Utah State University

DigitalCommons@USU

All Graduate Theses and Dissertations | Graduate Studies

5-2015

Evaluation of Tracking Regimes for, and Security of, PLI Systems

Shayan Taheri
Utah State University

Follow this and additional works at: https://digitalcommons.usu.edu/etd

Part of the Computer Engineering Commons

Recommended Citation

Taheri, Shayan, "Evaluation of Tracking Regimes for, and Security of, PLI Systems" (2015). *All Graduate Theses and Dissertations*. 4549.
https://digitalcommons.usu.edu/etd/4549

This Thesis is brought to you for free and open access by the Graduate Studies at DigitalCommons@USU. It has been accepted for inclusion in All Graduate Theses and Dissertations by an authorized administrator of DigitalCommons@USU. For more information, please contact digitalcommons@usu.edu.

UtahStateUniversity
MERRILL-CAZIER LIBRARY

EVALUATION OF TRACKING REGIMES FOR, AND SECURITY OF, PLI SYSTEMS

by

Shayan Taheri

A thesis submitted in partial fulfillment
of the requirements for the degree

of

MASTER OF SCIENCE

in

Computer Engineering

Approved:

Dr. Ryan Gerdes Major Professor	Dr. Tam Chantem Committee Member
Dr. Reyhan Baktur Committee Member	Dr. Mark R. McLellan Vice President for Research and Dean of the School of Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2015

Copyright © Shayan Taheri 2015

All Rights Reserved

Abstract

Evaluation of Tracking Regimes for, and Security of, PLI Systems

by

Shayan Taheri, Master of Science

Utah State University, 2015

Major Professor: Dr. Ryan Gerdes
Department: Electrical and Computer Engineering

In the area of computer and network security, due to the insufficiency, high costs, and user-unfriendliness of existing defending methods against a number of cyber attacks, focus for developing new security improvement methods has shifted from the digital to analog domain. In the analog domain, devices are distinguished based on the present variations and characteristics in their physical signals. In fact, each device has unique features in its signal that can be used for identification and monitoring purposes.

In this regard, the term physical layer identification (PLI) or device fingerprinting refers to the process of classifying different electronic devices based on their analog identities that are created by employment of signal processing and data analysis methods. Due to the fact that a device behavior undergoes changes due to variations in external and internal conditions, the available PLI techniques might not be able to identify the device reliably. Therefore, a tracking system that is capable of extracting and explaining the present variations in the electrical signals is required to be developed. In order to achieve the best possible tracking system, a number of prediction models are designed using certain statistical techniques. In order to evaluate the performance of these models, models are run on the acquired data from five different fabrications of the same device in four distinct

experiments. The results of performance evaluation show that the surrounding temperature of a device is the best option for predicting its signal.

The last part of this research project belongs to the security evaluation of a PLI system. The leveraged security examination technique exposes the PLI system to different types of attacks and evaluates its defending strength accordingly. Based on the mechanism of the employed attack in this work, the forged version of a device's signal is generated using an arbitrary waveform generator (AWG) and is sent to the PLI system. The outcomes of this experiment indicate that the leveraged PLI technique is strong enough in defeating this attack.

(86 pages)

Public Abstract

Evaluation of Tracking Regimes for, and Security of, PLI Systems

by

Shayan Taheri, Master of Science

Utah State University, 2015

Major Professor: Dr. Ryan Gerdes
Department: Electrical and Computer Engineering

In recent years, the researchers and engineers have realized that the trustiness of computer and networking devices and hardware can no longer be examined properly using the existing identification and security checking methods that operate based on the digital representation of data. As an example, since the digital identifiers can be copied, it is difficult to tie a digital identity to a device for sure. Also, the new or present created cyber attacks can manipulate the used digital data in a network easily. Due to these issues, the trend in development of new identification and security checking methods has moved toward analog signals of the devices that can be acquired from different parts of their circuits. In fact, these analog signals have adequate information and features to uniquely identify the devices.

The dark side of analog-based methods is when some changes appear in the behavior of devices in different conditions and over time. It causes the loss of ability of these methods in differentiation of the devices. This is due to the mismatch between the current signal of the device and the reference signal, which is obtained earlier. In this regard, a number of statistical models are designed that use the environmental or a device's circuit-related parameters in order to predict its future behavior. The achieved results from running the designed statistical models on the related data show that the surrounding temperature of the device is the best option for predicting its signal information and features.

In the last part of this study, the defending strength of an analog-based identification and security checking method in confrontation with a specific attack is evaluated. In the utilized attack, the forged version of a device's signal is generated and is checked by the security method. According to the outcomes of accomplished experiments, the leveraged security checking method is able to defeat this attack perfectly.

To my beloved parents and dear brother ...

Acknowledgments

This thesis would not have been possible without the dedicated support, guidance, and patience of my laudable advisor, Dr. Ryan Gerdes. I would like to thank him with all gratitude for believing in me, providing a great opportunity for me to work in his research laboratory and introducing me to the field of Hardware Security and Physical Layer Identification, in addition to everything that I learned from his kind-hearted personality. I would like to acknowledge other members of my committee, Dr. Tam Chantem and Dr. Reyhan Baktur, for their insightful suggestions, encouragement, understanding and help during the course of my research on this project.

My great appreciation goes to the ECE department and all of the staff members, for offering me this opportunity to pursue my M.S. degree, as well as the financial assistance towards my tuition. I would like to offer my special thanks to Dr. Todd Moon for helping me out in many tough situations. I am particularly grateful for the assistance given by Mary Lee Anderson and Tricia Brandenburg through their valuable advice.

I would like to express my special gratefulness to my wonderful and praiseworthy family for their endless love and selfless efforts throughout my whole life. Without their help and support, I could not have reached any of my goals and my life would be meaningless without them. At last, I am thankful to all my friends in Logan for the great time that I had with them.

Shayan Taheri

Contents

Page

Abstract . . . . . **iii**

Public Abstract . . . . . **v**

Acknowledgments . . . . . **viii**

List of Tables . . . . . **xi**

List of Figures . . . . . **xii**

Acronyms . . . . . **xiv**

1 Introduction **1**
1.1 Related Work 4
1.2 Organization of Chapters 7

2 Physical Layer Identification System **8**
2.1 Overview 8
2.2 Concepts 9
2.2.1 Matched Filter 9
2.2.2 Adaptive Thresholding Strategy 11
2.2.3 APRS Metrics and Misclassification Matrix 12
2.3 Experimental Approach 14
2.4 Results and Discussion 18
2.4.1 Overview of Experiments 18
2.4.2 Analysis of Results 22

3 Study of Tracking System Models **30**
3.1 Overview 30
3.2 Concepts for Data Preparation 30
3.2.1 Charging/Discharging Trend 30
3.2.2 Euclidean Norm 31
3.2.3 Mean of Absolute Value (MAV) 31
3.2.4 Autoregressive Model 32
3.2.5 Moving Average 32
3.2.6 Normalization 32
3.2.7 Standard Deviation 32
3.3 Techniques for Data Modeling 33
3.3.1 Correlation Analysis 33
3.3.2 Cross Correlation Analysis 34
3.3.3 Autocorrelation 34

3.3.4 Simple Linear Regression (SLR) 34
3.3.5 Multiple Linear Regression (MLR) 36
3.3.6 Non-Linear Regression (NLR) 36
3.3.7 Robust Regression 37
3.3.8 General Linear Model (GLM) 37
3.3.9 Smoothing Spline 38
3.3.10 ARMA and ARMAX Modeling 39
3.3.11 Analysis of Residuals 40
3.3.12 Thermal System Modeling (TSM) 41
3.4 Results and Discussion 43
3.4.1 Overview of Prediction Models 43
3.4.2 Basic Models 45
3.4.3 Combined Models 47

4 Security Evaluation of PLI Systems 56
4.1 Overview 56
4.2 Architecture of Attack 56
4.3 Arbitrary Waveform Generator (AWG) Configuration 58
4.3.1 AWG Performance Parameters 58
4.4 Simulation Framework for Security Evaluation 60
4.5 Results and Discussion 61

5 Conclusion 66

References 68

List of Tables

Table Page

2.1 Description of the designed experiments. 18

2.2 The information of Ethernet cards - (1). 19

2.3 Mean of APRS values for datasets 1 and 2. 23

2.4 Mean of APRS values for datasets 3 and 4. 25

2.5 Mean of APRS values for datasets 5 and 6. 26

2.6 Mean of APRS values for datasets 7 and 8. 29

3.1 The results of basic models - (1). 51

3.2 The results of basic models - (2). 52

3.3 The results of basic models - (3). 53

3.4 The results of combined models - (1). 54

3.5 The results of combined models - (2). 55

4.1 The information of Ethernet cards - (2). 62

4.2 The PLI system performance results - Generation of records at 1.0 GS/s rate. 65

4.3 The PLI system performance results - Generation of records at 2.0 GS/s rate. 65

List of Figures

Figure Page

2.1 Different components of a device's record. 10

2.2 The concept of adaptive thresholding strategy. 11

2.3 An Ethernet card under test. 14

2.4 The desktop TPC and DAQPC (left) and the slots of TPC (right). 15

2.5 The mini DAQPC and its data measurement location. 16

2.6 The mini TPC and its data measurement location. 16

2.7 Ethernet card's record (top) and synchronization signal (bottom). 19

2.8 The variations in the device's synchronization signal. 20

2.9 The significant change in the level of MFO signal. 21

2.10 APRS table (left) and misclassification matrix (right). 22

2.11 Matched filter output (upper) and surrounding temperature (lower) in Setup 1. 23

2.12 Matched filter output (upper) and surrounding temperature (lower) in Setup 2. 24

2.13 Matched filter output (upper) and surrounding temperature (lower) in Setup 3. 26

2.14 IC's supply voltage (upper) and bus's supply voltage (lower) in Setup 3. . . 27

2.15 Matched filter output (upper) and surrounding temperature (lower) in Setup 4. 28

2.16 IC's supply voltage (upper) and bus's supply voltage (lower) in Setup 4. . . 28

3.1 A scatter plot for Model 1. 45

3.2 Filtering MFO signal using moving average function with a window size of 10. 46

3.3 The created thermal system model. 49

3.4 A comparison between the actual MFO and four predicted MFOs. 50

4.1 The architecture of attack. 57

4.2 One period of the correct and forged synchronization signals and their differences. 63

4.3 The generated forged records at 1.0 GS/s (left) and 2.0 GS/s (right) rates. . 64

Acronyms

PLI	Physical Layer Identification
OSI	Open Systems Interconnection
PLIS	Physical Layer Identification System
TTL	Transductive Transfer Learning
AWG	Arbitrary Waveform Generator
USRP	Universal Software Radio Peripherals
GSM	Global System for Mobile
UMTS	Universal Mobile Telecommunications System
PSD	Power Spectral Density
MFO	Matched Filter Output
MAC	Media Access Control
TP	True Positive
FP	False Positive
TN	True Negative
FN	False Negative
APRS	Accuracy - Precision - Recall - Specificity
TPC	Test Personal Computer
DAQPC	Data Acquisition Personal Computer
DPO	Digital Phosphor Oscilloscope
IC	Integrated Circuit
RC	Resistor - Capacitor
MAV	Mean of Absolute Value
STD	Standard Deviation
TSM	Thermal System Modeling

SLR	Simple Linear Regression
MLR	Multiple Linear Regression
NLR	Non-Linear Regression
GLM	General Linear Model
IG	Inverse Gaussian
ARMA	Autoregressive Moving Average
MA	Moving Average
AR	Autoregressive
ARMAX	Autoregressive Moving Average with Exogenous Inputs
LAR	Least Absolute Residuals
DAC	Digital-to-Analog Converter
LPF	Low-Pass Filter
THD	Total Harmonic Distortion
SNR	Signal-to-Noise Ratio
AWGN	Additive White Gaussian Noise
THLD	Threshold
AFG	Arbitrary/Function Generator
CMOS	Complementary Metal-Oxide Semiconductor
RF	Radio Frequency
PVT	Process, Supply Voltage, and Temperature
LNA	Low-Noise Amplifier
FET	Field Effect Transistor
STT	Spin Transfer Torque

Chapter 1

Introduction

Existing methods in the area of computer and network security used to be concentrated primarily on digital domain, because of its flexibility and controllability in designing and creating new methods. However, due to the emergence of new cyber attacks in this branch of security field and vulnerability of existing defense techniques in digital domain such as leakage of digital tokens (network keys) or identifiers (username and password), attention has moved toward design and creation of methods based on the physical representation of information. The concept that is behind the physical domain is identification of the devices based on the differences in their analog signaling characteristics and behavior. In other words, the analog signal of every device has some unique features that are due to hardware and manufacturing inconsistencies, and can be used for identification and monitoring purposes.

The signal classification process starts by creating and utilizing analog identities for electronic devices such as wired Ethernet cards, sensors, RFID devices and so on, through the application and interpretation of applying signal processing techniques to either transient portion or steady-state portion of their signal. This process is called device fingerprinting or physical layer identification (PLI), and is defined as using the physical layer (i.e. lowest layer or first layer) of the Open Systems Interconnection (OSI) model for the identification of modern networking devices. Any systematic approach for accomplishment of this operation (which includes the equipment, algorithms, and so forth) is referred to as a physical layer identification system (PLIS).

The methodology of PLI can be divided into three steps: (a) identify and acquire a repetitive and always present signal, also known as Fingerprint, which is correlated to the device properties such as clock, design of circuitry, the amount of load on its IC, et cetera,

(b) extract a set of meaningful features from the signal, (c) employ a classification technique to compare a test feature set with a database of existing feature sets in order to verify the targeted identity of the device under test. The device is accepted if the differences between its test feature set and the chosen reference feature set from the database lie within a certain threshold range. Enhancement of the higher-level mechanisms in provision of security is achieved by integrating the physical-based methods and digital-based methods, which can be greatly efficient in defensive purposes such as Intrusion Detection (discovering node impersonation and network tampering), Authentication (preventing unauthorized access to the physical network), Forensic Data Collection (tying a physical device to a specific network incident), and Assurance Monitoring (determining whether a device will or is in the process of failing).

Changes in conditions and states cause differences in behavior of the electronic devices, which intervenes in the process of device identification. For example, the fingerprint of a device at two distinct times (before turning the PC off at night and after turning it on in the morning) is different. In this regard, a physical layer identification technique [1] is leveraged that has the ability of reliably identifying electronic devices over time based on information profiles that are created for them. Each information profile belongs to an electronic device and consists of three main components that are: (a) an optimal detector named Matched Filter, which is sensitive enough to perceive the small variations in the device' signal (for example, the steady-state portion of the entered signals to the matched filter function is used for identification purposes due to its sufficient amount of information); (b) the outputs of the applied matched filter to all of the acquired records from the device; and (c) the outcome of an adaptive thresholding strategy, in which the matched filter outputs of a certain number of records are used as the training data in order to calculate the threshold value for the acceptance of the upcoming data. The positive and negative versions of this value are used as the highest and lowest values for the threshold range.

The adaptive thresholding strategy also provides this possibility to re-identify a device after its connectivity to the network has been lost and re-established again, by using the last

calculated threshold value. There are two points regarding the electronic devices, Ethernet cards that are used in this project: (i) they are chosen from the same make and model in order to make differentiation of the devices more difficult; and (ii) their operational speed is 10 MB/second, which provides simplicity and extensibility. On the other hand, these devices have less information segments in their signals that limit their diversification.

In this study, a tracking system (a.k.a. tracking regime) that is capable of extracting and explaining the present variations in an electrical signal is developed. It is a requisite for identification of different devices based on their unique behavior under different conditions and states (for channel, position, temperature and so on). The role of this tracking system in transfer learning terminology [2] is defined as discovering a target prediction function for the target domain with unlabeled data (future fingerprint - such as matched filter output) using labeled source domain data (available fingerprint along with any other auxiliary data, for example, temperature), which is known as Transductive Transfer Learning (TTL). Once the target prediction function is found, its accuracy and performance is verified by checking the amount of closeness between the predicted data and the actual data.

At last, the security of PLI system under investigation is evaluated based on its strength in confrontation with the signal replay attack, in which a previously acquired record (or signal) from a device is reproduced. The framework [3] that is implemented for this purpose evaluates the defending strength of a PLI system by exposing the system to different types of attacks using an arbitrary waveform generator (AWG), which is an electronic equipment that is capable of generating arbitrary shaped signals. Each attack is designed with an AWG that has certain performance parameters such as sampling rate, resolution, signal-to-noise ratio, and total harmonic distortion.

The contributions of this thesis are listed as follows:

- Understanding and analyzing the behavior of networking devices (for example, Ethernet cards) comprehensively in different fabrications, states, and conditions and, over time. In this regard, five Ethernet cards are tested in four experiments. The purpose

in experiments 1, 2, and 4 is studying the device behavior when its surrounding temperature has small, large, and factual variations respectively. In experiment 3, the objective is finding the similarities and differences between the device's signal and the supplied voltages to its printed circuit board's general bus and the mounted IC on it.

- Developing a tracking system that is capable of extracting and explaining the present variations in a device's signal.
- Evaluating the defending strength of a PLI system in confrontation with the signal replay attack, in which a previously acquired signal from a device is reproduced.

1.1 Related Work

Research and development in the areas of security checking of electronic devices through their signal detection, classification, and identification has been investigated by many researchers and engineers during the last century [4–7]. The classification and identification techniques can be divided into two categories: (a) analog-based, which uses the characteristics of the device's analog signal; and (b) digital-based, which uses the variations in the digital representation of data. The analog-based techniques can be grouped based on their: (i) analysis domain (time or frequency); and (ii) signal portion of interest (transient or steady-state) or signal modulation features.

The techniques that are used for identification and classification of the networking devices based on the transient portion of their analog signal concentrate mostly on the wireless area [8–10], as opposed to the steady-state based techniques that focus primarily on the wired area [11, 12]. Due to the emergence of new cyber attacks in the wireless area in recent years, more attentions are drawn to this area [13–19]. Specifically, the subject of overcoming the eavesdropping attack has highly been investigated in the cited works. This attack is described as the act of stealing the transmitted information between the authorized users in a wireless network by a malicious person (a.k.a. man-in-the-middle).

Regardless of the concentration of the recent physical layer identification techniques on the wireless area, there are still different important aspects of the wired area that have

not been scrutinized sufficiently. The effects of different states and conditions (i.e. changes in time and cable length or variations of manufacturing process, supply voltage, and temperature) on identification of wired networking devices is one of these aspects that has been studied only in a few research works and insufficiently [11,12,20-22]. However, the performance degradation of electronic circuits (i.e. alteration of their output signal) due to environmental effects has been studied intensively since a few decades ago, and many innovative circuit design techniques have been presented to tackle this problem. This trend originated from the continuation of CMOS technology device scaling (process feature size shrinkage) that reinforces these effects.

