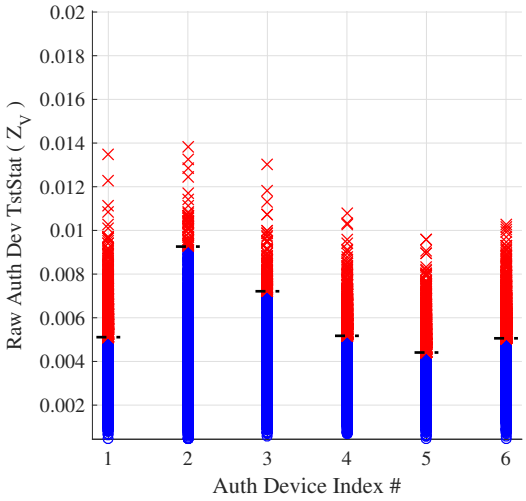


Figure 4.5. ID Verification Receiver Operating Characteristic (ROC) curves for single device Device Under Test (DUT) category at Signal-to-Noise Ratio (SNR) = 30 dB using an Euclidean distance measure of similarity. Classes 2 and 3 reach $TVR > 0.9$ and $FVR < 0.1$ criteria [12].



TVR = [81.86, 99.1, 97.14, 88.85, 78.2, 80.72]%

Figure 4.6. Euclidean distance test statistics for single device Device Under Test (DUT) category at Signal-to-Noise Ratio (SNR) = 30 dB. Dashed horizontal lines are device dependent $t_V(d)$ thresholds corresponding to Receiver Operating Characteristic (ROC) Equal Error Rate (EER) in Figure 4.5. Authorized device ID verification test statistics where blue circles indicate correct access granted and red X's indicate an incorrect access denied for $NTst = 5,000$ testing fingerprints per authorized device [12]. The True Verifiaction Rate (TVR) percent performance for each individual row statistic is also shown.

For rogue verification results, single device DUT class 4 is chosen as the rogue device. Figure 4.7 shows a ROC curve of TVR vs Rogue Accept Rate (RAR) at 30 dB SNR for the single device DUT category [12]. Classes 1, 2, 3, and 6 achieve an EER = 10%. The diagonal dashed line indicates that class 4 was not only accepted as an authorized device but also rejected as a rogue device. This is consistent with using an authorized device and labeling it a rogue for testing. Figure 4.8 displays the alternate view in the form of a Euclidean distance test statistic. As with the TVR vs FVR results at SNR = 30 dB there is room for improvement for rogue detection at an SNR much lower than the collected SNR.

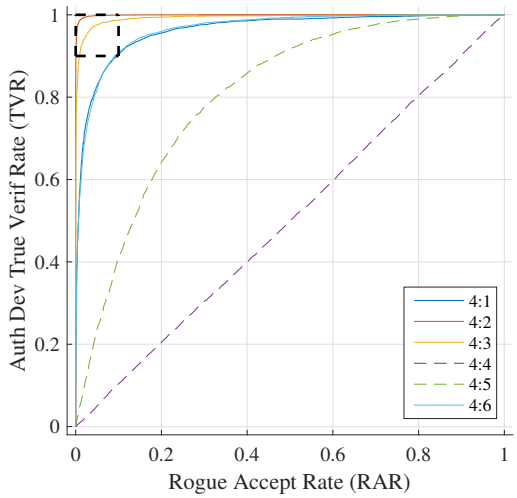
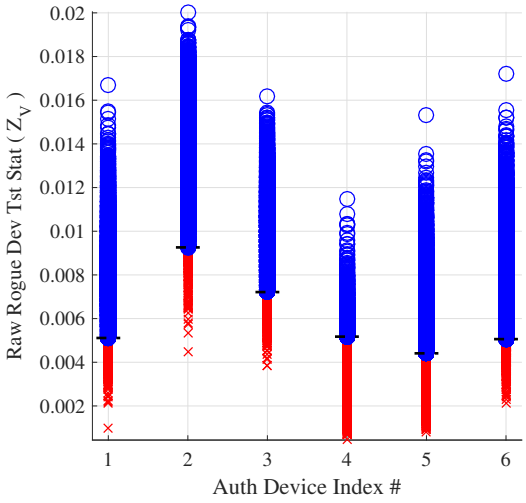


Figure 4.7. Rogue device verification Receiver Operating Characteristic (ROC) curves for single device Device Under Test (DUT) category with Signal-to-Noise Ratio (SNR) = 30 dB using an Euclidean distance measure of similarity. Rogue device class 4 rejection achieves $EER = 10\%$ for classes 1, 2, 3, and 6 [12].



RRR = [95.43, 98.25, 95.29, 11.21, 67.87, 95.18]%

Figure 4.8. Euclidean distance test statistics for single device Device Under Test (DUT) category rogue devices at Signal-to-Noise Ratio (SNR) = 30 dB. Dashed horizontal lines are device dependent $t_V(d)$ thresholds corresponding to Receiver Operating Characteristic (ROC) Equal Error Rate (EER) in Figure 4.7. Rogue device (class 4) 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 $NTst = 5,000$ testing fingerprints, with class 4 presenting a false ID in place of an authorized device [12]. The Rogue Reject Rate (RRR) percent performance for each individual row statistic is also shown.

Figure 4.9 shows a ROC curve of TVR vs FVR at 40 dB SNR for the single device DUT category [12]. All classes achieve 90% TVR. Figure 4.10 displays the alternate view in the form of a euclidean distance test statistic. With a simulated SNR of only 5 dB less than the average collected SNR, these results indicate that not much improvement can be made with respect to the 90% TVR threshold as all devices have achieved it.