Oscillators are very important elements in digital, analog, and radio frequency integrated circuits and their instability can affect different applications such as, communication networks, data link protocols, medical wireless sensor networks, and clock generation subsystems. Walls studied the environmental effects (for example, acceleration, temperature, humidity, pressure, vibration, magnetic field, electric field, load, and radiation) on the frequency, output level, and noise amplitude of precision oscillators output signal [20]. According to the results, the sensitivity of a given oscillator to a parameter depends on the value of other parameters along with the device history. Also, it is difficult to separate the influence of one parameter from that of another. The most important parameters that can affect the performance of these oscillators are acceleration, vibration, and temperature.

Wu *et al.* proposed a technique for improving robustness of a ring-oscillator based phase lock loop using an on-chip calibration module [21]. This module has a small footprint on the area and power consumption of chip and compensates the effects of supply voltage variations. The authors of [22] improved the stability of a ring oscillator efficiently by: (a) biasing the low drop-out regulator module with high accuracy band-gap reference in order to reject the influence of supply voltage variations on the output frequency; and (b) generating a bias voltage for weakening the effects of temperature variations using a temperature sensor and a voltage adder/subtractor. An adaptive body bias compensation technique to increase the resiliency of RF power amplifier to process, supply voltage, and temperature (PVT)

variations was presented in [23]. The variations are sensed using a current source and their effects on the device performance are reduced through threshold voltage adjustment. A similar work was accomplished by Gomez *et al.* for LNAs and mixers [24]. Different gate biasing schemes for reducing the effects of temperature variations on an RF power amplifier performance was analyzed in [25].

The reliability of a reconfigurable linearized low noise transconductance amplifier was strengthened by sensing and improving the linearity of device's output signal [26]. Omann *et al.* designed a new circuit model for RF power amplifiers that is robust against PVT variations [27]. According to this model, a scaled power amplifier replica cascade circuit and a controlled current mirror are utilized to form a feedback loop in order to stabilize the circuit operating point. The problem of CMOS technology device scaling is not limited to performance degradation. It can bring other challenges such as augmentation of short-channel effects and increase in power consumption. This causes the emergence of other technologies such as multiple gate field effect transistors (FETs) and spin transfer torque (STT) in the design of new integrated circuits. Although these technologies might have their own issues in the aspect of circuit reliability and stability. In this regard, a tool for evaluating and analyzing the effects of PVT variations on FinFET-based circuit models was presented in [28]. Vatajelu *et al.* presented a reliability evaluation methodology for STT magnetic random access memory cells to investigate the behavior of these cells under different operational conditions [29]. Therefore, it is required to understand and analyze the device behavior and its identification fingerprint under different operational conditions and states in order to construct a comprehensive identification and classification system. In this regard, development of a tracking system capable of extracting and explaining the variations of an electrical signal in different conditions and states is studied in this research work.

The security evaluation of a PLI system is accomplished by exposing it to different types of attack and measuring its defending strength accordingly [30]. In general, there are three main types of attack that can be used for defeating a PLI system: (a) Feature Replay,

in which a forged signal similar to the device's signal, according to the features that are used by the PLI system, is generated and sent to the system; (b) Signal Replay, in which a previously acquired record (or signal) from the device is reproduced; and (c) Coercion, in which an attacker accesses an authorized device directly and control it for running malicious functions. Only a few research works have been done in this area: Danev and Capkun [31] attacked a transient-based PLI system by sending the forged version of a device's signal to the system repeatedly and modifying the forged signal gradually in order to improve its similarity to the original signal. According to the results of this work, the PLI system was vulnerable in confronting this attack. A modulation-based PLI system was attacked in [32], using low-cost software-defined radios to reproduce modulation features in order to impersonate a target device. This identification system showed weak resistance in front of the applied attack. A new PLI system named GenePrint was introduced for UHF passive tags in [33], which showed enough resiliency to various malicious feature replay attacks. In this regard, the leveraged PLI system in this work is exposed to two versions of a signal replay attack in order to evaluate its defending strength.

1.2 Organization of Chapters

The rest of this thesis is organized as follows. In Chapter 2, the methodology of the PLI system and the concepts behind it are explained. Also, the designed experimental setups for performance analysis of the PLI system and the respective results are presented. The beginning part of Chapter 3 belongs to the description of all of the employed data preparation concepts and data modeling techniques for finding a relationship between the device's signal and either environmental or circuit-related parameters. Next, all of the developed models for the tracking system are presented and their results are delivered. Chapter 4 delineates the method used for security evaluation of the PLI system at the beginning. Then, the simulation framework for implementation of this method and the related results are presented. Finally, the thesis is concluded in Chapter 5.

Chapter 2

Physical Layer Identification System

2.1 Overview

The minute and unique variations in the signaling behavior of every electronic device due to hardware and manufacturing inconsistencies can be exploited for identification and monitoring purposes. These variations can be sensed and manifested more efficiently by applying various signal processing and data analysis methods to the test data. The employed physical layer identification technique in this study attempts to verify the identity of a networking device – 10 MB Ethernet card, based upon the layer-specific behavior of the Physical and Data Link layers. Verification is done by monitoring the analog characteristics of the synchronization signal, acquired from the device and determining whether the digital hardware address corresponds to the expected physical signal.

In this process, a profile is created from the trustworthy data (i.e. training data) in order to represent both the history of the device behavior and its expected future performance. The three main components of the profile are the matched filter, the output of the applied matched filter to all of the collected records, and the threshold values for acceptance of the previous records and the incoming records. The proposed technique can be effectively used in stability analysis (evaluating the device behavior over time) and forensic analysis (examining the newly received data from a device based on the previously collected data) of the networking devices.

2.2 Concepts

2.2.1 Matched Filter

Matched filter is an optimal linear detector that is commonly used in receiver systems. Its application in here is for maximizing the signal-to-noise ratio of an input signal (i.e. test signal) in the presence of additive white Gaussian noise (a basic noise model that is added to a signal for mimicking the effect of many random processes that occur in nature). The operation of this filter can be interpreted as the inner product of two time-aligned signals, and has a transfer function in the frequency domain according to the Equation 2.1, where $A^*(\omega)$ is the complex conjugate of the Fourier Transform of the reference signal $\alpha(t)$ in the time-domain, $P(\omega)$ is the power spectral density (i.e. the distribution of a signal power over the different frequencies) of the associated noise with the input signal, k is an arbitrary constant such that its values are chosen based on the operating environment, and t_0 is the sampling time of the maximum filter output that is determined by aligning the reference signal with a newly received signal (i.e. test signal).

$$H(\omega) = k.\frac{A^*(\omega)}{P(\omega)}.\exp(-j\omega t_0) \tag{2.1}$$

Consequently, the time-domain version of the transfer function can be obtained by applying inverse Fourier Transform to it, which will result in Equation 2.2.

$$h(t) = \begin{cases} \alpha(t_0 - t) & 0 \leq t \leq T \text{ (Period)} \\ 0 & \text{Otherwise} \end{cases} \tag{2.2}$$

Applying convolution to the time-aligned versions of the matched filter and the test signal delivers a value that is a measurement of the closeness of the newly received signal to the reference one. This parameter is called Matched Filter Output (MFO), and is presented by Equation 2.3. Prior to applying the matched filter, several pre-processing techniques can be applied to the device's signal in order to amplify its variations and characteristics.

This will empower the detection capability of the filter in discovering the device identity. According to Equation 2.3, $\lambda(t_0)$ is the filter output, $h(t_0)$ is the time-aligned matched filter that is acquired from a trustworthy record, and $\beta(t_0)$ is the time-aligned test signal that is acquired from a test record.

$$MFO : \lambda(t_0) = h(t_0) * \beta(t_0) = \int_{t_0-T}^{t_0} \alpha(\tau).\beta(\tau).d\tau \tag{2.3}$$

Depending on the analysis type, the test record can come from the same device or a different device. When a record from the same device is used, the filter output is called Control Response and when a record from a different device is used, it is called Subject Response. Among different components of a record (shown in Figure 2.1), including the noise (black part), transient to steady-state (red part), steady-state or synchronization signal (blue part), transient to MAC address (green part), and receiver MAC address and transmitter MAC address (brown part), the third one that is repetitive in behavior and is always present is used for these calculations. Meanwhile, the synchronization signal has the Manchester coding format, in which the data bits are represented by transitions from one logical state to the other (for example, running XOR function on the data and clock). This makes the signal self-clocking and provides additional reliability.

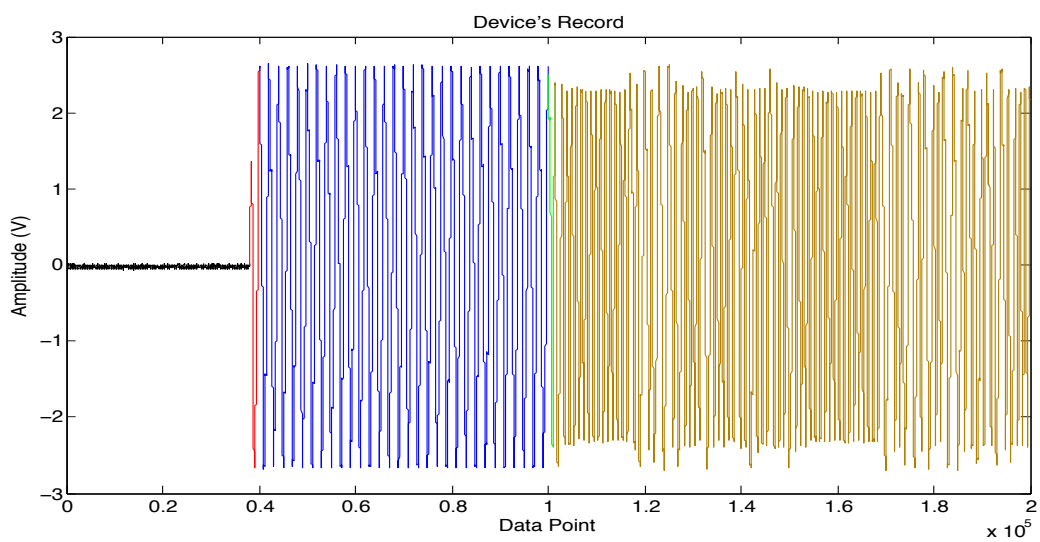

Fig. 2.1: Different components of a device's record.

2.2.2 Adaptive Thresholding Strategy

In order to determine the allowable range of variations for the future matched filter outputs of a device, a threshold parameter needs to be calculated based on the available ones. In other words, it provides an indication of the maximum amount of acceptable deviation in a filter response before its signal is marked as too different from the trustworthy one. Calculation of the threshold value is done based on the distributional properties of the previously obtained filter responses. Since the acquired signal from the device has a stochastic nature, the threshold value for accepting the matched filter output will be time variant. This requires having a strategy for tracking the filter outputs and calculating their threshold values accordingly.

According to the proposed strategy, the next m records of a device should be similar to the previous n records and the threshold value needs to be updated every n records respectively. In this way, the origin of the device's signal can be determined on a record-by-record basis. This concept is shown visually in Figure 2.2.

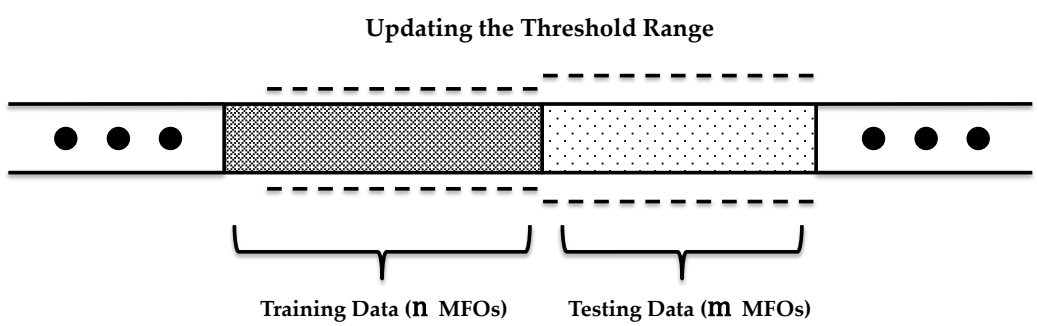

Fig. 2.2: The concept of adaptive thresholding strategy.

Due to the fact that the distribution (i.e. its type, location, and scale) of the filter output is unknown, prediction intervals must be used in order to determine the threshold value [34]. In this regard, a two-sided prediction interval is incorporated to establish the allowable range of variations for the m future filter outputs with $100 \times (1 - \gamma)\%$ level of confidence, as shown in Equation 2.4.

$$threshold_{+/-}(MFO^{j}, \ldots, MFO^{j+m-1}) =$$
$$\mu(MFO^{j-n}, \ldots, MFO^{j-1}) \pm r_{(1-\gamma;m,n)} \times \sigma(MFO^{j-n}, \ldots, MFO^{j-1}) \quad , \quad n < j \quad (2.4)$$

According to this equation, MFO^j represents the matched filter output of jth record, and $\mu(.)$ and $\sigma(.)$ are the mean and standard deviation functions respectively. The parameter $r_{(.)}$ is called Range Parameter and is calculated using Equation 2.5. In this equation, $t_{(.)}$ is the probability distribution function of the Student's t-distribution (i.e. it is used for estimating the mean of a set of few chosen samples from a stochastic variable data when the standard deviation and the mean of all data points are unknown), γ is the level of failure, n is the number of previous filter outputs that are used as the training data, and m is the number of future filter outputs that are utilized as the testing data.

$$r_{(1-\gamma;m,n)} \approx (1 + \frac{1}{n})^{\frac{1}{2}} \cdot t_{(\frac{1-\gamma}{2m};n-1)} \quad (2.5)$$

2.2.3 APRS Metrics and Misclassification Matrix

To present the outcome of employing the matched filter in device differentiation, four metrics common to machine learning and data mining along with the misclassification matrix (a.k.a. confusion matrix) are incorporated. The metrics provide only an overall picture of the system performance for a single device, while the misclassification matrix shows the amount of overlapping between two devices as well as the occurrence of misidentification for a device. In the context of this work, the result parameters that are used in calculating the performance metrics are defined according to the following:

- True Positive (TP): A record is correctly rejected as not having originated from the original device (a.k.a. True Reject).
- False Positive (FP): A record is wrongly rejected as not having originated from the original device (a.k.a. False Reject). Equation 2.6 is used in order to calculate this

parameter.

$$FP = n_c - n - n_r \tag{2.6}$$

- True Negative (TN): A record is correctly accepted as having originated from the original device (a.k.a. True Accept).
- False Negative (FN): A record is wrongly accepted as having originated from the original device (a.k.a. False Accept). Equation 2.7 is used in order to calculate this parameter.

$$FN = \frac{m}{n_c} \cdot \sum_{L=1}^{\frac{n_c}{m}} n_a^L \tag{2.7}$$

According to Equations 2.6 and 2.7, n_c is the total number of collected records for a device, n is the number of used records for training data (per each testing period), m is the number of used records for the testing data (per each testing period), n_r is the total number of rejected records, and n_a^L is the number of accepted records in L^{th} period of testing. According to these definitions, four major performance evaluation metrics namely, Accuracy (A) that is the rate of correctly accepted and rejected records, Precision (P) that is the rate of correctly rejected records, Recall (R) that is the success rate in rejection of records, and Specificity (S) that is the success rate in acceptance of records, are defined according to Equations 2.8 - 2.11.

$$A = \frac{TP + TN}{TP + TN + FP + FN} \tag{2.8}$$

$$P = \frac{TP}{TP + FP} \tag{2.9}$$

$$R = \frac{TP}{TP + FN} \tag{2.10}$$

$$S = \frac{TN}{TN + FP} \tag{2.11}$$

Next, a table containing the calculated metrics for all of the tested devices is assembled, which is also known as APRS table. Lastly, the misclassification matrix is constructed using the achieved true negative rates (a.k.a. specificity) and false negative rates from applying the device identification technique to the records of all of the examined devices. An ideal device identification method should produce a matrix, in which all of the diagonal elements are equal to one and all of the off-diagonal elements are equal to zero.

2.3 Experimental Approach

In order to achieve a comprehensive understanding of the device's circuit and its variabilities in different fabrications, the data collection process is run for five Ethernet cards (manufactured by Genica). In this way, enough data are collected to evaluate the ability of employed PLI technique in a forensic analysis. One of the tested Ethernet cards (i.e. m5c5) is shown in Figure 2.3. The process of acquiring records from the test Ethernet cards is similar between setups: two personal computers (PC) are used in each setup, one to act as the Test PC (TPC) that includes the test Ethernet card, and the other one as the Data Acquisition PC (DAQPC). The DAQPC includes a passively tapped Ethernet card (from Realtek company) in order to receive data from the TPC using a crossover cable. Each data packet is captured in the form of a differential signal (to attenuate environmental noise), and is observed via a Tektronix DPO 7254C Digital Phosphor Oscilloscope, which uses MATLAB for process configuration and control.

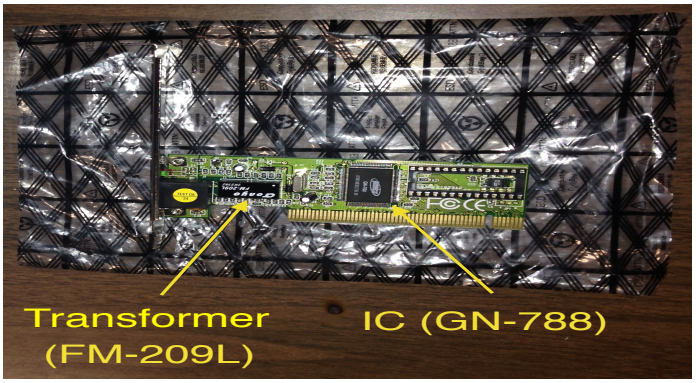

Fig. 2.3: An Ethernet card under test.

According to the oscilloscope configuration, the sampling rate is 10.0 Giga-Samples/Second, the bandwidth is 500 MHz, the record length is 1 million data points, the resolution is 8 bits, and record detection is based on a simple negative slope-based threshold. The TPC is instructed to ping the DAQPC to generate traffic for data acquisition with the goal of acquiring 10,000 numbers of correct records. Meanwhile, in order to reduce the effect of the measurement equipment on the load characteristics of the DAQPC and minimize the possibility of packet loss, only the receiving pins of the DAQPC's Ethernet card on the secondary side of transformer are connected to the oscilloscope. The collected records from all of the examined Ethernet cards during each run constitute a Dataset.

In each of the designed experimental setups according to the desired objectives for behavioral analysis of the devices, the related auxiliary data (for example, temperature data and supply voltage data) are acquired along with the records of the Ethernet cards under test. For each setup, there are two executions of the data acquisition process and consequently two datasets in order to attain a good apprehension of the characteristics and behaviors of the devices. In Setups 1 to 3, two desktop PCs are used for the TPC and DAQPC with GNU/Linux as their operating systems and are placed in the same room. These desktop PCs along with the slots (i.e. 5V 32-bit) of TPC are shown in the left and right parts of Figure 2.4 respectively.

Fig. 2.4: The desktop TPC and DAQPC (left) and the slots of TPC (right).

On the other hand, two mini PCs are used for the TPC and DAQPC with Windows and Xubuntu as their operating systems respectively and are placed in two different rooms

for Setup 4. This setup requires longer cables for PCs communications compare to the other setups. The general view of the experimental setup and the data measurement locations are shown in Figures 2.5 and 2.6.

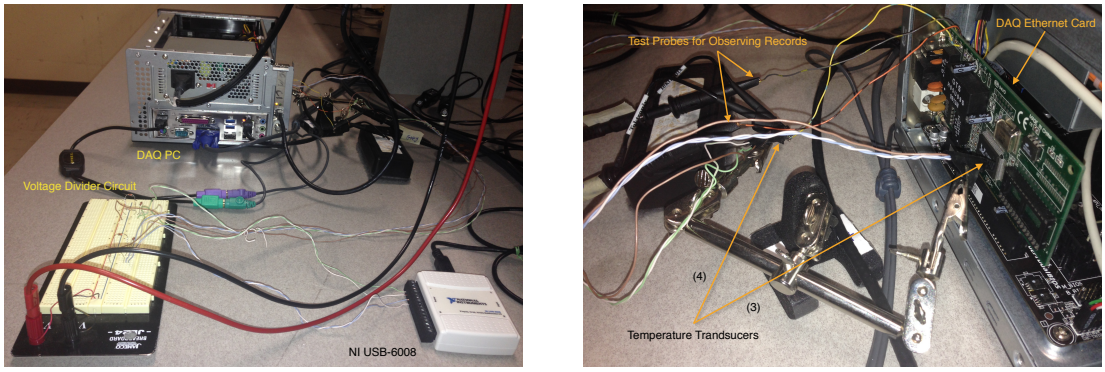

Fig. 2.5: The mini DAQPC and its data measurement location.

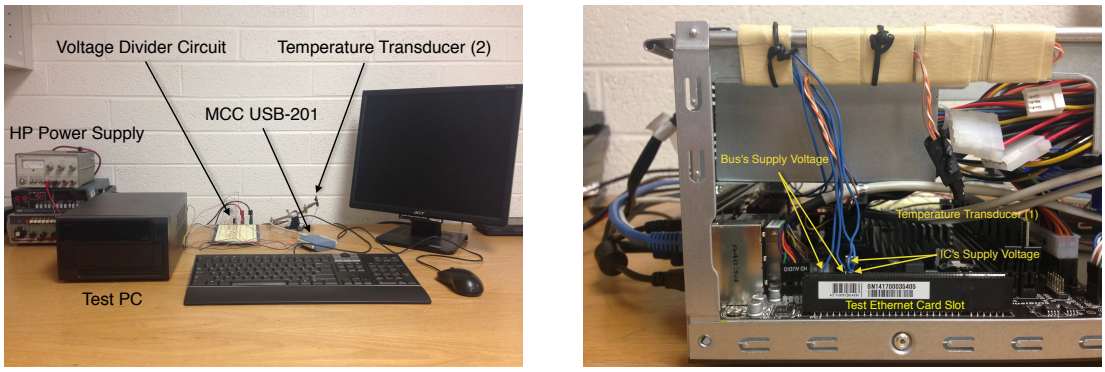

Fig. 2.6: The mini TPC and its data measurement location.

In Setups 1 and 2, the ambient temperature as well as the Ethernet card's surrounding temperature for both the TPC and DAQPC are acquired using a National Instruments USB-6008. According to the objectives of the Setup 2, a hairdryer is used in order to increase the surrounding temperature of the TPC's Ethernet card periodically. In the third and fourth setups, the voltages of the employed LAN transformer (Tonyo FM-209L) and IC (Genica GN-788) in the Ethernet card under test are acquired along with the previously stated temperatures. All of the discussed temperature and voltage parameters are collected via a National Instruments USB-6008 and a Measurement Computing USB-2523 respectively in Setup 3, while in the latter setup the TPC-related temperatures and voltages in addition

to the DAQPC-related temperatures are obtained via a Measurement Computing USB-201 and a National Instruments USB-6008 respectively. According to Figures 2.5-2.6, the TPC's surrounding and ambient temperatures are sensed using the first and second temperature transducers, while those of the DAQPC are sensed using the third and fourth temperature transducers respectively.

2.4 Results and Discussion

In order to examine the device behavior under different operational conditions and states along with achieving an understanding of the device behavior and activities over time, four experiments are designed according to Table 2.1.

Table 2.1: Description of the designed experiments.

Experiment	Datasets	Description
1	1-2	Analyzing the device behavior with respect to the small variations of its surrounding temperature.
2	3-4	Analyzing the device behavior with respect to the large variations of its surrounding temperature.
3	5-6	Analyzing the similarities and differences between the device's signal and the supplied voltages to its printed circuit board's general bus and the mounted IC on it.
4	7-8	Analyzing the device behavior with respect to the factual variations of its surrounding temperature.

2.4.1 Overview of Experiments

The core concept of the explained physical layer identification technique is manifesting and exploiting the existing unpredictable variations in the electronic devices signals (that are introduced during the design and fabrication processes) in order to mark their similarities and differences for identification purposes. Studying these unpredictable variations is helpful in analyzing the device behavior in different operational conditions and over time (i.e. its behavioral stability). In this regard, the developed methodology was applied to five Ethernet cards from Genica manufacturer in four different experimental setups, and at eight distinct times. The information of the Ethernet cards is shown in Table 2.2. According to this table, there should be a correspondence between the MAC address and the analog signal of every

Ethernet card.

Table 2.2: The information of Ethernet cards - (1).

Identifier	MAC Address	Serial
m5c1	00:00:e8:12:65:36	DB0211105319
m5c2	00:00:e8:12:17:db	DB0211105339
m5c3	00:00:e8:12:2c:85	DB0211105358
m5c5	00:00:e8:12:6d:77	DB0211105389
m5c7	00:00:e8:12:65:2e	DB0211105349

For each test run of an experimental setup, the data collection process was carried out on each Ethernet card for ten thousand times that resulted in obtaining 10,000 records (a.k.a. frame). An example of an Ethernet card record is shown in the top plot of Figure 2.7. This voltage signal is from the m5c1 card in the dataset 8 (i.e. the second test run of the fourth experimental setup) and its unit is volt. As was mentioned before, the steady-state part (i.e. synchronization signal) of Ethernet card record is selected in order to identify its nature. This is due to the fact that there are enough variations in this part of the signal for analyzing the device behavior. The synchronization signal of the shown record is presented at the bottom plot of Figure 2.7.

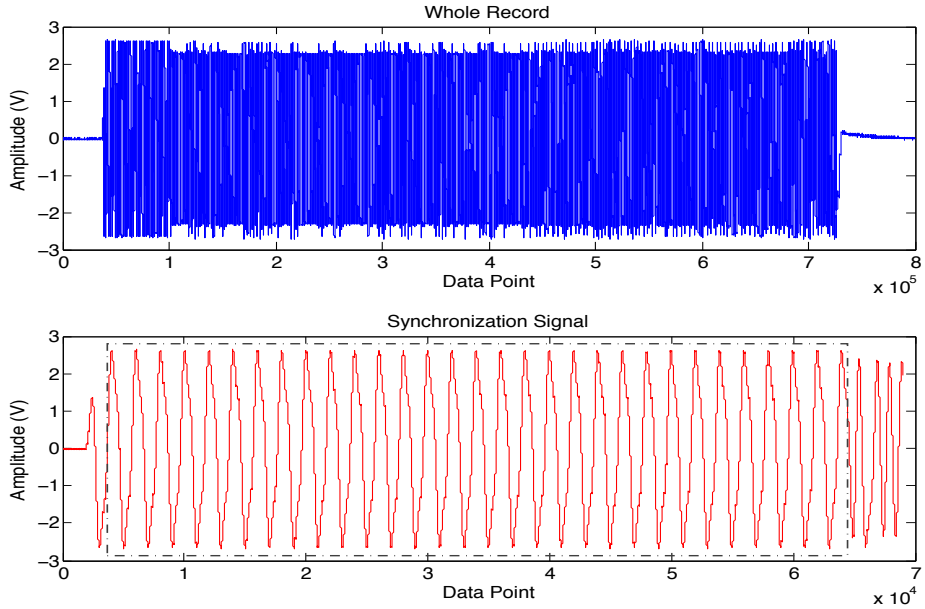

Fig. 2.7: Ethernet card's record (top) and synchronization signal (bottom).

Experimentally, it has been proven that: (a) an electronic device's signal is time-variant; and (b) the signals from two different devices have dissimilar variations at any given time, even if they have the same overall trend. Regarding the case (a), the upper plot of Figure 2.8 shows the variations in the synchronization signals of the first and second records of the m5c2 card, while the lower plot that corresponds to the case (b) shows the variations in the synchronization signals of the first records from the m5c2 and m5c3 cards.

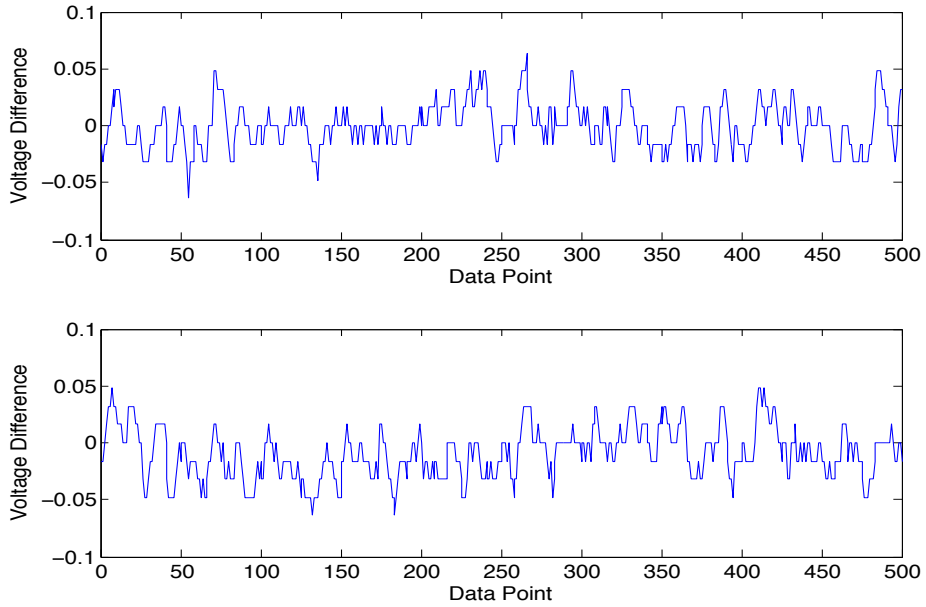

Fig. 2.8: The variations in the device's synchronization signal.

The shown variations are for the first 500 data points of the synchronization signals that are picked from the dataset 8. In fact, these variations can cause a significant change in the level of the matched filter output signal, even between two different test runs of the same setup. Figure 2.9 displays the significant change between the levels of the obtained matched filter outputs from the m5c3 card in the first and second test runs of Setup 3.

According to the implementation of the PLI system, the matched filter is applied to the steady-state portion of the collected records in order to identify the devices and also compare them. In the identification case, the first record of the device is chosen as the reference (i.e. trustworthy) record and the other instances (i.e. 9,999 records) are tested against it. While in the comparison case, the first record of the main device under check

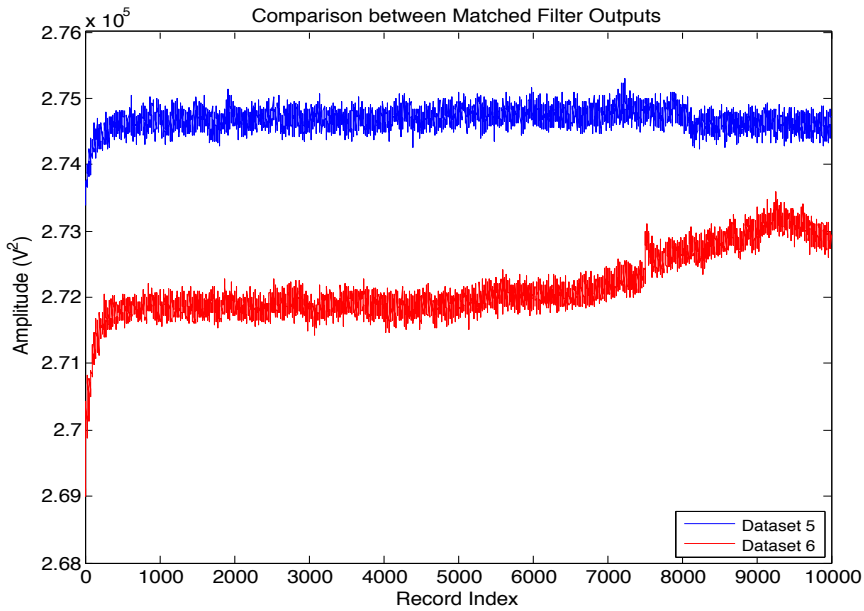

Fig. 2.9: The significant change in the level of MFO signal.

is chosen as the reference record and all of the other records (except the first one) of a secondary device are tested against it. In implementation, the reference records that are used for testing the devices records in all of the setups (except Setup 4) are obtained from the first dataset. In the fourth setup, the reference records are captured from the dataset 7.

The achieved matched filter outputs from these two cases are used to calculate a threshold that determines the acceptance or rejection of the records (i.e. specifically the synchronization signals). The selected values for the parameters n (the number of previous filter outputs that are used as the training data), m (the number of future filter outputs that are utilized as the testing data), and γ (the level of failure) are 25, 20, and 0.01 respectively. Next, the performance metrics are calculated, and the APRS table and misclassification matrix are constructed accordingly. Figure 2.10 displays the APRS table and misclassification matrix for the dataset 8.

The individual and mean values for the accuracy, precision, recall, and specificity (APRS) metrics show the performance of the identification system in acceptance of correct records and rejection of wrong records. In fact, the system demonstrates a good

Tested Card	A	P	R	S
m5c1	0.813	0.999	0.767	0.998
m5c2	0.811	0.999	0.764	0.997
m5c3	0.999	0.999	1.000	0.997
m5c5	1.000	0.999	1.000	0.998
m5c7	1.000	1.000	1.000	0.999
Mean	**0.924**	**0.999**	**0.906**	**0.998**

	Subject m5				
Control	c1	c2	c3	c5	c7
m5c1	0.998	0.934	0	0	0
m5c2	0.943	0.997	0	0	0
m5c3	0	0	0.997	0	0
m5c5	0	0	0	0.998	0
m5c7	0	0	0	0	0.999

Fig. 2.10: APRS table (left) and misclassification matrix (right).

performance in the second test run of experimental setup 4. As was mentioned before, the misclassification matrix is a representation of the true negative rates (i.e. specificity) and false negative rates of the identification system. This matrix shows the capability and weakness of system in identification of the tested devices based on its diagonal and off-diagonal elements respectively. The system indicates an acceptable capability in identification of the devices in this test run. However, it is not successful enough in distinguishing the m5c1 and m5c2 cards.

2.4.2 Analysis of Results

The results of accomplished behavioral analysis on the collected datasets from each designed experiment are presented and discussed in this section. The records of the devices are collected along with the auxiliary data (for example, temperature data and supply voltage data) for the purpose of finding a correlation between them.

Experiment 1: In the first experimental setup that is used for the datasets 1 and 2, it can be observed that there is a relationship between the matched filter output and the surrounding temperature of the Ethernet card under test based on their trends. Depending on the environmental conditions and the internal state and characteristics of the devices, the degree of similarities between these two signals varies.

In other words, the correlation between the matched filter output and the temperature signal can be stronger or weaker from time to time and/or from device to device. Figure 2.11 shows the MFO signal (upper plot) and the device's surrounding temperature signal (lower plot) of the m5c7 card in the first run of Setup 1. The units of the MFO signal

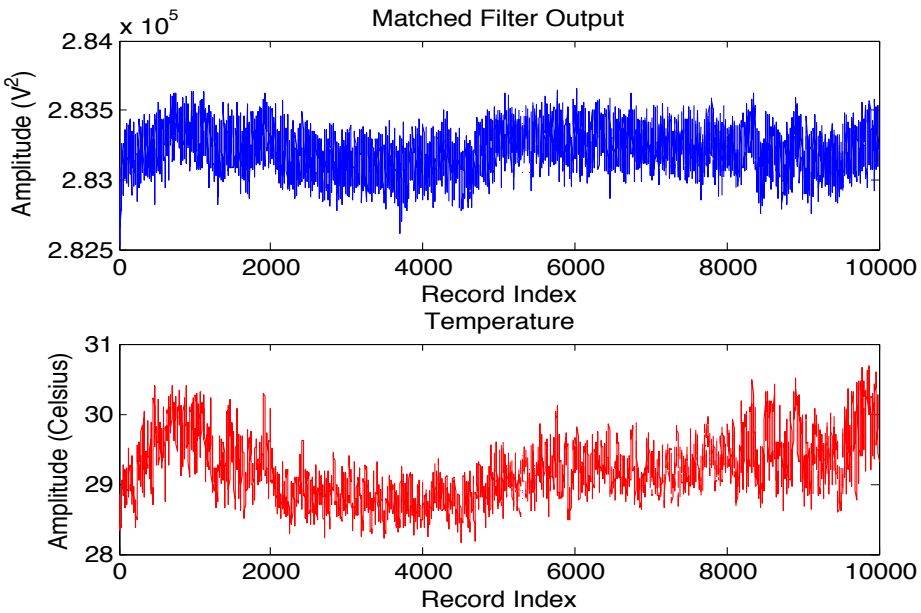

Fig. 2.11: Matched filter output (upper) and surrounding temperature (lower) in Setup 1.

and temperature signal are Volt-Squared (V^2) and Celsius ($^\circ C$) respectively. The PLI system demonstrated a satisfactory performance in identifying the devices and comparing them. Furthermore, the system marked the m5c1 and m5c2 cards as similar devices in both datasets of this experimental setup. The mean of APRS values for datasets 1 and 2 from the tested devices are presented in Table 2.3.

Table 2.3: Mean of APRS values for datasets 1 and 2.

	A	**P**	**R**	**S**
Dataset 1	0.941	1.000	0.926	1.000
Dataset 2	0.927	1.000	0.909	0.999

Experiment 2: In order to scrutinize the relationship between the matched filter output and the device's surrounding temperature, the Setup 2 has been designed for which the temperature is manually increased for the aim of studying its effect on the device's signal. In this setup, the amount of correlation between the filter output and temperature signal at different orders of signal variations is evaluated. According to the results obtained from two iterations of this experiment, the matched filter output is highly affected by changes in the temperature signal. In other words, the device's signal exhibits more dependency on the temperature when it is varied in larger orders. An example of either of the matched filter output and temperature signal for this setup is shown in Figure 2.12 that are appertained to the m5c7 card in the second test run. It can be seen that the matched filter output of the device follows moderated version of the temperature data variations.