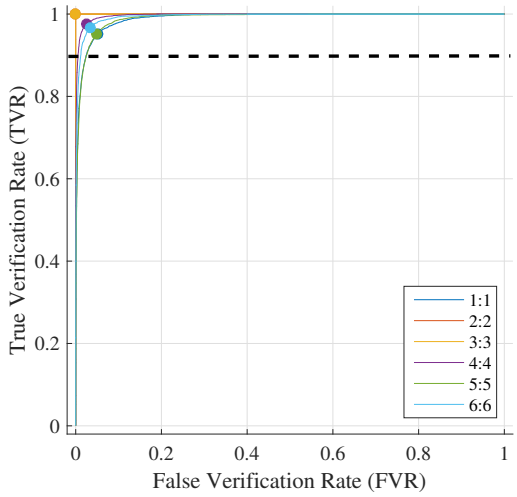
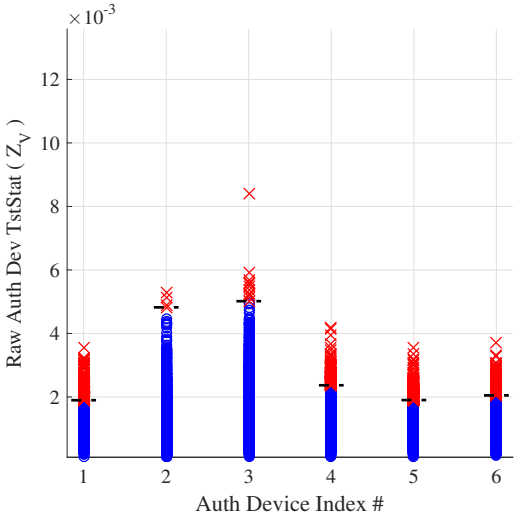


Figure 4.9. ID Verification Receiver Operating Characteristic (ROC) curves for single device Device Under Test (DUT) category at Signal-to-Noise Ratio (SNR) = 40 dB using an Euclidean distance measure of similarity. All classes reach $TVR > 0.9$ and $FVR < 0.1$ criteria [12].



TVR = [94.77, 99.92, 99.76, 97.26, 96.78]%

Figure 4.10. Euclidean distance test statistics for single device Device Under Test (DUT) category at Signal-to-Noise Ratio (SNR) = 40 dB. Dashed horizontal lines are device dependent $t_V(d)$ thresholds corresponding to Receiver Operating Characteristic (ROC) Equal Error Rate (EER) in Figure 4.9. Authorized device ID verification test statistics where blue circles indicate correct access granted and red X's indicate an incorrect access denied for $NTst = 5,000$ testing fingerprints per authorized device [12]. The True Verifiaction Rate (TVR) percent performance for each individual row statistic is also shown.

Figure 4.11 shows a ROC curve of TVR vs RAR at SNR = 40 dB for the single device DUT category with class 4, an actual authorized device representing the rogue device [12]. All classes achieve EER = 10%. The diagonal dashed line indicates that class 4 acceptance and rejection was no better than a random guess. This result is expected for class 4 as it was included in the training set for authorized devices. Figure 4.12 displays the alternate view in the form of a Euclidean distance test statistic. This is consistent with the TVR vs FVR results at SNR = 40 dB with all devices achieving EER = 10% with little room for improvement.

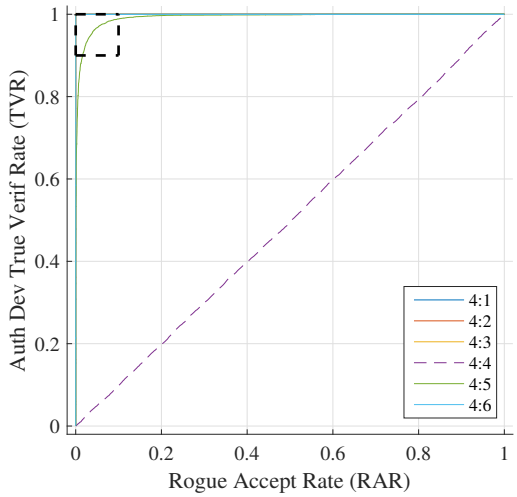
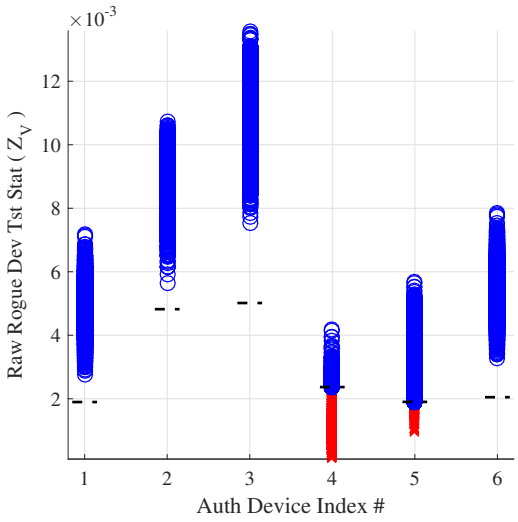


Figure 4.11. Rogue device verification Receiver Operating Characteristic (ROC) curves for single device Device Under Test (DUT) category with Signal-to-Noise Ratio (SNR) = 40 dB using an Euclidean distance measure of similarity. Rogue device class 4 rejection achieves $EER = 10\%$ for all non-rogue classes [12].



RRR = [100, 100, 100, 2.628, 96.32, 100]%

Figure 4.12. Euclidean distance test statistics for single device Device Under Test (DUT) category rogue devices at SNR = 40 dB. Dashed horizontal lines are device dependent $t_V(d)$ thresholds corresponding to Receiver Operating Characteristic (ROC) EER in Figure 4.11. Rogue device (class 4) 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 $NTst = 5,000$ testing fingerprints, with class 4 presenting a false ID in place of an authorized device [12]. The Rogue Reject Rate (RRR) percent performance for each individual row statistic is also shown.