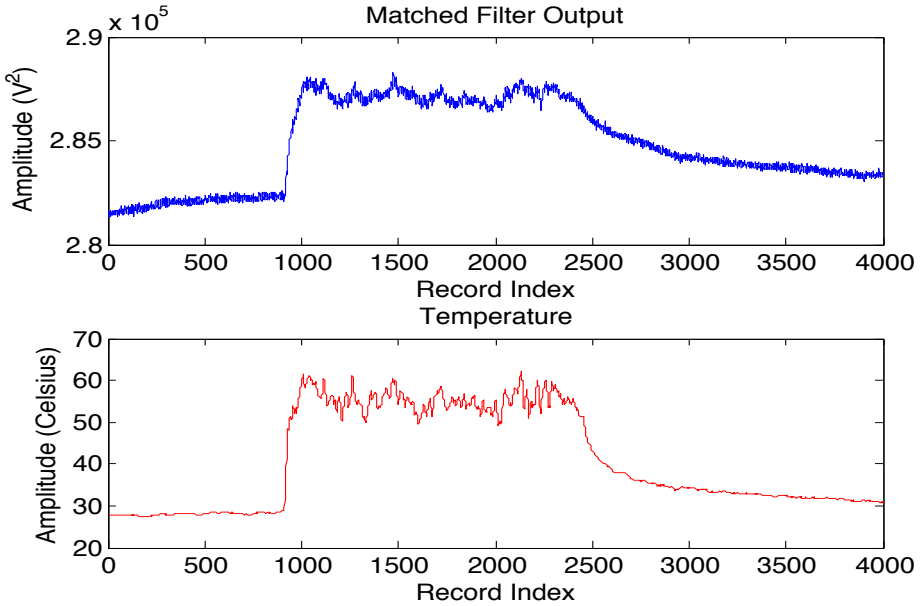

Fig. 2.12: Matched filter output (upper) and surrounding temperature (lower) in Setup 2.

The PLI system has a poor performance in identifying the devices due to getting a large number of false positives and consequently low specificity values for all of the cards (except for the m5c5 in the dataset 2). Also, a number of the Ethernet cards were misidentified in this setup. For example, the m5c1 card was marked as the m5c3, and the m5c7 card was marked as the m5c1 during the first and second test runs. In fact, an attacker can use this

notion in order to defeat the PLI system by increasing the surrounding temperature of a victim device. The results of identification process for this setup are presented in Table 2.4.

Table 2.4: Mean of APRS values for datasets 3 and 4.

	A	**P**	**R**	**S**
Dataset 3	0.838	0.853	0.964	0.331
Dataset 4	0.832	0.870	0.932	0.431

Experiment 3: Although it was demonstrated that the matched filter output has a clear relationship with the device's surrounding temperature, especially at larger orders of variations, it is required to investigate the device circuit-related parameters and the other environmental parameters. In this regard, the voltage that is supplied from the LAN transformer to the general bus of the circuit in addition to the voltage that is supplied to the mounted IC on the circuit are measured in order to find their relationship with the MFO signal. The results of this experiment illustrate a very weak relation between the measured voltages and the matched filter output, which was not expected. The Bus's supply voltage (a.k.a. transformer's supply voltage) exhibits an exponential behavior similar to the MFO signal, while the IC's supply voltage shows an inverse exponential behavior. However, this coherent behavior between these parameters can be eliminated completely by the noise interferences. Meanwhile, the amount of correlation between the matched filter output and the device's surrounding temperature in this setup is similar to the first setup, which was discussed previously.

The MFO signal and the device's surrounding temperature for the m5c2 card during the first test run are shown in Figure 2.13. Additionally, the Bus and IC supply voltages for the same card and test run are shown in Figure 2.14. The unit of these voltage signals is volt. According to these figures, similarities exist between these parameters with the difference that the temperature signal has a higher rank in having relationship with the device's signal in comparison with the other parameters. In fact, due to the noise interference with a supply voltage signal, a sensible mathematical relationship between it and the device's signal can not be established. Finally, the performance of the PLI system in this setup is similar to the

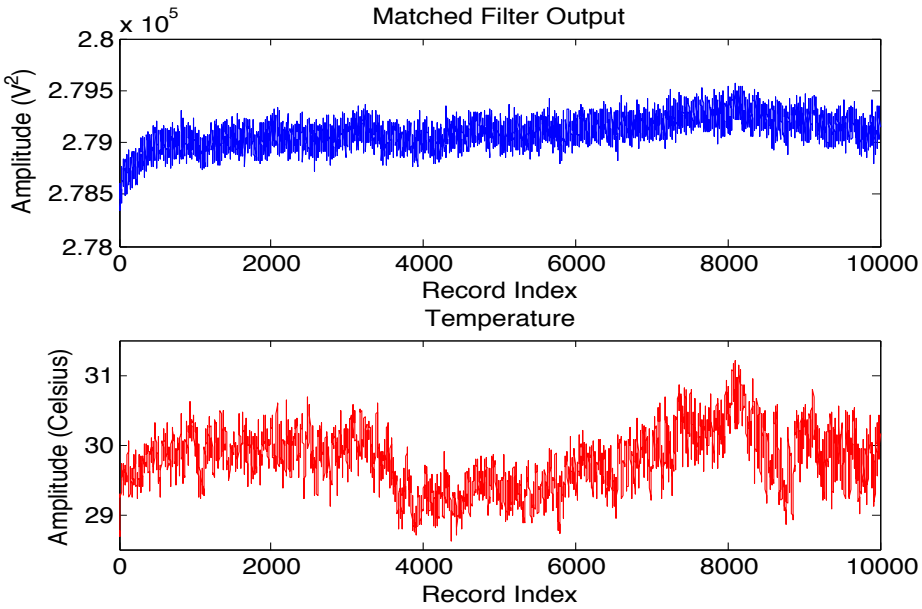

Fig. 2.13: Matched filter output (upper) and surrounding temperature (lower) in Setup 3.

first setup; therefore, the discussions that were made earlier for it will apply here as well. This was expected because these two setups have the same operational conditions including, the room, communication cable length, etc. The results for the performance evaluation of this setup are presented in Table 2.5.

Table 2.5: Mean of APRS values for datasets 5 and 6.

	A	**P**	**R**	**S**
Dataset 5	0.938	1.000	0.923	0.999
Dataset 6	0.933	1.000	0.916	0.999

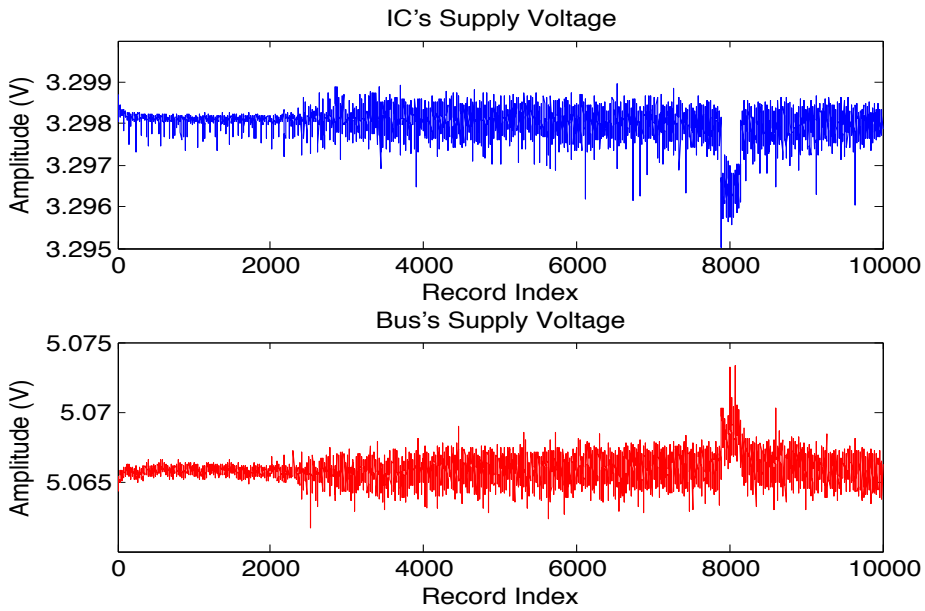

Fig. 2.14: IC's supply voltage (upper) and bus's supply voltage (lower) in Setup 3.

Experiment 4: While the personal computers, the cable type and length, and the location of TPC and DAQPC were all identical for the previous setups, it is beneficial to investigate the effects of changing these components on the device fingerprint. To do this, newer mini personal computers, longer cable, and different locations for the TPC and DAQPC are leveraged in the design of Setup 4. Also, the responsible sensor for measuring the surrounding temperature of the Ethernet card under test is enclosed inside the TPC by limiting the air flow.

According to the acquired data from two test runs with this setup, four major effects are observed: (a) the amplitude of device's voltage signal is decreased by 18-19%; (b) the range of variations in the temperature signal is increased; (c) the direction of the trends of the supply voltages signals is reversed; and (d) the IC's supply voltage shows an observable exponential behavior, which will correlate better with the matched filter output. Meanwhile, a highly smoothed version of the variations in the temperature signal can be seen in both MFO signal and IC's supply voltage signal of this setup.

For the m5c1 card in the dataset 8, the matched filter output and the device's surrounding temperature are shown in Figure 2.15, while the IC's supply voltage and the

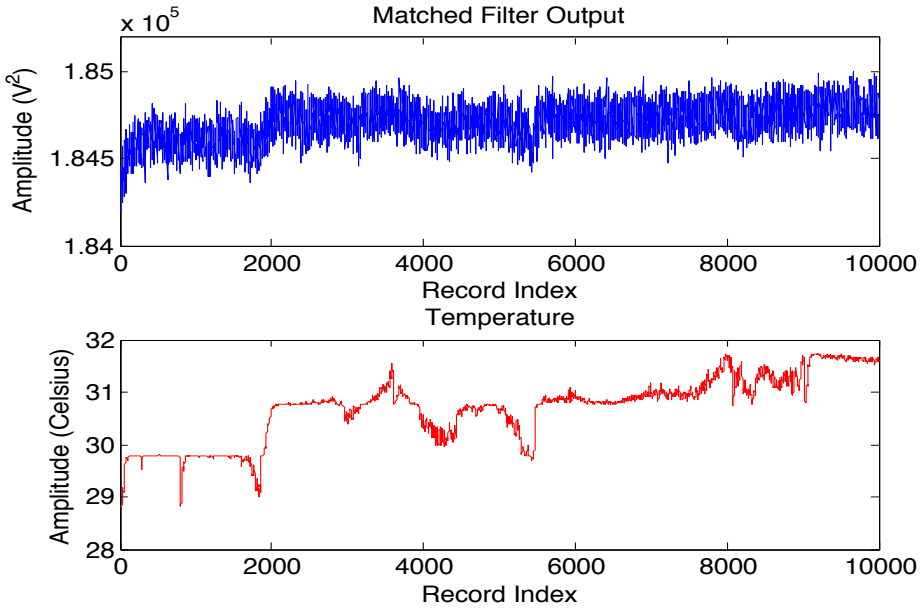

Fig. 2.15: Matched filter output (upper) and surrounding temperature (lower) in Setup 4.

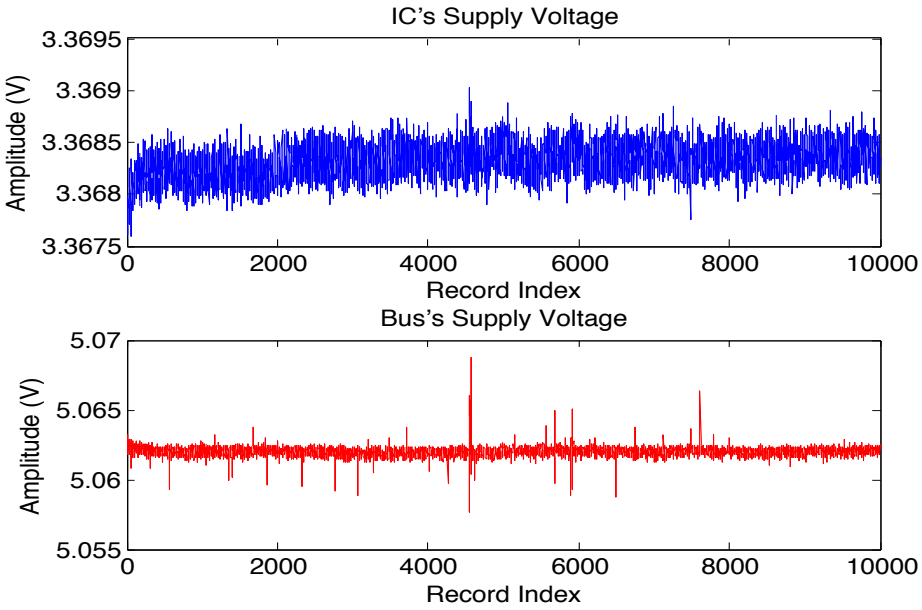

Fig. 2.16: IC's supply voltage (upper) and bus's supply voltage (lower) in Setup 4.

Bus's supply voltage signals are shown in Figure 2.16. Finally, it should be pointed out that the PLI system could function properly in this setup, similar to the first and third setups. The values of the specificity metric for the tested cards decreased slightly, which can be caused by the existence of the larger range of variations in the temperature signal. The performance analysis results for this test setup are listed in Table 2.6.

Table 2.6: Mean of APRS values for datasets 7 and 8.

	A	**P**	**R**	**S**
Dataset 7	0.924	1.000	0.906	0.998
Dataset 8	0.924	0.999	0.906	0.998

Chapter 3

Study of Tracking System Models

3.1 Overview

Studying the unique variations of a device's electrical signal under different operational conditions and states is crucial for developing a robust and integral physical layer identification system. In this regard, a tracking system capable of modeling the device behavior and predicting its future signal data should be developed. The proposed strategy for implementing this tracking system has two steps. In the first step, different data preparation concepts are applied to the device's signal and/or the auxiliary data (for example, ambient temperature and supply voltage) in order to study their variations, and eventually manifest their trends. Next, various data modeling techniques are executed on the prepared data with the goal of constructing the most efficient data predictive model for the device future signals.

3.2 Concepts for Data Preparation

In this section, the employed data preparation concepts for development of the tracking system are introduced.

3.2.1 Charging/Discharging Trend

According to the results of the applied matched filter to the acquired signals from the Ethernet cards under test, it can be seen that there is charging/discharging trend in the time-domain behavior of the device's circuit (refer to Figure 2.9). This behavior is possibly due to the leveraged series resistor-capacitor (RC) sub-circuit in the main circuit. An RC circuit is composed of resistor(s) and capacitor(s), and is driven by a voltage or current source. When the circuit is active, the capacitor is charged up gradually through

the resistor until the voltage across the capacitor reaches that of the supply voltage. Once the supply voltage is disconnected from the circuit, the capacitor would discharge itself back through the resistor. The formulations that depict the charging and discharging trends of the circuit are presented in Equations 3.1 and 3.2 respectively [35]. In these equations, V_C is the voltage across the capacitor, V_S is the supply voltage, t is the elapsed time since the connection/disconnection of the supply voltage, and RC is the circuit time constant. In implementation, the expression in the right side of charging/discharging equation (excluding V_S) is used in prediction of the matched filter output signal. The parameter t is described as the duration time of collecting records for each device in each test run.

$$V_C = V_S.(1 - \exp(\frac{-t}{RC})) \qquad (3.1)$$

$$V_C = V_S.\exp(\frac{-t}{RC}) \qquad (3.2)$$

3.2.2 Euclidean Norm

The Euclidean norm (or 2-norm) of a data vector provides a measure of the magnitude of the vector elements. In other words, it calculates the Euclidean distance of the vector with respect to the origin of the space. The Euclidean norm of the data vector x defined in an n-dimensional space can be calculated by using Equation 3.3 [36].

$$\|x\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2} \qquad (3.3)$$

3.2.3 Mean of Absolute Value (MAV)

MAV is one of the most popular time-domain feature extraction methods for signals, which provides the average of the rectified version of a signal (i.e. the average of the absolute values of the signal data points), and technically specify the signal power level. Equation 3.4 represents the mean of the absolute value of signal $f[k]$, with N number of data points [37].

$$MAV = \frac{1}{N} \cdot \sum_{i=1}^{N} \left| f[i] \right| \qquad (3.4)$$

3.2.4 Autoregressive Model

Autoregressive model is used for describing certain time-varying processes that exist in nature, economics, etc. According to this model, a signal data at a certain time depends linearly on its previous values and on a stochastic error term. Also, the "autoregressive" term is defined as the linear regression of a variable against its previous values (with respect to time). Equation 3.5 shows the autoregressive model in which, X is the time-domain signal, ϵ is the error data, c is the constant term, p is the model order, and ϕ is for the model parameters (a.k.a. coefficients) [38].

$$AR(p) : X_t = c + \epsilon_t + \sum_{i=1}^{p} \phi_i . X_{t-i} \tag{3.5}$$

3.2.5 Moving Average

Moving average is a filter that smooths out short-term fluctuations and highlights long-term trend of a signal. The filtering process is done by averaging the signal data points in equal length subsets. These subsets are represented by a mobile Window, which starts its action from the first data point and moves toward the last data point. In Equation 3.6, the relationship between the input signal and the output signal of this filter is presented [39]. The parameter $x[t]$ represents the input signal that has N data points, M is the window size, and $y[k]$ is the output signal.

$$y[k] = \frac{1}{M} \cdot \sum_{j=0}^{M-1} x[k+j] \quad , \quad 1 \leq k \leq N - (M-1) \tag{3.6}$$

3.2.6 Normalization

Normalization is the process of regularizing data values based on a specific statistical analysis concept. The normalization concept used in this work refers to the adjustment of a data vector with respect to its magnitude (i.e. 2-norm) [40].

3.2.7 Standard Deviation

The standard deviation of a signal data indicates the amount of variations or dispersions

of its data points from their average value. When the outcome of this function is close to zero, it is interpreted that the data points of a signal are very close to the expected value (i.e. signal average). Contrariwise, they are diffused over a wider range of values when the outcome is a high value. The standard deviation of signal $x[t]$ that has N data points is calculated using Equation 3.7 [41]. The parameter μ_x represents the average value of the signal.

$$STD = \sqrt{\frac{1}{N-1} \cdot \sum_{i=1}^{N} \left|x[i] - \mu_x\right|^2} \tag{3.7}$$

3.3 Techniques for Data Modeling

The data modeling techniques used for developing the tracking system are described in this section.

3.3.1 Correlation Analysis

Correlation analysis is used to measure the degree of linear dependency between two variables. In this approach, one variable is called Independent and the other one is called Dependent. Then, the correlation function tries to discover whether a change in the independent variable will result in a change in the dependent one. The outcome of this function is called Correlation Coefficient, which is always between -1 and +1. When the outcome is equal to 0, it means that there is no linear relationship between the variables. The correlation coefficient of either -1 or +1 indicates that the variables are perfectly related. The positive sign shows that the change occurs in the same direction, while the negative one shows the direction is opposite. Equation 3.8 is used to calculate the correlation coefficient of variables X and Y [42].

$$Correlation\ Coefficient\ (X,Y) = \frac{\sum (X-\mu_X).(Y-\mu_Y)}{\sqrt{\sum (X-\mu_X)^2 \cdot \sum (Y-\mu_Y)^2}} \tag{3.8}$$

3.3.2 Cross Correlation Analysis

It is a measurement of similarity between two time-series of data as a function of the time lag between them. In other words, if X and Y are two time-series signals, the cross correlation function (a.k.a. sliding dot product) tries to find a relationship between X and the shifted copies (in both negative and positive directions) of Y. The outcome of this analysis is presented in the form of a function of the examined lags. The cross correlation function is defined as [43]:

$$(X * Y)\,[n] = \sum_{m=-\infty}^{\infty} X^*[m].Y[m+n] \tag{3.9}$$

3.3.3 Autocorrelation

Autocorrelation is the cross correlation of a time-series signal with itself. This procedure tries to find a relationship between a time-series signal and its own time-lagged copies. This function is useful in finding obscured repetitive patterns in a signal [44].

3.3.4 Simple Linear Regression (SLR)

Simple linear regression (SLR) is a technique that is used to determine the effect of changes of a variable (the explanatory variable) on another variable (the response variable) with the purpose of finding the linear relationship between the variables and predicting the future values of the response variable (a.k.a. the variable of interest) [45]. In this method, a straight line is fitted through the cloud of data points in the X-Y plane. The shape of the fitted line depends on the degree of the explanatory variable. The slope (β) and vertical intercept (α) of this line are calculated based on the correlation between the variables and crossing of the line from the center of the cloud of data points respectively. The Equations 3.10 and 3.11 represent the actual (based on assumption) and the modeled relationships between the response variable (y) and the explanatory variable (x) respectively. The predicted data points using this model are represented by $\hat{y}$ variable in this context.

$$Actual\ Model\ (Assumption) : y_i = \alpha + \beta.x_i + \epsilon_i \quad , \quad i = 1, \ldots, N \tag{3.10}$$

$$Prediction\ Model : Y = \alpha + \beta.X \tag{3.11}$$

$$\hat{y}_i = \alpha + \beta.x_i \quad , \quad i = 1, \ldots, N \tag{3.12}$$

The fitted line will not pass through all of the data points and deviates from each by a certain degree. The vertical distance between each data point and the fitted line (i.e. the difference between the actual value and the predicted value of the response variable) is called a Residual, which in fact specifies the error of the prediction model. The residual parameter is used to define a minimization function (shown in Equation 3.13), which its solution provides the coefficients of the prediction model.

$$Q(\alpha, \beta) = \sum_{i=1}^{N} \epsilon_i^2 = \sum_{i=1}^{N} (y_i - \hat{y}_i)^2 \tag{3.13}$$

Moreover, it is used in calculation of Coefficient of Determination (a.k.a. R-Squared), a statistical measure that provides information regarding the goodness of the fit (i.e. the model accuracy in predicting data). The R-Squared value of 0 corresponds to a completely scattered data points around the fitted line, whereas the value of 1 specifies a fitted line that passes through all of the data points. Equations 3.14 - 3.17 are employed to calculate the R-Squared value.

$$Total\ Sum\ of\ Squares : SS_{tot} = \sum_{i=1}^{N} (y_i - \mu_y)^2 \tag{3.14}$$

$$Regression\ Sum\ of\ Squares : SS_{reg} = \sum_{i=1}^{N} (\hat{y}_i - \mu_y)^2 \tag{3.15}$$

$$Residual\ Sum\ of\ Squares : SS_{res} = \sum_{i=1}^{N} (y_i - \hat{y}_i)^2 \tag{3.16}$$

$$Coefficient\ of\ Determination : R^2 = 1 - \frac{SS_{res}}{SS_{tot}} \tag{3.17}$$

Also, the coefficient of determination is influenced by the number of introduced explanatory variables into the model, which might either improve or harm its value. In order to achieve an optimal number of explanatory variables for the prediction model, an associated statistical measure named, Adjusted R-Squared is presented, the value of which is always less than or equal to the R-Squared value. Growth in the value of this measure is achieved only if the introduced explanatory variable(s) into the model improves the R-Squared value more than what is expected. In this way, the achieved prediction model provides the best functionality without having redundant terms. The formulation for the adjusted R-Squared is defined as:

$$Adjusted\ R - Squared : \bar{R}^2 = 1 - \frac{\frac{SS_{res}}{SS_{tot}} \cdot (N-1)}{N-P} \tag{3.18}$$

Where, the parameter P is the number of regressors in the model (including the constant term). Other regression-based techniques have a lot in common with the simple linear regression technique, except some differences in the data prediction mechanism.

3.3.5 Multiple Linear Regression (MLR)

This technique is very similar to the SLR technique with the difference that the response variable is a function of more than one explanatory variables. The prediction model for this technique is shown in Equation 3.19. In this equation, Y represents the response variable, X_i represents the ith explanatory variable, and other parameters are coefficients [46].

$$Y = \alpha + \beta_1.X_1 + \beta_2.X_2 + \beta_3.X_3 + \cdots \tag{3.19}$$

3.3.6 Non-Linear Regression (NLR)

According to this technique, the prediction model for the response data is a non-linear combination of the model parameters (a.k.a. the coefficients) and one or more explana-

tory variables. The fitted line is achieved by a method of successive approximations (for example, numerical optimization algorithms). $Y = f(X, \beta)$ shows a general representation of the prediction model, which is a non-linear function of the coefficients and explanatory variable(s) [47]. Meanwhile, it is possible to suitably linearize some non-linear prediction models (for example, exponential or logarithmic functions) by applying different mathematical methods to them.

3.3.7 Robust Regression

The common regression-based techniques can provide accurate results when their underlying assumptions are satisfied. Dissatisfaction of these assumptions (for example, when the error data in a linear regression are not normally distributed) causes insensibility of the techniques to the outliers (i.e. the data points that do not follow the pattern of the rest), which leads to misleading results. In order to overcome this problem, the robust versions of the techniques are used [48]. These modified techniques use a process called Iteratively Reweighted Least Squares to resist against the outliers. This process works based on using the weighted data points in an iterative process. According to this approach, all of the data points are weighted equally using a weighting function such as Bisquare, Huber, etc. From the next iteration, the data points that were located farther from the other data points in previous iteration are given lower weight values. This iterative process continues until the best coefficients for predicting the response data are achieved [49].

3.3.8 General Linear Model (GLM)

In most of the common regression-based techniques, the default assumptions for the error terms are: (a) they are uncorrelated across measurements, and (b) they follow a normal (a.k.a. Gaussian) distribution (either one-dimensional or multi-dimensional depending on the number of error terms). The Gaussian distribution is considered for the response data conventionally. However, there exist some cases that both the response data and error data do not follow a normal distribution. In order to tackle this issue, general linear model (GLM) technique is used that relaxes the assumptions for the response and error data by

using other data distribution models such as Inverse Gaussian (IG), Poisson, and Gamma distributions. The best distribution for the prediction model is the one that results in the highest accuracy in predicting the response data with the lowest error.

Due to the fact that each type of distribution has a unique formula for calculating the mean value (a.k.a. expected value), it is required to have a function for relating the explanatory variables to the mean of the employed distribution. A function, $f(.)$ that is used for this purpose is called Link Function, which creates a mapping between the mean of the response data (according to the chosen distribution) and the explanatory data. Meanwhile, the model of this technique is in fact a generalization of the model of MLR technique. This is due to the fact that there is a linear relationship between the response data and the explanatory data. However, the possibility of entering multiple response variables along with having various options for the response data distribution exists in this technique.

The formulations for the prediction model and link function are shown in Equations 3.20 and 3.21 respectively [50]. In these equations, Y represents the response variable(s), X represents the explanatory variable (s), U represents the error variable(s), and B represents the coefficients. Also, the constant term of the model is included in the X parameter.

$$Y = X.B + U \tag{3.20}$$

$$f(\mu_Y) = X.B \tag{3.21}$$

3.3.9 Smoothing Spline

Smoothing spline is a dual-purpose technique since it can be used either as a predictive model for the response data or as a filter for the output signal of a system in order to smooth it and eliminate the noise. When using this technique as a predictive model, a spline function is employed to fit a smooth curve to the response data using the explanatory data. The filtering process is accomplished in a similar way. The desired spline function is obtained by solving the minimization problem that is shown in Equation 3.22. In this equation, y is the

response variable, x is the explanatory variable, $S(.)$ is the spline function, w is the weight that is equal to 1 for all of the data points by default, and ρ is the smoothing parameter [51].

$$\rho.\sum_{i=1}^{N} w_i.(y_i - S(x_i))^2 + (1-\rho).\int_{x_1}^{x_n} (\frac{d^2S}{dx^2})^2.dx \tag{3.22}$$

If the value of smoothing parameter is not specified, it is selected automatically near the value of interest that is calculated by Equation 3.23. The parameter h in this equation represents the average of distances between the data points.

$$Value\ of\ Interest = \frac{1}{1+\frac{h^3}{6}} \tag{3.23}$$

3.3.10 ARMA and ARMAX Modeling

Autoregressive Moving Average (ARMA) technique is used to understand the behavior of a time-series of data (i.e. a stationary stochastic process) with the purpose of predicting its future values. The ARMA model that is shown in Equation 3.24 consists of two polynomials that are built by applying the autoregressive (AR) model and moving average (MA) model to the previous values of the time-domain signal under study [52]. In fact, this model is capable of predicting the future values of a signal with the knowledge of its previous values solely.

$$ARMA(p,q) : X_t = c + \epsilon_t + \sum_{i=1}^{p} \phi_i.X_{t-i} + \sum_{i=1}^{q} \theta_i.\epsilon_{t-i} \tag{3.24}$$

In Equation 3.24, X is the time-domain signal, ϵ is the error data, c is the constant term, p and q are the orders of AR and MA models respectively, and ϕ and θ are the model parameters (a.k.a. coefficients) of AR and MA models respectively. The model error terms are considered as a white noise signal that is sampled from a normal distribution with zero mean value. These terms are independent and identically distributed random variables, where each has the same probability distribution as the other ones and all are mutually independent. After specifying the best values for the orders of the AR and MA models,

the model parameters are calculated by minimizing the error data using the least squares regression method.

Autoregressive Moving Average with Exogenous Inputs (ARMAX) technique is considered as the developed version of the ARMA technique. In this technique, an exogenous input (X) model is employed along with the previously mentioned models in order to understand the behavior of the signal under investigation and predict its future values. The formulation of ARMAX model is shown in Equation 3.25, in which d and η are the exogenous input signal and its associated coefficient(s) respectively, and b is the order of the exogenous input model [52].

$$ARMAX(p,q,b) : X_t = c + \epsilon_t + \sum_{i=1}^{p} \phi_i.X_{t-i} + \sum_{i=1}^{q} \theta_i.\epsilon_{t-i} + \sum_{i=0}^{b} \eta_i.d_{t-i} \tag{3.25}$$

3.3.11 Analysis of Residuals

Analysis of residuals is a powerful diagnosis tool that can be used for the following purposes [53,54]: (a) validating the relationship between the response data and explanatory data, and finding the sensitivity of a prediction model to each explanatory variable, (b) checking the response data distribution, and (c) evaluating the response data dispersion. So, it helps to understand the accuracy of a prediction model, provides intuition on how to improve the model, and detects any violation of the underlying statistical assumptions (for example, the incorrect shape of chosen distribution, the existence of outliers or any unusual features).

For an ideal case, the magnitude of residuals should be small and there should not be any pattern in their scatter plot (i.e. having noisy residuals data). This implies that all of the required explanatory variables were found successfully and the response signal is predicted with a good degree of accuracy. If any of the required explanatory variables is missing, any of the underlying statistical assumptions in developing the regression model is violated, and/or there is no correlation between the response data and explanatory data, then it will result in a non-random pattern in the residuals scatter plot.

3.3.12 Thermal System Modeling (TSM)

A thermal system operates based on storing and/or transferring the heat flux [55]. Heat can flow between objects in three different mechanisms that are conduction, convection (including mass transfer), and radiation. In conduction mechanism, the heat flows when there is a temperature difference across an object or between objects. Convection occurs in the fluids (for example, liquids and gases) when groups of molecules move through advection or through diffusion or as a combination of both. Radiation is made by thermal motion of the charged particles (for example, ions, electrons, and protons) due to electromagnetic radiation. Thermal systems can be modeled with certain mathematical formulations that are analogous to those of electrical circuits.

The fundamental elements in a thermal system are ambient temperature (which is modeled as ground in electrical circuits), thermal resistance (in accordance with electrical resistance), thermal capacitance (similar to electrical capacitance), heat source (similar to current source), and external temperature (similar to supply voltage). There are four components that determine the heat flow through an object: (a) the temperature difference between two objects or between the inside and outside of an object, (b) the thickness of the side of an object that the heat is passing through, (c) the object cross-sectional area, and (d) the thermal conductivity (i.e. the ability to conduct heat) of the object material. Using these parameters, two formulations can be defined for the system thermal resistance that are presented in Equations 3.26 and 3.27.

$$Thermal\ Resistance\ (R_{th}) = \frac{Object\ Thickness}{Thermal\ Conductivity \times Object\ Area} \quad (\frac{^{\circ}Kelvin}{Watt}) \quad (3.26)$$

$$Q_{High-to-Low} = \frac{\theta_{High} - \theta_{Low}}{R_{th}} \quad (Watt) \quad (3.27)$$

In Equation 3.27, Q is the heat flow, θ_{High} is the temperature of the warmer object, θ_{Low} is the temperature of the colder object, and R_{th} is the thermal resistance. Thermal

capacitance is defined as an indication for the amount of heat that an object can store. According to this definition, there is either increase or decrease in the internal temperature of an object when the heat flows in or out.

Based on Equation 3.28 that is used to calculate the thermal capacitance of an object, m is the object mass and C_{th} is its specific heat (i.e. the required amount of heat per unit mass to raise the temperature of an object by one degree Celsius).

$$Thermal\ Capacitance\ (C_{th}) = m \times C_p \tag{3.28}$$

The generation of a certain amount of heat (or power) in a system is accomplished by a heat source that can operate in either constant or variable modes with respect to time. The generated heat can be calculated by different mathematical models. The formulation that is used in this study to calculate the heat flux is shown in Equation 3.29. In this equation, $\Delta\theta$ is the difference between the final internal temperature (θ_{Final}) and initial internal temperature ($\theta_{Initial}$) of an object, and Δt is the time that the object goes through the heating or cooling process.

$$Q_{(\theta_{Final}-\theta_{Initial})} = \frac{m \times C_p \times \Delta\theta}{\Delta t} \tag{3.29}$$

Finally, it should be stated that any thermal system can be mathematically modeled using the Energy Balance theory. Based on this theory, at any given node (i.e. location) in the system, the entered heat into the node is equal to the emitted heat from the node plus the stored heat inside the node.

3.4 Results and Discussion

3.4.1 Overview of Prediction Models

In this section, the results of the prediction models that are constructed using the studied data preparation concepts and data modeling techniques are presented and discussed. Analyzing the results provides an understanding of the device's signal behavior and its dependency on the environmental and circuit-related parameters. It will help in developing an efficient tracking system capable of predicting the device behavior under different conditions and over time. The created prediction models are divided into two categories: (a) Basic Models that are constructed using a single data modeling technique; and (b) Combined Models that are built by leveraging two different data modeling techniques. The performance of each of these models is evaluated by studying the minimum, mean, median, and maximum of the R-Squared values that are achieved by running the model on the respective data (for example, the matched filter output, device's surrounding temperature, et cetera), acquired from the five Ethernet cards under test.

Tables 3.1-3.5 show the results of running the developed basic and combined models on the data acquired from the Ethernet cards. The main parameters that are present in most of these models are MFO, Temperature, IC's Supply Voltage, Bus's Supply Voltage, and Charging/Discharging Trend Data. These parameters correspond to the matched filter output, the surrounding temperature, the supplied voltage to the IC mounted on the device's circuit, the supplied voltage to the circuit general bus, and the calculated data using the charging/discharging trend formulation respectively. The prediction models are designed with the purpose of discovering the relationship between two or more parameters that can be employed in the tracking system. During the model development process, with respect to the purpose that is followed, different statistical methods (such as normalization, mean of absolute value, and moving average) are applied to the parameters data in order to manifest their behavior more accurately.

Many of these models are applied to multiple datasets in order to guarantee the consistency of their performance results. In the "Dataset(s)" column of Tables 3.1-3.5, the

sign "+" means concatenation of the datasets and the word "*and*" means the datasets are used in the same data matrix (i.e. they have their own positions in the matrix of data and aren't concatenated). The sign "$\sim$" in the "Model" column is used to represent the similarity between the left side variable (i.e. response variable) and right side variable(s) (i.e. explanatory variable(s)).

The utilized data prediction techniques in the basic and combined models are: simple linear regression for Models 1-19, multiple linear regression for Models 20-25, general linear model for Model 26, non-linear regression for Model 27, ARMA modeling in Model 28, ARMAX modeling in Models 29-30, correlation analysis in Model 31, autocorrelation analysis in Model 32, cross correlation analysis in Model 33, the combination of smoothing spline method and simple linear regression in Models 34-35, the combination of multiple linear regression and non-linear regression in Models 36-49, and the combination of thermal system modeling and simple linear regression in Model 50.

3.4.2 Basic Models

Regarding the SLR-based models, the purpose of building Models 1-6, 8, 11, 12, and 16-19 is to find the relationship between the device's record (i.e. in terms of its noisy and steady-state parts and the related matched filter output) and its surrounding temperature. Figure 3.1 shows the achieved scatter plot from running Model 1 on the acquired data from the m5c2 card in the second test run of Setup 3.