4.3.2 SPN DUT.

SPN DUT category verification results are created for $N_{c_{IH}} = 24$ classes with $N_{F_{SPN}} = 5,000$ total fingerprints utilized. These total fingerprints are equally split with $N_{Trn_{SPN}} = 2,500$ fingerprints used for *Training* and $N_{Tst_{SPN}} = 2,500$ fingerprints used for *Testing*. Results for all 24 classes are presented along with results for a subset that contains only classes 1, 5, 9, 13, 17, and 21. Referring to Table 3.3 this subset of classes contain the same *peripheral* devices for each class with only the *transmit* device changing. The results are presented with ROC curves and euclidean distance test statistic charts at $SNR = 50$ dB for the subset of classes as well as the entire class set. Figure 4.13 shows a ROC curve of TVR vs FVR at 50 dB SNR for the SPN DUT category subset [58]. Classes 5, 9, 13, and 21 achieve 90% TVR with

the rest failing to meet the established benchmark. Figure 4.14 displays the alternate view in the form of a euclidean distance test statistic. The simulated SNR is within 1 dB of the average collected SNR of 51 dB which suggests that improvement will have to be achieved in a way other than increasing SNR.

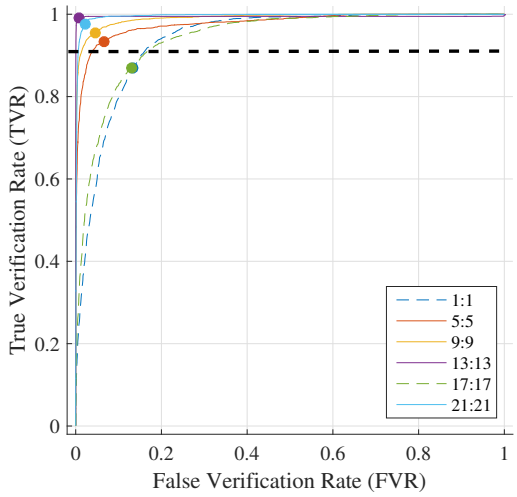
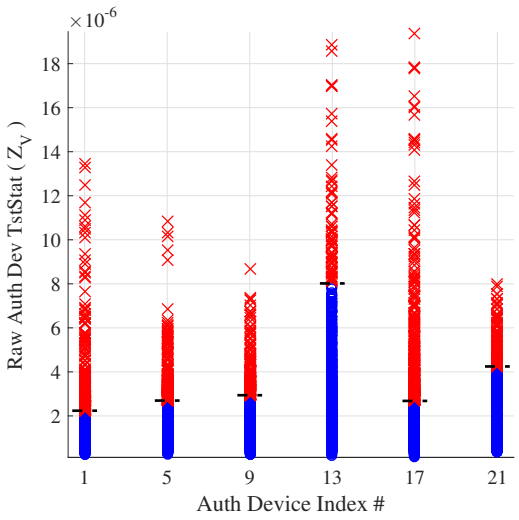


Figure 4.13. ID Verification Receiver Operating Characteristic (ROC) curves for Simulcasting PLC Network (SPN) Device Under Test (DUT) category subset at Signal-to-Noise Ratio (SNR) = 50 dB using an Euclidean distance measure of similarity. Classes 5, 9, and 13 reach $TVR > 0.9$ and $FVR < 0.1$ criteria [58].



TVR = [82.76, 90.32, 93.08, 94.92, 84.68, 96.56]%

Figure 4.14. Euclidean distance test statistics for Simulcasting PLC Network (SPN) Device Under Test (DUT) category subset at Signal-to-Noise Ratio (SNR) = 50 dB. Dashed horizontal lines are device dependent $t_V(d)$ thresholds corresponding to Receiver Operating Characteristic (ROC) Equal Error Rate (EER) in Figure 4.13. Authorized device ID verification test statistics where blue circles indicate correct access granted and red X's indicate an incorrect access denied for $NTst = 2,500$ testing fingerprints per authorized device [58]. The True Verifiaction Rate (TVR) percent performance for each individual row statistic is also shown.

For rogue verification results, SPN DUT class 9 is chosen as the rogue class. Figure 4.15 shows a ROC curve of TVR vs RAR at 50 dB SNR for the SPN DUT category [58]. All classes achieve an EER = 10%. The diagonal dashed line represents a random guess for class 9 and is as expected as class 9 was used during training of authorized devices. Figure 4.16 displays the alternate view in the form of a euclidean distance test statistic. Opposed to the TVR vs FVR results, all devices achieve EER = 10%.

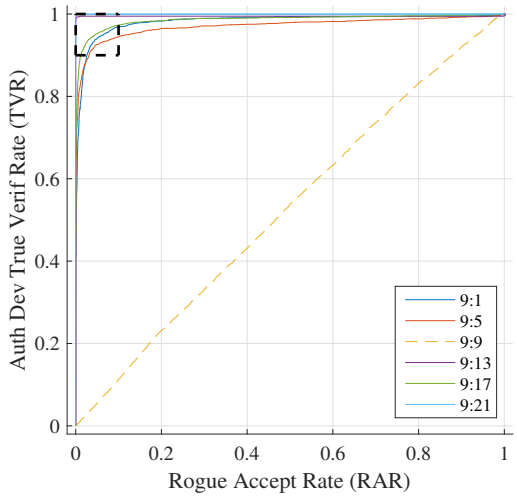
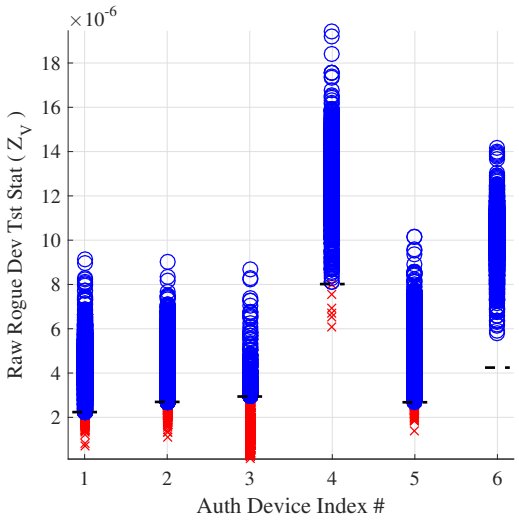


Figure 4.15. Rogue device verification Receiver Operating Characteristic (ROC) curves for Simulcasting PLC Network (SPN) Device Under Test (DUT) category subset with Signal-to-Noise Ratio (SNR) = 50 dB using an Euclidean distance measure of similarity. Rogue device class 9 rejection achieves $EER = 10\%$ for all non-rogue classes [58].



RRR = [98.06, 92.72, 5.78, 99.86, 99.24, 100]%

Figure 4.16. Euclidean distance test statistics for Simulcasting PLC Network (SPN) Device Under Test (DUT) category subset rogue devices at Signal-to-Noise Ratio (SNR) = 50 dB. Dashed horizontal lines are device dependent $t_V(d)$ thresholds corresponding to Receiver Operating Characteristic (ROC) Equal Error Rate (EER) in Figure 4.15. Rogue device (class 9) 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 $NTst = 2,500$ testing fingerprints, with class 9 presenting a false ID in place of an authorized device [58]. The Rogue Reject Rate (RRR) percent performance for each individual row statistic is also shown.

With the addition of the *peripheral* devices the performance of the SPN DUT subset is poorer when compared to the single device DUT category. This implies that the additional signal of the *peripheral* devices act simply as a "noise" source that degrades classification performance. It follows that the more devices that are added to the SPN network, the poorer the verification performance will be. Figure 4.17 shows a ROC curve of TVR vs FVR at 50 dB SNR for the SPN DUT category with all classes included. Only classes 13, 15, and 16 achieve 90% TVR. Figure 4.18 displays the alternate view in the form of a euclidean distance test statistic.

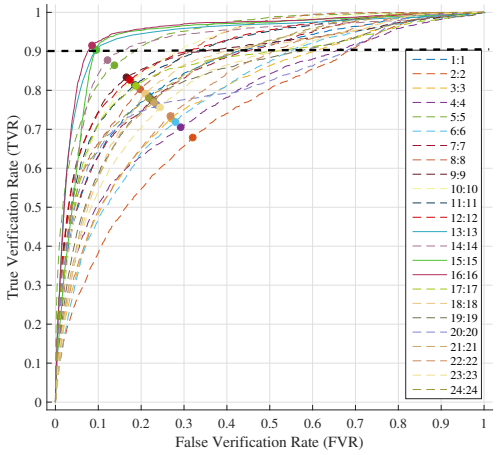
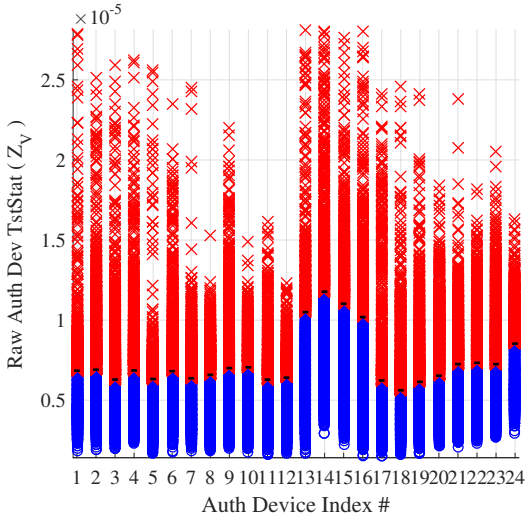


Figure 4.17. ID Verification Receiver Operating Characteristic (ROC) curves for Simulcasting PLC Network (SPN) Device Under Test (DUT) category at Signal-to-Noise Ratio (SNR) = 50 dB using an Euclidean distance measure of similarity. Classes 13, 15, and 16 reach $TVR > 0.9$ and $FVR < 0.1$ criteria.



TVR = [80.24, 69.36, 69.4, 69.16, 82.84, 68.92, 78.56, 78.6, 80.64, 83.32, 77.64, 82.52, 92.30, 79.36, 91.08, 90.96, 83.8, 76.08, 79.2, 75.48, 75.12, 72.32, 70.64,]%

Figure 4.18. Euclidean distance test statistics for Simulcasting PLC Network (SPN) Device Under Test (DUT) category at Signal-to-Noise Ratio (SNR) = 50 dB. Dashed horizontal lines are device dependent $t_V(d)$ thresholds corresponding to Receiver Operating Characteristic (ROC) Equal Error Rate (EER) in Figure 4.17. Authorized device ID verification test statistics where blue circles indicate correct access granted and red X's indicate an incorrect access denied for $NTst = 2,500$ testing fingerprints per authorized device. The True Verifiaction Rate (TVR) percent performance for each individual row statistic is also shown.

For rogue verification results, SPN DUT class 9 is chosen as the rogue class. Figure 4.19 shows a ROC curve of TVR vs RAR at 50 dB SNR for the SPN DUT category. Classes 13, 14, 15, and 16 achieve an EER = 10%. The diagonal dashed line indicates that class 9 achieved high TVR as well as low RAR. Figure 4.20 displays the alternate view in the form of a euclidean distance test statistic.