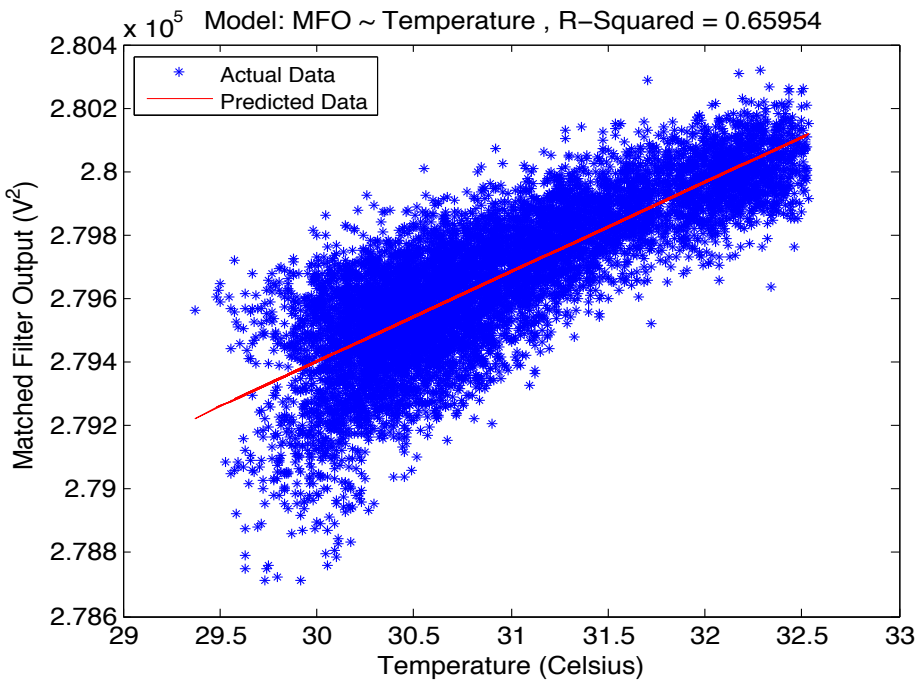

Fig. 3.1: A scatter plot for Model 1.

For Models 7, 9, and 13-15, the goal is to find the correlation between the matched filter output and the IC's supply voltage. Also, finding the connection between the matched filter output and the Bus's supply voltage is the objective in Model 10. The Aligned Synchronization Signals variable in Models 3 and 4 is referred to as the steady-state parts of the records under test that are aligned before the matched filter is applied to them. The window size for moving average function is 100 in Model 8 and it is 15 in Models 15-17. Figure 3.2 shows the ability of this function to filter out the present fluctuations and noise in the signal.

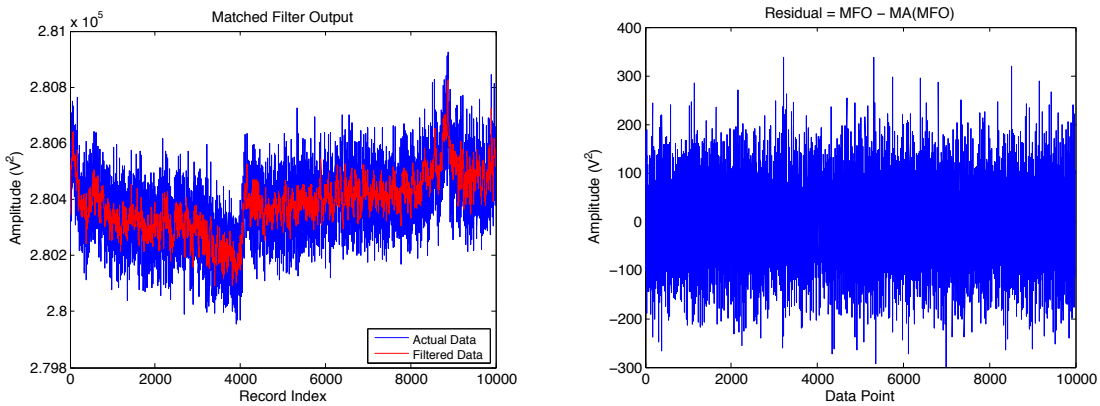

Fig. 3.2: Filtering MFO signal using moving average function with a window size of 10.

The derivation function that is used in Model 16 is for manifesting the device's signal trend (a.k.a. the average signal). However, it increases the noise effects due to amplification of the signal high frequency components. In order to tackle this issue, a filter (such as the moving average function with large window size) is required to attenuate these unwanted effects.

Models 18 and 19 are designed based on two different but related strategies: (a) there might be a delay between the effects of the device's surrounding temperature and its synchronization signal. Therefore, it is assumed that there is a lag between sensing the temperature and observing its effect on the matched filter output. This delay is implemented in Model 18 by shifting the matched filter output data vector to the right and the temperature data vector to the left; and (b) the process of collecting records might be accomplished with a lower speed than the temperature data acquisition. In other words, it is assumed that the corresponding temperature of the device's synchronization signal is seen with a delay due to the possible difference between the operating speeds of the oscilloscope and the DAQ device. This strategy is implemented in Model 19 by shifting the matched filter output data vector to the left and the temperature data vector to the right. The shift operation (either left or right) in each of these cases is run fifteen times.

Once the amount of linear correlation between each pair of parameters is found, it is required to study other assumptions in creating the prediction models: (a) more than one explanatory variables, and (b) different types of connecting functions. Due to the fact

that all of the characteristics of the matched filter output cannot be predicted by using the device's surrounding temperature solely, the Model 20 was designed, for which the device's matched filter output is predicted by using its corresponding temperature data along with the matched filter output of the same card from the previous dataset. Model 25 was tested in both non-robust and robust modes in order to investigate the influence of outliers on the amplitude of residuals. Moreover, the outcome of examining different distributions for the response data is shown in the results of Model 26.

The ARMA regression technique is incorporated in Model 28, which has two stages of training and testing for data prediction. In the training stage, the values of the p and q orders are in the range of {1:5,10,20,50,100,110}. Once the model is run on a dataset, the desired values of orders in predicting the MFO signal of each Ethernet card are calculated. These values are used to create the Outcome Range that is used in the testing stage. In this stage, the data prediction process is run on another dataset. Models 29 and 30 were created using ARMAX modeling technique. The difference between these two models is in the used range in the training stage. In Model 29, the employed range is similar to the one used in Model 28. While in Model 30, the leveraged range of values for the orders is {1:10}.

3.4.3 Combined Models

In order to construct a more accurate model for prediction of the device behavior, multiple data modeling techniques can be combined. In fact, each of the leveraged techniques in creation of a prediction model can be helpful in understanding a portion of the device's signal. The goal in designing Models 34 and 35 was to eliminate the disturbing fluctuations and noise effects that exist in the matched filter output signal in order to achieve a smoother data to be predicted by the device's surrounding temperature. The difference between these two models is in the mode of robust simple linear regression technique, which determines the method for residuals calculation. The robust mode used in Model 34 is Bisquare Weight, while it is Least Absolute Residuals (LAR) in Model 35. The residuals are calculated in bisquare weight mode by minimization of a weighted sum of squares (i.e. the weight given to each data point depends on how far the point is located from the fitted line). In other

words, the closer the point is to the fitted line, the larger the weight it gets. In LAR mode, a line or curve is determined that minimizes the absolute difference of the residuals rather than the squares difference (which is used in the regular mode).

The parameter "Fitted MFO" in Models 40 and 41 represents the predicted matched filter output data that are calculated using non-linear regression technique. In the NLR model, the explanatory variable is time and the function is the formulation of the circuit charging/discharging trend. The moving average function implemented in Models 42-45 has the window size of 25 for the related parameters. The technique of analyzing the residuals that is used in Models 46-49 consists of two stages in this study. In stage 1, the matched filter output data are predicted by either multiple linear regression technique (using the device's surrounding temperature and IC's supply voltage) or non-linear regression technique (using the charging/discharging trend data) and the respective residuals are calculated. The residual parameter from stage 1 has the role of response variable in the second stage, and is predicted by parameter(s) other than the one(s) used in the previous stage. In other words, if the matched filter output was predicted by using the charging/discharging trend data, then the stage 1's residual parameter is predicted using the device's surrounding temperature and the IC's supply voltage, and vice versa. By analyzing the achieved residuals from both stages, we will be able to determine the priority and importance of each explanatory parameter in getting a high R-Squared value.

According to the strategy of Model 50, the device's signal and consequently its matched filter output can be affected directly by the device's internal temperature rather than the surrounding temperature, despite the correlation between them. Therefore, the thermal system modeling technique is utilized in order to create a model for calculating the device's internal temperature, which is used as the explanatory variable for predicting the matched filter output. The employed model [56] for this purpose is shown in Figure 3.3, in which Q_{in} is the heat source, θ_{int} is the device's internal temperature, θ_{ext} is the device's external temperature that is time-variant, R_{th} is the thermal resistance, and C_{th} is the thermal capacitance.

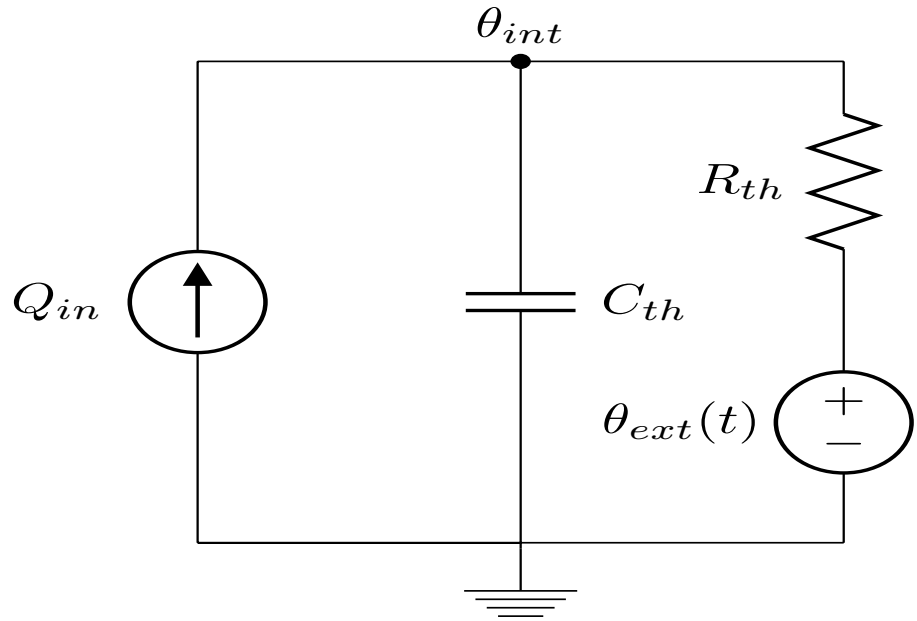

Fig. 3.3: The created thermal system model.

Generally, the two main materials in manufacture of every IC are silicon and plastic (i.e. for packaging). Consequently, determination of the IC's thermal conductivity and specific heat was accomplished by several examinations according to the values of these two parameters for the materials. At last, it should be stated that the IC's initial temperature parameter that is present in the respective equations is measured using a thermometer.

Based on analyzing the results of all presented models, it can be interpreted that the surrounding temperature of the device has the highest priority among all of the discussed parameters for predicting the matched filter output. The reason for this correlation is believed to be owing to the temperature role, which is an intrusion into the device's signal. In other words, there is a base behavior in the device's signal over time (i.e. either charging or discharging trend according to the circuit activities) and the temperature tries to change this behavior. On the other side, the device has a resistive manner in confrontation with this intrusion, but its strength is not sufficient. Due to the fact that the effects of noise or any other environmental interferences can be present in the actual data of the matched filter output and the device's surrounding temperature, it is clear that the trends of these two parameters should be considered for the tracking system development. In this regard,

a comparative analysis is run on the actual MFO and the predicted MFOs by Models 35, 36, 1, and 7, which is shown in Figure 3.4. The used data for this analysis are from the m5c2 card in the dataset 6.

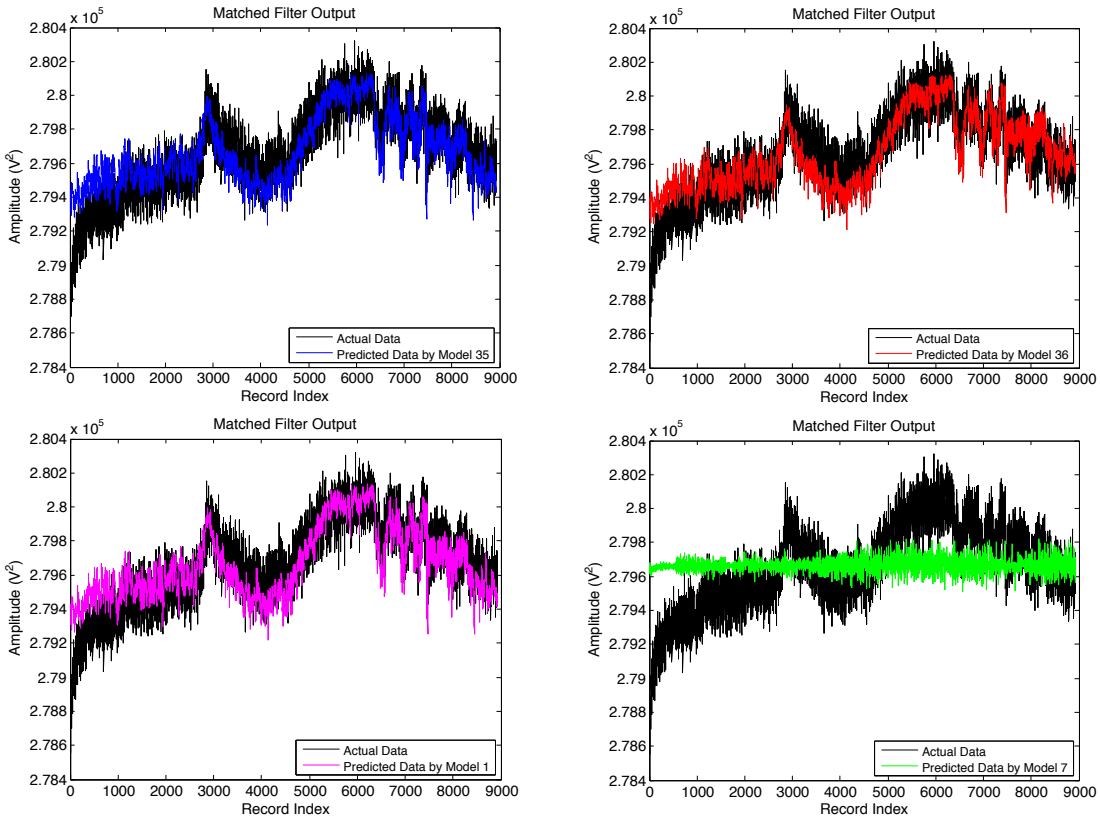

Fig. 3.4: A comparison between the actual MFO and four predicted MFOs.

Table 3.1: The results of basic models - (1).

Number	Model	Dataset(s)	R-Squared (%)			
			Minimum	Mean	Median	Maximum
1	MFO ~ Temperature	1	3.4274	15.3892	8.8275	38.984
		2	1.1636	6.62916	6.8874	10.587
		3	90.879	92.834	93.022	95.217
		4	87.102	91.2528	92.014	93.684
		5	0.0234	8.48116	10.109	18.141
		6	0.0579	25.3906	3.3027	65.954
		7	4.412	17.157	13.711	34.651
		8	8.9329	25.4824	13.018	43.33
		1 + 2	0.4533	3.35042	1.2408	9.9828
		1 + 2 + 3	92.574	94.4912	93.8	97.145
		1 + 2 + 5 + 6	13.704	36.5778	30.972	75.978
2	Normalized MFO ~ Temperature	1	0.0594	0.1544	0.0749	0.303
3	Euclidean Norm of Aligned Synch. Signals ~ Temperature	1	3.9106	16.3136	10.853	41.336
4	MFO ~ Euclidean Norm of Aligned Synch. Signals	1	95.434	97.064	96.364	99.054
5	Mean of Absolute Value(Aligned Synch. Signals) ~ Temperature	1	3.5305	15.9571	10.411	40.58
		2	1.3247	6.7344	7.3856	11.004
6	Mean of Absolute Value(MFO) ~ Temperature	1	3.5305	15.9571	10.411	40.58
		2	1.3247	6.7344	7.3856	11.004
7	MFO ~ IC's Supply Voltage	5	0.0103	2.6065	0.6453	7.5458
		6	0.1295	0.8734	0.4940	2.5094
		7	2.2333	9.0122	5.9355	18.549
		8	0.4211	4.22734	4.2131	8.9731
8	Moving Average(MFO) ~ Moving Average(Temperature)	1	10.418	44.6944	41.022	83.481
		2	12.084	38.7274	38.222	55.502
9	[Mean(MFO of Card 1);Mean(MFO of Card 2);…] ~ [Mean(IC's Voltage of Card 1);Mean(IC's Voltage of Card 2);…]	1 and 2	3.3112			
		1 + 2	4.8446			

Table 3.2: The results of basic models - (2).

Number	Model	Dataset(s)	R-Squared (%)			
			Minimum	Mean	Median	Maximum
10	MFO ~ Bus's Supply Voltage	5	0.0182	2.40126	1.7701	7.2353
		6	0.39588	3.7495	2.7953	9.6343
		7	1.4013	8.48874	7.6861	16.228
		8	0.09612	0.582342	0.1971	1.9846
11	MFO ~ Mean(Record's Noisy Part)	1	0.016715	1.30865	0.30126	5.6557
		2	~ 0	0.0274	0.03315	0.053
12	MFO ~ Standard Deviation(Record's Noisy Part)	1	~ 0	0.065	0.04541	0.15117
		2	~ 0	0.057113	0.03134	0.19821
13	MFO ~ Temperature * IC's Supply Voltage	5	0.2596	10.2745	11.083	18.749
		6	0.0644	25.3003	5.85	65.431
14	MFO ~ Temperature / IC's Supply Voltage	5	0.2797	10.4249	11.267	18.842
		6	0.05714	25.349	5.7639	65.541
15	Moving Average(MFO) ~ Moving Average(IC's Supply Voltage)	5 + 6	5.6187	58.1059	70.071	93.469
16	MFO ~ Derivation(Moving Average(Temperature))	1	0.12876	0.32914	0.36645	0.48856
		2	0.011492	0.069433	0.057447	0.12364
17	MFO ~ Moving Average(Temperature)	1	3.3137	15.993	10.128	39.907
		2	0.98628	5.30138	8.5805	11.382
18	Right Shift(MFO) ~ Left Shift(Temperature)	1	1.2923	9.8848	4.3121	32.118
		2	0.414	3.76786	3.4852	7.1716
19	Left Shift(MFO) ~ Right Shift(Temperature)	1	2.1177	11.9229	6.3057	33.751
		2	0.4575	5.38282	5.8108	9.0241
20	MFO(Now) ~ Temperature(Now) + MFO(Old)	7	4.45	19.5344	15.214	42.98
		8	8.451	25.1526	19.144	43.012
21	MFO ~ Moving Average(Temperature) + ... Derivation(Moving Average(Temperature))	1	3.3343	16.165	10.406	40.07
		2	1.0915	7.59322	8.5865	11.418

Table 3.3: The results of basic models - (3).