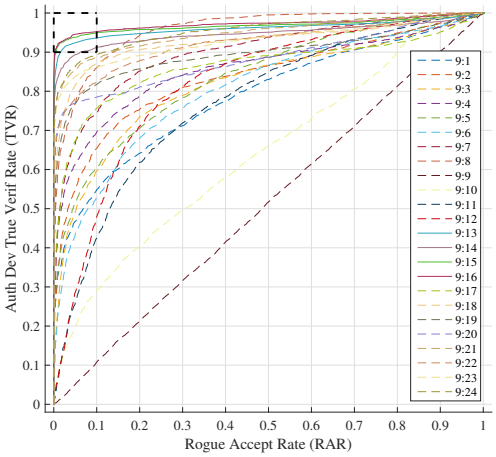


Figure 4.19. Rogue device verification Receiver Operating Characteristic (ROC) curves for Simulcasting PLC Network (SPN) Device Under Test (DUT) category with Signal-to-Noise Ratio (SNR) = 50 dB using an Euclidean distance measure of similarity. Rogue device class 9 rejection achieves $EER = 10\%$ for classes 13, 14, 15, and 16.

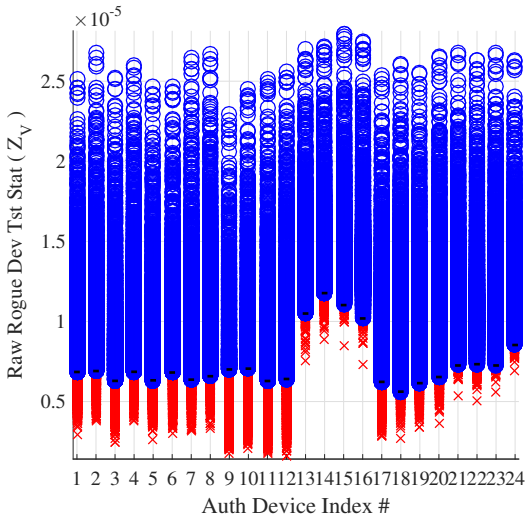


Figure 4.20. Euclidean distance test statistics for Simulcasting PLC Network (SPN) Device Under Test (DUT) category rogue devices at Signal-to-Noise Ratio (SNR) = 50 dB. Dashed horizontal lines are device dependent $t_V(d)$ thresholds corresponding to Receiver Operating Characteristic (ROC) EER in Figure 4.19. Rogue device (class 9) 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 $NTst = 2,500$ testing fingerprints, with class 9 presenting a false ID in place of an authorized device. The Rogue Reject Rate (RRR) percent performance for each individual row statistic is also shown.

The poor verification performance of the SPN DUT category can be partly attributed to the *peripheral* devices just as seen in the subset results, but also to the sheer number of classes used in verification. It is expected that as the number of classes increases, the harder it is for the model to classify them and thus perform verification.

V. Summary and Conclusions

This chapter supplies a summary and conclusions for the research presented in previous chapters. A summary of the main research aspects and results are discussed in Section 5.1 which covers Wired Signal Distinct Native Attribute (WS-DNA) fingerprinting using single device and Simulcasting PLC Network (SPN) Device Under Test (DUT) categories. Section 5.2 discusses relevant future works and the expansion of the research topic.

5.1 Research Summary

As more devices become interconnected with their influence directly affecting many networks, there is a need to increase intrusion detection and security. Power Line Communication (PLC) is an example of technology that has seen rapid growth in network connectivity without a corresponding focus on securing the network communication protocols. PLC can be used for large scale automation and control networks as well in home automation networks. The United States has seen a drastic increase in attacks on critical infrastructure in between 2009 and 2011 [8]. With PLC as a potential method of controlling any number of critical infrastructure systems, adequate security and intrusion detection must be investigated. In addition, PLC is currently used in various home automation systems to control various deceives around the home introducing another avenue for military and government personal to be targeted.

This research successfully demonstrated the WS-DNA fingerprinting approach in [53, 59] for wired PLC and SPN network communications. The results are consistent with previous wireless results found in [34, 44, 45]. Single device DUT category discrimination of $N_{c_{IH}}$ Insteon Hub devices were distinguishable with Average Cross-Class Percent Correct Classification (%C) = 90% at SNR = 36 dB. SPN DUT

category discrimination had much poorer performance when all $N_{cSPN} = 24$ classes are used with average %C = 90% never achieved which can be explained simply by the sheer number of classes being discriminated. Thus, when a subset of classes are extracted from the SPN DUT category such that the *peripheral* device are constant and the *transmit* device remains constant, average %C = 90% is achieved at $SNR = 50$ dB. This also illustrates that the majority of features that the WS-DNA process used to discriminate are found in the *transmit* device.

5.1.1 Conclusions.

WS-DNA was successfully implemented to fingerprint and discriminate the single device DUT and SPN DUT categories. The single device DUT category classification and verification results were consist with previously mentioned research and showed an improvement in performance when the simulated SNR was increased. Each single device achieved %C = 90% classification, however some of the single devices were more often confused with each other than others. This suggests the more similar devices are the more difficult the discrimination of the devices will be. It then follows that if a high level of discrimination can be obtained for very similar devices, it will be easier to discriminate devices that are less similar. For example, if two of the same device that are produced by the same manufacturer can be successfully discriminated, then two of the same kind of devices produced by different manufactures should be easier to discriminate.

When *peripheral* devices are added to the discrimination process and held consonant between classes, performance decreases. This suggests that the *peripheral* devices simply add a "noise" like effect that degrades the performance of the fingerprinting process. Thus, when the *peripheral* devices are held constant between classes there are no new identifiers introduced by the *peripheral* devices that the model can

use to discriminate.

When the *peripheral* devices are not held constant and the number of classes increase to 24, performance further degrades. However, the majority of this degradation can be attributed to the large number of classes begin discriminated. The results suggest that the *transmit* device in a SPN network provides the most features that are used in discrimination. When the *transmit* device is held constant and it is the *peripheral* devices that vary and produce the features, the performance is reduced. However, if the *transmit* device varies between classes along with the *peripheral* devices, the performance is increased.

5.2 Future Research

This section provides possible future work for the expansion of WS-DNA fingerprinting of PLC networks and SPNs.

5.2.1 Real World Expansion.

This research used the test fixture discussed in Chapter III to collect PLC and SPN communication signals. A natural expansion of this is to collect these types of signals in a real world home automation environment under real world conditions. This would allow other types of noise that would normally be present on the powerline of a home as well as provide varying distances between devices.

5.2.2 Configuration Control.

The ability to control configuration of devices on a PLC network is desirable. Implementing the same techniques of this research into the ability to discover the movement of devices on the network or other configuration changes is advisable. WS-DNA fingerprint could be used to detect if individual devices on a PLC network or

SPN have moved by detecting fingerprinting changes due to change in device position in an otherwise identical setup.

5.2.3 High Speed PLC.

This research focused on slower speed PLC communications like those used for home automation. A natural evolution is to implement the same processes for higher speed PLC communications like those used in Broadband over Power Line (BPL). The higher speeds and higher bit rate can increased the number of features present and improve performance.

5.2.4 Alternate Classifiers.

The classification technique of Multiple Discriminate Analysis Maximum Likelihood (MDA/ML) does not provide a relevance ranking for individual features, i.e., it does not provide any insight into how much influence individual features have in the classification decision [53]. Ranking the feature relevance to identify the most important features can be used to reduce the dimensionality of the subset of features. This can shrink the time needed for the process and improve overall performance. The Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) classifier supports classification feature relevance ranking [53] and can be used to improve the classification of PLC and SPN communication signals.

Bibliography

[1] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, and D. Wolber, "A Network Security Monitor," in *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on.* IEEE, 1990, pp. 296–304.

[2] T. Karygiannis and L. Owens, "Wireless Network Security," *NIST special publication*, vol. 800, p. 48, 2002.

[3] G. Bumiller, L. Lampe, and H. Hrasnica, "Power Line Communication Networks for Large-Scale Control and Automation Systems," *IEEE Communications Magazine*, vol. 48, no. 4, pp. 106–113, 2010.

[4] L. T. Berger, A. Schwager, and J. J. Escudero-Garzás, "Power Line Communications for Smart Grid Applications," *Journal of Electrical and Computer Engineering*, vol. 2013, p. 16, 2013, doi:10.1155/2013/712376.

[5] C. Semiconductor, "What is Power Line Communication," *EE Times*, vol. 8, p. 17, 2011.

[6] S. H. Horowitz and A. G. Phadke, *Power System Relaying.* John Wiley & Sons, 2008, vol. 22.

[7] J. Newbury, "Communication Requirements and Standards for Low Voltage Mains Signaling," *IEEE transactions on power delivery*, vol. 13, no. 1, pp. 46–52, 1998.

[8] D. Sanger and E. Schmitt, "Rise is Seen in Cyberattacks Targeting US Infrastructure," *The New York Times*, vol. 26, 2012.

[9] N. Caplan, "Cyber War: The Challenge to National Security," *Global Security Studies*, vol. 4, no. 1, pp. 93–115, 2013.

[10] "Developer's Guide 2nd Edition," Insteon, Tech. Rep., 2007.

[11] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," *Computer*, vol. 36, no. 10, pp. 103–105, 2003.

[12] B. P. Ross, T. J. Carbino, and S. J. Stone, "Physical-Layer Discrimination of Power Line Communications," in *Computing, Networking and Communications (ICNC), 2017 International Conference on*, Jan 2017, pp. 7–13.

[13] Department of Defense Manual, "Special Access Program (SAP) Security Manual: Physical Security (DOD Manual 5205.07V3 Air Force Manual16-703V3)," *Washington, DC*, SAF/AAZ Sept 2015.

[14] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.

[15] B. Danev, D. Zanetti, and S. Capkun, "On Physical-layer Identification of Wireless Devices," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 6:1–6:29, Dec. 2012. [Online]. Available: http://doi.acm.org/10.1145/2379776.2379782

[16] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on Physical-layer Identification," in *Proceedings of the Third ACM Conference on Wireless Network Security*, ser. WiSec '10. New York, NY, USA: ACM, 2010, pp. 89–98. [Online]. Available: http://doi.acm.org/10.1145/1741866.1741882

[17] B. Danev and S. Capkun, "Transient-Based Identification of Wireless Sensor Nodes," in *Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*. IEEE Computer Society, 2009, pp. 25–36.

[18] L. C. C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee, "Identifying Unique Devices Through Wireless Fingerprinting," in *Proceedings of the first ACM conference on Wireless network security*. ACM, 2008, pp. 46–55.

[19] K. Ellis and N. Serinken, "Characteristics of Radio Transmitter Fingerprints," *Radio Science*, vol. 36, no. 4, pp. 585–597, 2001.

[20] D. B. Faria and D. R. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," in *Proceedings of the 5th ACM workshop on Wireless security*. ACM, 2006, pp. 43–52.

[21] W. A. Gardner, "Signal Interception: A Unifying Theoretical Framework for Feature Detection," *IEEE Transactions on Communications*, vol. 36, no. 8, pp. 897–906, 1988.