Number	Model	Dataset(s)	R-Squared (%) or Analysis Outcome			
			Minimum	Mean	Median	Maximum
22	MFO ~ Temperature + Euclidean Norm of Aligned Synch. Signals	1	95.502	97.0898	96.551	99.055
23	MFO ~ Temperature + IC's Supply Voltage	5	6.0535	13.3755	13.741	18.831
		6	0.1898	25.8041	5.8978	65.628
		5 + 6	47.142	74.4048	81.225	93.782
24	MFO ~ Temperature + Bus's Supply Voltage	5	2.2466	12.8571	15.147	18.801
		6	3.0415	27.5374	10.6	65.85
		5 + 6	47.106	68.6494	74.327	85.441
25	MFO ~ Temperature + IC's Supply Voltage + ... Mean(Record's Noisy Part) , Non-Robust Mode	5 + 6	53.368	76.9688	81.71	93.544
	MFO ~ Temperature + IC's Supply Voltage + ... Standard Deviation(Record's Noisy Part) , Non-Robust Mode	5 + 6	50.192	74.8496	81.309	93.534
	MFO ~ Temperature + IC's Supply Voltage + ... Mean(Record's Noisy Part) , Robust Mode	5 + 6	53.361	76.6564	81.592	92.351
	MFO ~ Temperature + IC's Supply Voltage + ... Standard Deviation(Record's Noisy Part) , Robust Mode	5 + 6	50.17	74.5388	81.188	92.342
26	MFO ~ Temperature (Distributions: Gamma, Inverse Gaussian (IG), Normal, and Poisson)	1	3.4267 (IG)	15.2382	8.8272	38.984 (Normal)
27	MFO ~ a * exp(b/Temperature)	1	3.1115	14.8535	8.762	37.776
		2	1.0231	6.25314	6.6943	10.232
28	Main Signal = MFO Mode: Training , Range 1	7	1.4432	7.91226	6.2235	15.0119
	Main Signal = MFO Mode: Testing , Outcome Range	8	3.6987	8.37136	5.2954	19.3301
29	Main Signal = MFO , Exogenous Input = Temperature Mode: Training , Range 1	7	4.5156	14.2828	15.0345	25.7814
	Main Signal = MFO , Exogenous Input = Temperature Mode: Training, Outcome Range	8	6.9882	16.0243	11.1678	26.6816
30	Main Signal = MFO , Exogenous Input = Temperature Mode: Training , Range 2	7	3.5157	13.5641	14.1118	25.1073
		8	6.1626	15.1022	10.8614	26.9627
31	Correlation(MFO,Temperature)	1	0.18513	0.36321	0.30262	0.62437
		2	0.10787	0.24616	0.26244	0.32537
32	Autocorrelation(Residuals = Actual MFO – Predicted MFO)	1	No deterministic and/or periodic pattern can be seen in the results of all of the Ethernet cards.			
		2				
33	Cross Correlation(MFO,Temperature)	1	For all of the Ethernet cards, maximum output of the function is achieved at a lag of zero.			
		2				

Table 3.4: The results of combined models - (1).

Number	Model	Dataset(s)	R-Squared (%)			
			Minimum	Mean	Median	Maximum
34	Spline(MFO) ~ Temperature Robust Mode = Bisquare Weights	1	32.361	47.418	45.375	72.156
		2	17.119	33.0804	33.848	42.555
		5	22.979	44.2766	46.595	64.093
		6	4.8476	54.4275	73.553	85.14
35	Spline(MFO) ~ Temperature Robust Mode = Least Absolute Residuals	1	72.952	91.0634	95.524	98.189
		2	89.919	94.001	93.705	97.542
		5	90.418	96.1212	97.124	98.252
		6	-1.8579	63.4162	72.19	98.999
36	MFO ~ Temperature + IC's Supply Voltage + Charging Trend Data	5	6.1389	24.7638	19.951	41.435
		6	52.003	70.962	68.762	95.019
37	MFO ~ Temperature + IC's Supply Voltage + Discharging Trend Data	5	26.166	35.7736	35.972	49.591
		6	53.497	70.5032	72.72	81.233
38	MFO ~ Temperature + Bus's Supply Voltage + Charging Trend Data	5	2.5571	24.0206	19.942	41.749
		6	52.086	70.9838	68.604	95.169
39	MFO ~ Temperature + Bus's Supply Voltage + Discharging Trend Data	5	15.175	30.5358	31.466	49.962
		6	52.371	69.4022	72.169	81.311
40	MFO ~ Temperature + IC's Supply Voltage + Fitted MFO (based on Charging Trend)	5	7.5232	18.2152	20.804	24.72
		6	0.56222	35.827	49.723	66.475
41	MFO ~ Temperature + IC's Supply Voltage + Fitted MFO (based on Discharging Trend)	5	11.022	26.3378	21.992	43.5
		6	47.583	70.4312	71.97	92.527
42	Moving Average(MFO) ~ Moving Average(Temperature) + ... Moving Average(Charging Trend Data)	7	24.039	41.9878	41.631	66.89
		8	39.807	59.3744	64.439	83.436
43	Moving Average(MFO) ~ Moving Average(Temperature) + ... Moving Average(Discharging Trend Data)	7	24.566	55.4722	57.896	83.199
		8	36.072	59.1124	64.391	83.057

Table 3.5: The results of combined models - (2).

Number	Model	Dataset(s)	R-Squared (%)			
			Minimum	Mean	Median	Maximum
44	Moving Average(MFO) ~ Moving Average(Temperature) + ... Moving Average(Charging Trend Data) + ... Moving Average(IC's Supply Voltage)	7	36.331	56.2328	64.824	71.472
		8	39.254	68.0928	76.556	86.196
45	Moving Average(MFO) ~ Moving Average(Temperature) + ... Moving Average(Discharging Trend Data) + ... Moving Average(IC's Supply Voltage)	7	43.055	61.9466	67.336	84.66
		8	39.193	61.2096	67.181	84.701
46	Analysis of Residuals – Version 1 Stage 1: Using Temperature and IC's Supply Voltage	5	6.0535	13.3755	13.741	18.831
		6	0.18977	25.8041	5.8978	65.628
	Analysis of Residuals – Version 1 Stage 2: Using Charging Trend Data	5	22.846	30.6766	28.24	43.656
		6	33.495	55.6848	52.621	77.981
47	Analysis of Residuals – Version 1 Stage 1: Using Temperature and IC's Supply Voltage	5	6.0535	13.3755	13.741	18.831
		6	0.18977	25.8041	5.8978	65.628
	Analysis of Residuals – Version 1 Stage 2: Using Discharging Trend Data	5	9.9943	25.0849	21.887	40.051
		6	27.85	63.4444	70.951	82.001
48	Analysis of Residuals – Version 2 Stage 1: Using Charging Trend Data	5	2.1532	6.90174	2.6891	17.378
		6	0.38889	11.88	4.1364	41.861
	Analysis of Residuals – Version 2 Stage 2: Using Temperature and IC's Supply Voltage	5	7.3632	18.0546	20.693	24.277
		6	0.56209	34.8793	48.781	66.314
49	Analysis of Residuals – Version 2 Stage 1: Using Discharging Trend Data	5	1.1326	13.8854	5.3353	37.365
		6	25.989	53.4564	41.514	92.522
	Analysis of Residuals – Version 2 Stage 2: Using Temperature and IC's Supply Voltage	5	11.015	26.214	21.877	43.222
		6	44.939	67.2844	66.782	92.527
50	MFO ~ Device's Internal Temperature	7	4.4623	17.1825	13.754	34.713
		8	8.958	25.5718	19.633	43.565

Chapter 4

Security Evaluation of PLI Systems

4.1 Overview

Generation of a forged signal using an arbitrary waveform generator (AWG) – an electronic equipment that produces arbitrarily shaped signals – is one of the most effective techniques in attacking the PLI systems [3]. Evaluating the defending strength and weaknesses of a PLI system and, finding the required AWGs for defeating it can be accomplished using three different strategies: (a) constructing the models of all of the available AWGs in the market and attacking the PLI system by employing them; (b) accomplishing comparison between multiple PLI systems, and finding the one that can be crushed in confrontation with the most expensive AWG; and (c) developing and solving a cost minimization problem for the purpose of finding the most cost-effective AWG (i.e. the AWG that has the smallest run-time). The configuration and performance parameters (for example, sampling rate and resolution) of an AWG determine the characteristics and behavior of the generated forged signal.

4.2 Architecture of Attack

According to the general strategy of defeating a PLI system, an attacker tries to reproduce those portions of a device's signal that are used for identification as accurate as possible. This process can be implemented in two different forms: (a) Feature Replay, in which the specific features of the trustworthy signals that are used for identification by the PLI system are sent to it repeatedly; and (b) Signal Replay, in which the attacker acquires a sampled version of the device's signal and tries to generate highly similar versions of those portions of it that are used for identification (i.e. synchronization portion in here) using an AWG. Figure 4.1 shows an architecture that leverages the second form in order to attack

the targeted PLI system.

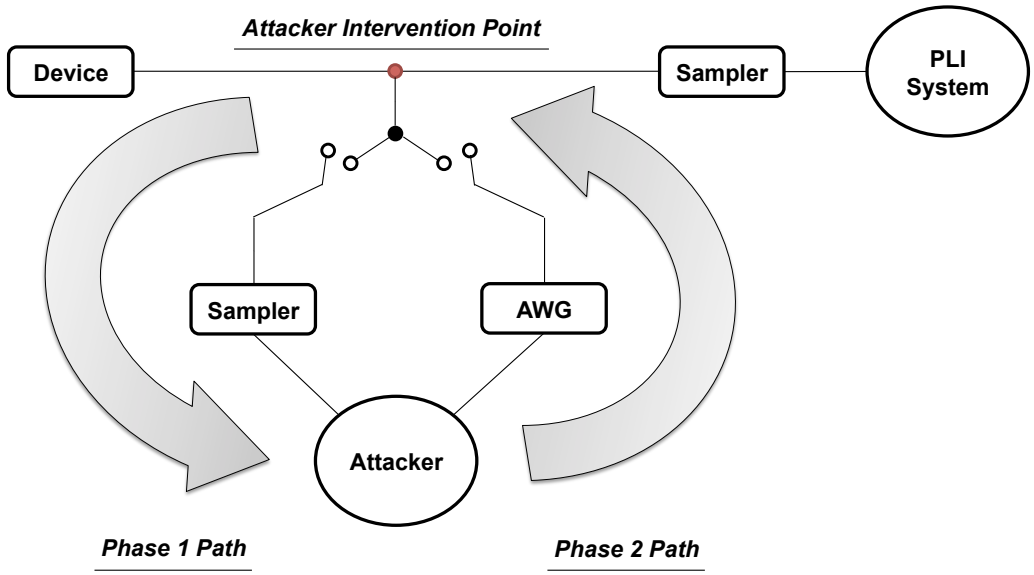

Fig. 4.1: The architecture of attack.

This attack's architecture consists of two main phases. Phase 1: the device's signal is captured and sampled for both the attacker and PLI system using the same samplers (i.e. with the same resolution and sampling rate). In this way, the attacker and PLI system will have the same sampled version of the signal for processing. Additionally, having a sampler for the attacker with higher sampling rate and resolution compare to either the PLI system's sampler or the AWG's built-in sampler is not advantageous. This is due to the fact that the attacker's signal will be down-sampled again for the identification process and it will not provide any new information for the AWG function. Also, it is useful in the applied implementation of this architecture because of requiring less number of oscilloscopes.

Phase 2: the sampled version of the device's signal is transmitted to the AWG to create a forged signal that can be accepted by the PLI system. The attacker intervention point in this architecture acts as a leaker of the trustworthy information in the first phase, and as an exporter of the false information in the second phase. Meanwhile, transmission of data between the architecture' components is accomplished through a loss-less channel. This is the ideal case for the attacker since modeling the channel effects is not needed.

4.3 Arbitrary Waveform Generator (AWG) Configuration

Generally, the structure of an arbitrary waveform generator (AWG) consists of three main components that are source memory, digital-to-analog converter (DAC), and low-pass filter (LPF). According to the AWG function, the source memory renders the binary values of the sampled version of a waveform (known as Codes) to the DAC in order to generate a stepped analog waveform with certain characteristics, which is then smoothed by the low-pass filter. For simplification, evaluating the AWG's output quality is limited to the DAC performance, and other components are considered to be in their ideal conditions.

At high frequencies, the dynamic non-linear behavior (i.e. the time-variant and non-linear characteristics) of the DAC's output is dominant, and consequently only the dynamic parameters of this component are considered for performance analysis. The most important parameters that can be selected in this regard are Settling Time, Resolution, Total Harmonic Distortion (THD), and Signal-to-Noise Ratio (SNR). Finally, the resemblance of the generated forged signal to the device's signal, which is an indication of its attacking strength, is checked by sending it to the PLI system for extracting its features and comparing them with the reference feature set.

4.3.1 AWG Performance Parameters

The most important parameters that can be selected for performance analysis of an AWG are discussed in the following [3]:

Settling Time: It is the required amount of time for a system's output to reach its steady state. This parameter is used in AWG's built-in sampler(s) and low-pass filter (a.k.a. reconstruction filter) of an arbitrary waveform generator. It specifies the maximum allowable sampling rate value. The sampling rate should be less than or equal to the inverse of the settling time. For an ideal case, the settling time should be very low that results in getting a pulse waveform nearly. In this way, there is no need to focus on the transient part of the DAC's output signal. Usually, the sampled version of a signal becomes indistinguishable based on the design of a sampler. This behavior is caused by the Aliasing

phenomenon [57], which can be prevented by leveraging an anti-aliasing filter. This filter provides a trade-off between the aliasing effect and signal bandwidth. In fact, the signal is band-limited by the filter in order to attenuate this effect. The low-pass filter component of the AWG runs this function on the DAC's output.

Resolution: This parameter is defined as the number of discrete values that a sampler can produce over the range of values of an analog signal. Due to the differences between the AWG's built-in sampler(s) and the identical samplers of the attacker and PLI system, the data points of the generated forged signal will not be exactly equivalent to the discrete voltage levels of the initial sampled signal. This problem is solved by using a discretizer, which rounds each data point of the test signal to the nearest voltage level of the desired signal.

Total Harmonic Distortion: In general, distortion is defined as the unwanted alterations in the original shape and/or other characteristics of a signal or waveform. Total harmonic distortion (THD) parameter is a measure for the amount of existing harmonic distortion in a signal. This parameter is defined as the sum of the powers of all harmonic components relative to the power of the fundamental frequency. The amount of existing distortion in the DAC's output depends on its architecture as well as its non-ideal constituent parts.

Signal-to-Noise Ratio: This parameter is a measure for comparing the level of a desired signal to the level of background noise (i.e. the existing noise in the actual signal) and is defined as the ratio of the signal power to the noise power. Due to various possibilities for modeling noise, a basic model named additive white Gaussian noise (AWGN) can be utilized for the performance analysis. The SNR parameter in this case is described as the ratio of the distorted signal power to the AWGN signal power. So, a noise signal having the same length as the distorted signal is created according to the specified SNR value and is added to it in order to obtain a signal that is both distorted and noisy.

4.4 Simulation Framework for Security Evaluation

A simulation framework regarding the generation of a forged signal and its identity assessment by a PLI system is presented in here. This simulation framework consists of two major parts: one is of them is for emulation of the AWG's function and the other one is for accomplishment of the PLI system role. Regarding the first part, a sampled version of a trustworthy device's analog signal is acquired in the beginning. The achieved discrete signal is directly sent to the discretizer if its sampler has the same sampling rate as the AWG's sampler. Otherwise, it is down-sampled before sending it for discretizing. In this stage of processing the signal, it is discretized according to the AWG's resolution. In order to complete this part of the simulation framework, the distortion model (based on the found value for the coefficient M), the up-sampling function (if the signal was down-sampled previously because of the AWG's sampler), the reconstruction filter, and the noise model are applied to the signal in order.

There are three reasons behind having this order: (a) if the signal was down-sampled previously, it needs to be up-sampled for having the same number of data points as the original sampled version of the device's signal; (b) if the distortion model is not applied to the down-sampled signal, then the high frequency distortion components are introduced to the signal that are not desirable; and (c) it is a requisite to apply the noise model to the smoothed signal; otherwise, its major effects would be filtered by the reconstruction filter. Once the forged signal is constructed, it is sent to the PLI system part of the simulation framework. In this part, the signal is discretized according to the resolution of PLI system's sampler before it is dispatched to feature extraction and comparison with the reference signal.

4.5 Results and Discussion

The practical implementation of the leveraged PLI system security evaluation is presented in this section. It is accomplished according to the simulation framework with the difference that the distortion and noise injection parts are ignored. In this implementation, a Tektronix AFG 3252 with the sampling rate of up to 2.0 Giga-Samples/Second and resolution of 14 bits is used as the AWG in order to generate the forged versions of the records of 26 Ethernet cards that are acquired via a Tektronix DPO 7254C Digital Phosphor Oscilloscope at 40.0 Giga-Samples/Second rate in an experimental setup similar to Setup 1, which was explained in chapter 2.

In this experiment, the records of the devices are detected based on a positive slope-based threshold and each has the length of 4 million data points. Also, the information of the used Ethernet cards that are from the D-Link (i.e. model 4), Genica (i.e. model 5), and Netronix (i.e. model 6) manufacturers are presented in Tables 2.2 and 4.1. Once the forged version of an original record is generated, it is observed by the oscilloscope at 40.0 Giga-Samples/Second rate and has the length of 500 thousand data points. Due to the fact that an original record has a different length than its corresponding forged one, they are aligned before the comparison analysis is accomplished on them. Meanwhile, even with ignoring the noise injection part of the simulation framework, a small amount of environmental and equipment-related noise is still present in the generated forged record.

Table 4.1: The information of Ethernet cards - (2).

Identifier	MAC Address	Serial
m4c1	00:40:05:34:a0:31	B229237077076
m4c2	00:40:05:36:01:15	B229237077139
m4c3	00:40:05:36:01:19	B229237077140
m4c4	00:40:05:35:75:40	B229237077075
m4c5	00:40:05:34:a0:30	B229237077074
m4c6	00:40:05:36:01:1a	B229237077133
m5c6	00:00:e8:12:61:47	DB0211105364
m5c8	00:00:e8:12:c4:a0	DB0211105317
m5c9	00:00:e8:12:61:09	DB0211105326
m5c10	00:00:e8:12:32:4a	DB0211105404
m5c11	00:00:e8:12:65:3e	DB0211105394
m6c1	00:08:54:0c:37:5f	122901133CF05938
m6c2	00:08:54:0c:37:13	122901133CF05997
m6c3	00:08:54:0c:37:4c	122901133CF05948
m6c4	00:08:54:0c:37:42	122901133CF05949
m6c5	00:08:54:0c:37:10	122901133CF06000
m6c6	00:08:54:0c:37:55	122901133CF05939
m6c7	00:08:54:0c:37:54	122901133CF05940
m6c8	00:08:54:0c:37:0f	122901133CF05999
m6c9	00:08:54:0c:4c:bf	122901133CF06650
m6c10	00:08:54:0c:37:4d	122901133CF05947

Among all of the collected records (10,000) for each device, 25 of them are selected (i.e. records 1001-1025) to be forged by the AFG and observed via the oscilloscope. The desired resolution and sampling rate for the forged record are determined based on the AFG configuration. In this regard, the maximum and minimum voltages of the AFG are set to 1.982 (V) and -1.968 (V) respectively. Also, two different sampling rates, 1.0 Giga-Samples/Second and 2.0 Giga-Samples/Second are considered in designing the forged records for ensuring the PLI system performance in confronting this attack. After the generation of the forged records for all of the Ethernet cards, they are aligned with their corresponding original ones. Figure 4.2 shows one period of the synchronization signals of the correct and forged records (i.e. 23th records) for the m5c8 card in the dataset of 1.0 GS/s rate. As it can be seen from the figure, the aligned signals look alike and the difference between them at each data point is relatively small.