[22] J. Hall, M. Barbeau, and E. Kranakis, "Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase," *Wireless and Optical Communications*, pp. 13–18, 2003.

[23] ——, "Radio Frequency Fingerprinting for Detection in Wireless Networks," *IEEE Transactions on Defendable and Secure Computing*, 2005.

[24] M. Barbeau, J. Hall, and E. Kranakis, "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*. Citeseer, 2006, pp. 4–6.

[25] J. Hall, M. Barbeau, and E. Kranakis, "Using Transceiverprints for Anomaly Based Intrusion Detection," *Proceedings of 3rd IASTED, CIIT*, pp. 22–24, 2004.

[26] P. K. Harmer, M. D. Williams, and M. A. Temple, "Using De-Optimized LFS Processing to Enhance 4g Communication Security," in *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*. IEEE, 2011, pp. 1–8.

[27] P. K. Harmer, D. R. Reising, and M. A. Temple, "Classifier Selection for Physical Layer Security Augmentation in Cognitive Radio Networks," in *2013 IEEE International Conference on Communications (ICC)*. IEEE, 2013, pp. 2846–2851.

[28] P. K. Harmer, M. A. Temple, M. A. Buckner, and E. Farquahar, "Using Differential Evolution to Optimize' Learning from Signals' and Enhance Network Security," in *Proceedings of the 13th annual conference on Genetic and evolutionary computation*. ACM, 2011, pp. 1811–1818.

[29] R. D. Hippenstiel and Y. Payal, "Wavelet Based Transmitter Identification," in *Signal Processing and Its Applications, 1996. ISSPA 96., Fourth International Symposium on*, vol. 2. IEEE, 1996, pp. 740–742.

[30] R. W. Klein, M. A. Temple, M. J. Mendenhall, and D. R. Reising, "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance," in *2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–5.

[31] R. W. Klein, "Application of Dual-Tree Complex Wavelet Transforms to Burst Detection and RF Fingerprint Classification," Ph.D. dissertation, Air Force Institute of Technology, WPAFB OH, 2009, DTIC Document, Accession Number: AD-A505175.

[32] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 544–555, 2009.

[33] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking*. ACM, 2007, pp. 99–110.

[34] D. R. Reising, M. A. Temple, and M. E. Oxley, "Gabor-Based RF-DNA Fingerprinting for Classifying 802.16e WiMAX Mobile Subscribers," in *Computing, Networking and Communications (ICNC), 2012 International Conference on*, Jan 2012, pp. 7–13.

[35] D. R. Reising and M. A. Temple, "WiMAX Mobile Subscriber Verification Using Gabor-Based RF-DNA Fingerprints," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 1005–1010.

[36] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints," *IEEE*

Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1180–1192, June 2015.

[37] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improved Wireless Security for GMSK-Based Devices Using RF Fingerprinting," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 1, pp. 41–59, 2010.

[38] ——, "Improving Intra-Cellular Security Using Air Monitoring with RF Fingerprints," in *2010 IEEE Wireless Communication and Networking Conference*. IEEE, 2010, pp. 1–6.

[39] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Radio Frequency Fingerprinting Commercial Communication Devices to Enhance Electronic Security," *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 3, pp. 301–322, 2008.

[40] D. Takahashi, Y. Xiao, Y. Zhang, P. Chatzimisios, and H.-H. Chen, "IEEE 802.11 User Fingerprinting and its Applications for Intrusion Detection," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 307–318, 2010.

[41] O. H. Tekbas, O. Ureten, and N. Serinken, "Improvement of Transmitter Identification System for Low SNR Transients," *Electronics Letters*, vol. 40, no. 3, pp. 182–183, 2004.

[42] J. Toonstra and W. Kinsner, "A Radio Transmitter Fingerprinting System ODO-1," in *Electrical and Computer Engineering, 1996. Canadian Conference on*, vol. 1. IEEE, 1996, pp. 60–63.

[43] ——, "Transient Analysis and Genetic Algorithms for Classification," in *WESCANEX 95. Communications, Power, and Computing. Conference Proceedings., IEEE*, vol. 2. IEEE, 1995, pp. 432–437.

[44] M. D. Williams, S. A. Munns, M. A. Temple, and M. J. Mendenhall, "RF-DNA Fingerprinting for Airport WiMax Communications Security," in *Network and System Security (NSS), 2010 4th International Conference on*, Sept 2010, pp. 32–39.

[45] M. D. Williams, M. A. Temple, and D. R. Reising, "Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec 2010, pp. 1–6.

[46] D. Zanetti, B. Danev *et al.*, "Physical-layer Identification of UHF RFID Tags," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. ACM, 2010, pp. 353–364.

[47] O. Ureten and N. Serinken, "Wireless Security Through RF Fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27–33, 2007.

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

[49] R. M. Gerdes, T. E. Daniels, M. Mina, and S. F. Russell, "Device identification via analog signal fingerprinting: A matched filter approach," in *In 144 Proceedings of the Network and Distributed System Security Symposium (NDSS*, 2006, p. 78.

[50] R. M.Gerdes, M. Mina, S. F. Russell, and T. E. Daniels, "Physical-layer Identification of Wired Ethernet Devices," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1339–1353, 2012.

[51] S. J. Stone, "Radio Frequency Based Programmable Logic Controller Anomaly Detection," Ph.D. dissertation, Air Force Institute of Technology, WPAFB OH, 2013, DTIC Document, Accession Number: AD-A583973.

[52] B. C. Wright, "PLC Hardware Discrimination Using RF-DNA Fingerprinting," Master's thesis, Air Force Institute of Technology, WPAFB OH, 2014, DTIC Document, Accession Number: AD-A602984.

[53] D. R. Reising, "Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing," Ph.D. dissertation, Air Force Institute of Technology, WPAFB OH, 2012, DTIC Document, Accession Number: AD-A572506.

[54] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using Spectral Fingerprints to Improve Wireless Network Security," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE, 2008, pp. 1–5.

[55] W. E. Cobb, "Exploitation of Unintentional Information Leakage from Integrated Circuits," Ph.D. dissertation, Air Force Institute of Technology, WPAFB OH, 2011, DTIC Document, Accession Number: AD-A550584.

[56] W. E. Cobb, E. W. Garcia, M. A. Temple, R. O. Baldwin, and Y. C. Kim, "Physical Layer Identification of Embedded Devices Using RF-DNA Fingerprinting," in *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, Oct 2010, pp. 2168–2173.

[57] J. Lopez Jr, M. A. Temple, and B. E. Mullins, "Exploitation of HART Wired Signal Distinct Native Attribute (WS-DNA) Features to Verify Field Device Identity and Infer Operating State," in *International Conference on Critical Information Infrastructures Security*. Springer, 2014, pp. 24–30.

[58] B. P. Ross, T. J. Carbino, and M. A. Temple, "Simulcasted Power Line Communication Network (SPN) Discrimination Using Wired Signal Distinct Native Attribute (WS-DNA) Features," in *Cyber Warfare and Security (ICCWS), 2017 International Conference on*, March 2017, pp. 7–13.

[59] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, and Y. C. Kim, "Intrinsic Physical-Layer Authentication of Integrated Circuits," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 14–24, Feb 2012.

[60] H. C. Ferreira, H. M. Grové, O. Hooijen, and A. Han Vinck, *Power Line Communication*. Wiley Online Library, 2001.

[61] P. S. C. Committee *et al.*, "Summary of an IEEE Guide for Power-Line Carrier Applications," *Power Apparatus Systems, IEEE Trans. on*, pp. 2334–2337, 1980.

[62] N. Pavlidou, A. H. Vinck, J. Yazdani, and B. Honary, "Power Line Communications: State of the Art and Future Trends," *IEEE Communications magazine*, vol. 41, no. 4, pp. 34–40, 2003.

[63] M. Nassar, J. Lin, Y. Mortazavi, A. Dabak, I. H. Kim, and B. L. Evans, "Local Utility Power Line Communications in the 3–500 kHz Band: Channel Impairments, Noise, and Standards," *Signal Processing Magazine, IEEE*, vol. 29, no. 1, pp. 116–127, 2012.

[64] D. Rye, "My Life at x10," X10 (USA) Inc., Tech. Rep., 1999, available at http://www.hometoys.com/content.php?url=/htinews/oct99/articles/rye/rye.htm.

[65] "Insteon WHITEPAPER: The Details," Insteon, Tech. Rep., 2013.

[66] S. Goldfisher and S. Tanabe, "IEEE 1901 Access System: An Overview of Its Uniqueness and Motivation," *Communications Magazine, IEEE*, vol. 48, no. 10, pp. 150–157, 2010.

[67] "Insteon WHITEPAPER: Compared," Insteon, Tech. Rep., 2013.

[68] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 116–127. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409959

[69] M. Edman and B. Yener, "Active Attacks Against Modulation-Based Radiometric Identification," Tech. Rep. 09–02, 2009.

[70] Y. Huang and H. Zheng, "Radio frequency fingerprinting based on the constellation errors," in *2012 18th Asia-Pacific Conference on Communications (APCC)*, Oct 2012, pp. 900–905.

[71] L. Marple, "Computing the Discrete-Time Analytic Signal via FFT," *IEEE Transactions on signal processing*, vol. 47, no. 9, pp. 2600–2603, 1999.

[72] S. Theodoridis and K. Koutroumbas, "Pattern Recognition, Academic Press," *New York*, 1999.

[73] D. J. MacKay, *Information Theory, Inference and Learning Algorithms*. Cambridge university press, 2003.

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

[75] J. Friedman, T. Hastie, and R. Tibshirani, *The Elements of Statistical Learning*. Springer series in statistics Springer, Berlin, 2001, vol. 1.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

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

4. TITLE AND SUBTITLE

Physical-Layer Identification of Power Line Communications Using WS-DNA Fingerprinting

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

17G231

6. AUTHOR(S)

Ross, Brady P, Capt, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

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

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-17-M-067

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

14. ABSTRACT

Vulnerabilities in networked systems can leave critical infrastructure exposed to cyber attacks and short falls in home automation communication security permit similar attacks against government personnel. PLC as a network communication method is a cost effective solution supporting many of these networks. Global time synchronization can allow a SPN of multiple interconnected devices to transmit repeated signals simultaneously which can increase operating range and reliability. PLC device and SPN discrimination using WS-DNA fingerprinting is investigated for PHY intrusion detection. 6 Insteon Hubs are used for single device DUT discrimination. The same 6 Insteon Hubs are integrated with 4 different Insteon On/Off Outlets to create 24 distinct SPNs that are used in SPN DUT discrimination. For single device DUT, an average %C = 90% is achieved at SNR 36 dB. ROC curves are used to illustrate rogue detection results with EER of 10% achieved for all devices at SNR = 40 dB. For the SPN DUT subset an average of %C = 90% is achieved for SNR 50 dB with rogue detection resulting in a EER = 10% achieved at SNR = 50 dB.

15. SUBJECT TERMS

WS-DNA, RF-DNA, Power Line Communications, Physical-Layer, Intrusion Detection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Maj Timothy J. Carbino, AFIT/ENG
U	U	U	U	96	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x4220; timothy.carbino@afit.edu