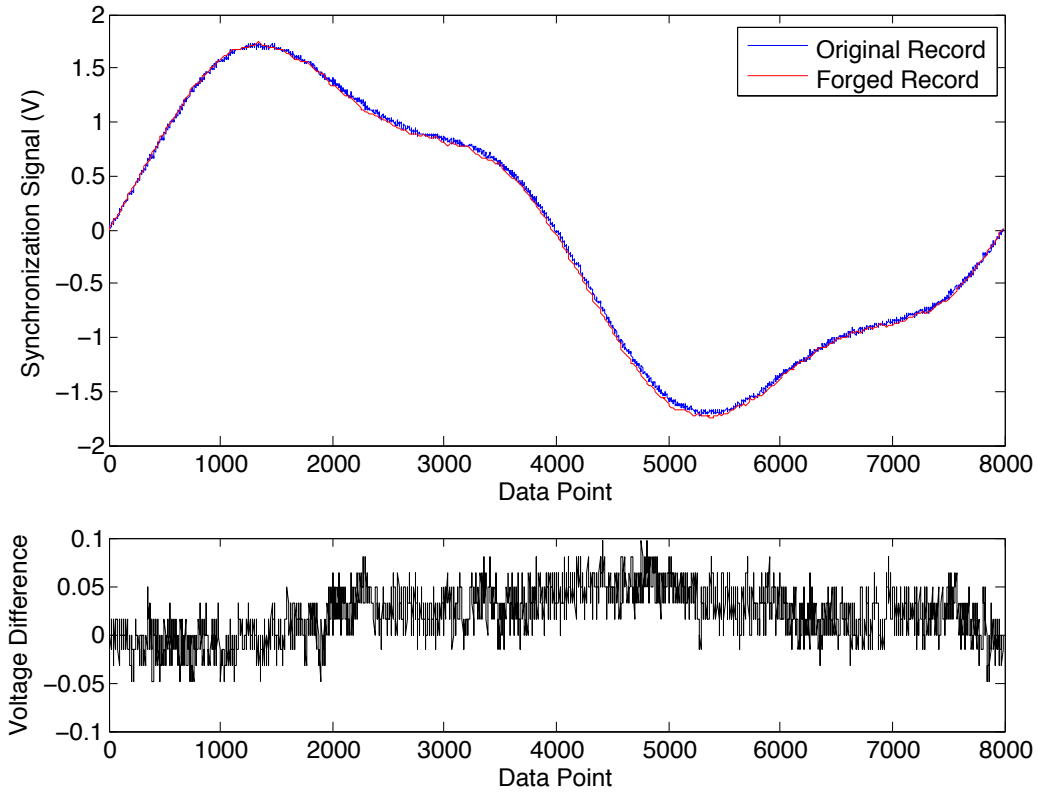

Fig. 4.2: One period of the correct and forged synchronization signals and their differences.

Next, the matched filter is applied to them in order to measure their differences. The left and right plots in Figure 4.3 show the matched filter outputs of the correct records and forged records for the m5c8 card. As it can be observed, there are noticeable differences between the actual and forged matched filter outputs that can be detected by the PLI system.

Experimentally, it has been realized that a test signal is rejected by the PLI system if the difference between its matched filter output and the reference signal's matched filter output is greater than 1000. Also, the dispersion of the forged matched filter outputs is relatively high. In fact, even if the mean of the forged matched filter outputs was close to the desired value, they should lie within a confidence interval to be unrecognizable.

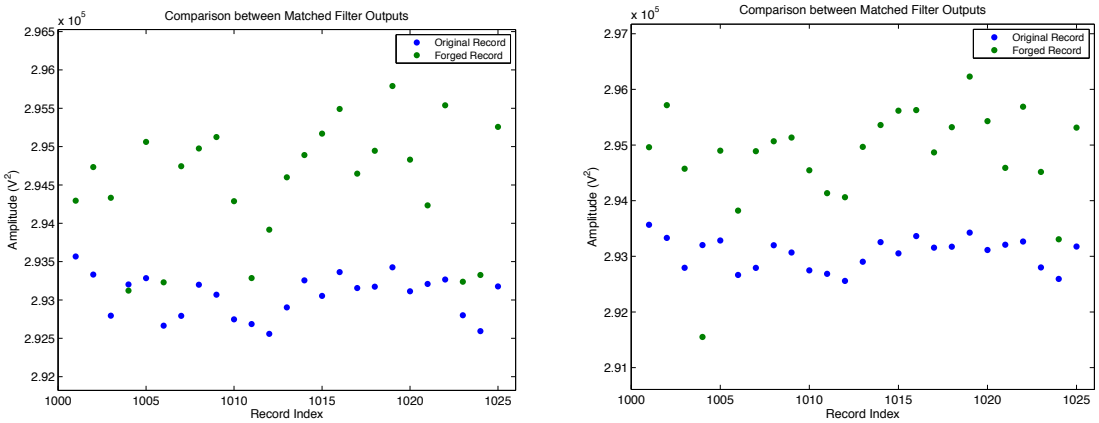

Fig. 4.3: The generated forged records at 1.0 GS/s (left) and 2.0 GS/s (right) rates.

The calculated values for the specificity parameter in accomplishing overall identification on the concatenation of the correct records and the generated forged records at 1.0 GS/s and 2.0 GS/s rates that are equal to 1.2% and 0.9%, show that the PLI system is not consistently defeatable using the employed AFG. The results of the PLI system security evaluation can be seen in Tables 4.2 and 4.3.

Table 4.2: The PLI system performance results - Generation of records at 1.0 GS/s rate.

Tested Card	Mean of MFO Difference	Standard Deviation of MFO Difference
m4c1	2633.9328	243.5335
m4c2	2726.6279	258.9514
m4c3	2674.2843	285.7394
m4c4	2561.8614	239.8448
m4c5	2624.5832	286.6853
m4c6	2687.3948	369.6344
m5c1	2697.2938	374.1369
m5c2	2597.4423	405.5606
m5c3	2419.3011	406.8911
m5c5	2822.1364	371.5194
m5c6	2610.8769	381.1607
m5c7	2826.8154	388.2999
m5c8	1473.4116	630.917
m5c9	2887.1808	337.133
m5c10	2369.8088	453.0534
m5c11	1871.7038	375.2898
m6c1	3571.1074	351.2073
m6c2	3512.3917	360.4098
m6c3	3630.3118	331.6449
m6c4	3384.2011	265.0739
m6c5	3377.6708	295.8297
m6c6	3267.8174	269.5025
m6c7	3255.9447	241.17
m6c8	3331.2028	301.6552
m6c9	3532.2908	324.5976
m6c10	3450.3552	370.7902

Table 4.3: The PLI system performance results - Generation of records at 2.0 GS/s rate.

Tested Card	Mean of MFO Difference	Standard Deviation of MFO Difference
m4c1	2660.0017	279.4235
m4c2	2703.3737	308.4298
m4c3	2674.9187	370.7383
m4c4	2668.6305	243.3249
m4c5	2754.092	355.6048
m4c6	2814.6057	395.445
m5c1	2870.246	412.34
m5c2	2752.9736	362.2898
m5c3	2601.093	446.8713
m5c5	2928.349	467.2262
m5c6	2677.4696	468.7418
m5c7	2992.5637	486.4892
m5c8	1884.0954	474.6846
m5c9	2904.4833	433.7018
m5c10	2490.3316	395.3304
m5c11	2066.8977	294.4031
m6c1	3452.8653	423.1126
m6c2	3399.8502	403.6955
m6c3	3455.4232	404.0636
m6c4	3313.2883	377.0952
m6c5	3249.2712	330.8913
m6c6	3297.9493	368.935
m6c7	3146.379	299.4883
m6c8	3230.928	335.7953
m6c9	3384.926	413.9747
m6c10	3446.3713	474.6577

Chapter 5

Conclusion

This research project embodies three main parts that are: (i) testing networking devices according to their analog signals and understanding their behavior in different conditions and over time; (ii) developing a tracking system for predicting the future behavior of the devices; and (iii) attacking the leveraged testing method in the first part and evaluating its security strength accordingly. In the first part, the signals of five different Ethernet cards along with their associated environmental and circuit-related data (i.e. the surrounding temperature, the bus's supply voltage, and the IC's supply voltage) in four different conditions are acquired for their behavioral analysis. Next, a PLI system is leveraged in order to examine the possibility of identifying the devices in each condition. According to the achieved results, a relationship can be observed between the device's signal and its surrounding temperature. Also, the temperature should not exceed a certain high threshold value; otherwise, the signal will seem too different from the reference signal.

In the second part, the development of a tracking system capable of predicting the future behavior of the devices is studied. In this regard, diverse models based on multiple data preparation concepts and data modeling techniques are designed. The models use the previously collected environmental and circuit-related data in order to estimate the future signals of the devices. Based on analyzing the achieved results in this part, it can be understood that the surrounding temperature of the device is the best option in predicting its signal. The reason of this relationship is interpreted to be due to the temperature role as an intruder into the circuit activities.

The security evaluation of the leveraged PLI system is investigated in the last part. Hereof, the attack is accomplished by generating the forged versions of the original records of 26 different Ethernet cards and sending them to the system. The creation of forged

records is done by an arbitrary waveform generator, wherein its configuration determines the characteristics and alikeness of these forged records to the original records. The results of this part demonstrate that both the mean and dispersion of the forged matched filter outputs are greater than those of the original matched filter outputs. Therefore, the PLI system is able to defend itself against this designed attack.

References

[1] R. M. Gerdes, M. Mina, S. F. Russell, and T. E. Daniels, "Physical-layer identification of wired ethernet devices," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 4, pp. 1339–1353, 2012.

[2] S. J. Pan and Q. Yang, "A survey on transfer learning," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 22, no. 10, pp. 1345–1359, 2010.

[3] R. M. Gerdes, M. Mina, and T. E. Daniels, "Towards a framework for evaluating the security of physical-layer identification systems," in *Security and Privacy in Communication Networks*. Springer, 2013, pp. 328–348.

[4] R. V. Jones, *Most secret war*. Penguin UK, 2009.

[5] K. I. Talbot, P. R. Duley, and M. H. Hyatt, "Specific emitter identification and verification," *Technology Review*, p. 113, 2003.

[6] 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.

[7] Y. Payal, "Identification of push-to-talk transmitters using wavelets," Ph.D. dissertation, Monterey, California. Naval Postgraduate School, 1995.

[8] C. Zhao, L. Huang, L. Hu, and Y. Yao, "Transient fingerprint feature extraction for wlan cards based on polynomial fitting," in *Computer Science & Education (ICCSE), 2011 6th International Conference on*. IEEE, 2011, pp. 1099–1102.

[9] S. U. Rehman, K. Sowerby, and C. Coghill, "Rf fingerprint extraction from the energy envelope of an instantaneous transient signal," in *Communications Theory Workshop (AusCTW), 2012 Australian*. IEEE, 2012, pp. 90–95.

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

[11] J. Erbskorn, "Detection of intrusions at layer one: The ieee 802.3 normal link pulse as a means of host-to-network authentication a preliminary performance analysis and survey of environmental effects," *Masters, Iowa State Univ., Ames*, 2009.

[12] R. Gerdes, "Physical layer identification: methodology, security, and origin of variation," *Ph.D. dissertation, Iowa State Univ., Ames*, 2011.

[13] A. Mukherjee, S. A. Fakoorian, J. Huang, A. L. Swindlehurst *et al.*, "Principles of physical layer security in multiuser wireless networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 3, pp. 1550–1573, 2014.

[14] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *Network, IEEE*, vol. 29, no. 1, pp. 42–48, 2015.

[15] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *Communications, IEEE Transactions on*, vol. 62, no. 6, pp. 2006–2021, 2014.

[16] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 2, pp. 247–258, 2014.

[17] D.-B. Ha, N. G. Nguyen, D.-D. Tran, and T.-H. Nguyen, "Physical layer security in uwb communication systems with transmit antenna selection," in *Computing, Management and Telecommunications (ComManTel), 2014 International Conference on.* IEEE, 2014, pp. 280–285.

[18] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 6, pp. 3442–3451, 2014.

[19] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "A new model for physical layer security in cellular networks," in *Communications (ICC), 2014 IEEE International Conference on.* IEEE, 2014, pp. 2147–2152.

[20] F. L. Walls, "Environmental sensitivities of quartz crystal oscillators," in *Proc. 22nd Ann. Precise Time and Time Interval (PTTI) Applications and Planning Meeting.* DTIC Document, 1990, pp. 465–477.

[21] T. Wu, K. Mayaram, and U.-K. Moon, "An on-chip calibration technique for reducing supply voltage sensitivity in ring oscillators," *Solid-State Circuits, IEEE Journal of*, vol. 42, no. 4, pp. 775–783, 2007.

[22] C. Huo, T. Xia, and H. Li, "A 400mhz current starved ring oscillator with temperature and supply voltage insensitivity," in *Solid-State and Integrated Circuit Technology (ICSICT), 2014 12th IEEE International Conference on.* IEEE, 2014, pp. 1–3.

[23] J. Yuan and E. Kritchanchai, "Power amplifier resilient design for process, voltage, and temperature variations," *Microelectronics Reliability*, vol. 53, no. 6, pp. 856–860, 2013.

[24] D. Gómez, M. Sroka, and J. L. G. Jiménez, "Process and temperature compensation for rf low-noise amplifiers and mixers," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 57, no. 6, pp. 1204–1211, 2010.

[25] S. Chen and J.-S. Yuan, "Adaptive gate bias for power amplifier temperature compensation," *Device and Materials Reliability, IEEE Transactions on*, vol. 11, no. 3, pp. 442–449, 2011.

[26] H. K. Subramaniyan, E. Klumperink, B. Nauta, S. Venkatesh, A. Kiaei *et al.*, "Rf transconductor linearization technique robust to process, voltage and temperature variations," in *Solid-State Circuits Conference (A-SSCC), 2014 IEEE Asian*. IEEE, 2014, pp. 333–336.

[27] P. Obmann, J. Fuhrmann, J. Moreira, H. Pretl, and A. Springer, "A circuit technique to compensate pvt variations in a 28 nm cmos cascode power amplifier," in *Microwave Conference (GeMiC), 2015 German*. IEEE, 2015, pp. 131–134.

[28] Y. Yang and N. K. Jha, "Finprin: Finfet logic circuit analysis and optimization under pvt variations," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 22, no. 12, pp. 2462–2475, 2014.

[29] E. I. Vatajelu, R. Rodriguez-Montanes, M. Indaco, P. Prinetto, and J. Figueras, "Sttmram cell reliability evaluation under process, voltage and temperature (pvt) variations," in *Design & Technology of Integrated Systems in Nanoscale Era (DTIS), 2015 10th International Conference on*. IEEE, 2015, pp. 1–6.

[30] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, p. 6, 2012.

[31] 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.

[32] M. Edman and B. Yener, "Active attacks against modulation-based radiometric identification," *RPI Department of Computer Science Technical Report*, pp. 09–02, 2009.

[33] D. Ma, C. Qian, W. Li, J. Han, and J. Zhao, "Geneprint: Generic and accurate physical-layer identification for uhf rfid tags," in *Network Protocols (ICNP), 2013 21st IEEE International Conference on*. IEEE, 2013, pp. 1–10.

[34] G. J. Hahn and W. Q. Meeker, *Statistical intervals: a guide for practitioners*. John Wiley & Sons, 2011, vol. 328.

[35] Rc time constant. [Online]. Available: https://en.wikipedia.org/wiki/RC_time_constant

[36] Norm (mathematics). [Online]. Available: https://en.wikipedia.org/wiki/Norm_(mathematics)

[37] Mean absolute value. [Online]. Available: https://www.delsys.com/KnowledgeCenter/NetHelp/default.htm?turl=HTMLDocuments%2Fmeanabsolutevalue.htm

[38] Autoregressive model. [Online]. Available: https://en.wikipedia.org/wiki/Autoregressive_model

[39] Moving average filter. [Online]. Available: http://www.mathworks.com/help/econ/filtering.html

[40] Unit vector. [Online]. Available: https://en.wikipedia.org/wiki/Unit_vector

[41] Standard deviation. [Online]. Available: https://en.wikipedia.org/wiki/Standard_deviation

[42] Correlation coefficient. [Online]. Available: http://www.stat.wmich.edu/s216/book/node122.html

[43] Cross-correlation. [Online]. Available: https://en.wikipedia.org/wiki/Cross-correlation

[44] Autocorrelation. [Online]. Available: https://en.wikipedia.org/wiki/Autocorrelation

[45] Simple linear regression. [Online]. Available: https://en.wikipedia.org/wiki/Simple_linear_regression

[46] Multiple linear regression. [Online]. Available: https://www.mathworks.com/help/stats/what-is-linear-regression.html

[47] Nonlinear regression. [Online]. Available: https://www.mathworks.com/help/stats/nonlinear-regression-1.html

[48] Robust regression. [Online]. Available: https://en.wikipedia.org/wiki/Robust_regression

[49] Robust regression reduce outlier effects. [Online]. Available: http://www.mathworks.com/help/stats/robust-regression-reduce-outlier-effects.html

[50] Generalized linear models. [Online]. Available: https://www.mathworks.com/help/stats/generalized-linear-regression.html

[51] Smoothing splines. [Online]. Available: http://www.mathworks.com/help/curvefit/smoothing-splines.html

[52] Autoregressivemoving-average model. [Online]. Available: https://en.wikipedia.org/wiki/Autoregressivemoving-average_model

[53] Model diagnostics. [Online]. Available: https://onlinecourses.science.psu.edu/stat504/node/161

[54] Analysis of residuals. [Online]. Available: http://www.unige.ch/ses/sococ/cl//stat/action/analyse_residuals0.html?

[55] Thermal systems background. [Online]. Available: http://lpsa.swarthmore.edu/Systems/Thermal/SysThermalIntro.html

[56] Mathematical models of thermal systems. [Online]. Available: http://lpsa.swarthmore.edu/Systems/Thermal/SysThermalModel.html

[57] Aliasing. [Online]. Available: https://en.wikipedia.org/wiki/Aliasing