NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INNOVATIVE ELECTROMAGNETIC PROTECTION TECHNIQUES AGAINST ADVANCED JAMMING WAVEFORM THREATS

by

Alexandra Feltes

June 2021

Thesis Advisor: Ric Romero
Second Reader: David C. Jenn

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
INNOVATIVE ELECTROMAGNETIC PROTECTION TECHNIQUES AGAINST ADVANCED JAMMING WAVEFORM THREATS

5. FUNDING NUMBERS

6. AUTHOR(S) Alexandra Feltes

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

In this thesis, we develop electromagnetic protection (EP) receiver techniques to mitigate the false alarm probability and detection effects generated by transmit waveform shaped noise jammers (TWS-NJs) and deceptive coherent jammers (CJs). Unlike traditional wideband NJ (WB-NJ) and narrowband NJ (NB-NJ) that produce spectral densities almost uniformly distributed across their respective bandwidths, a TWS-NJ assumes apriori knowledge of a signal spectral shape, thereby utilizing the waveform dominant bands in generating jammer noise. While noise jammers produce a significant number of false targets, CJs manipulate and retransmit the received signal to generate a few false targets in the victim receiver. For illustration in this thesis, we utilize the basic rectangular and Hamming pulses as transmit waveforms to evaluate the detection performance effects of the TWS-NJ and CJ waveforms. The bandwidths of the TWS-NJs are parameterized to reflect the effect of practical narrowband constraints. The performance effect of various jammers, including the TWS eigenjammer, on detection performance is also investigated. To mitigate the TWS-NJs, we develop an adaptive matched filter and evaluate performance improvement. To mitigate the CJ, we develop a non-coherent EP matched filter and evaluate false detection rate improvement.

14. SUBJECT TERMS	**15. NUMBER OF PAGES**
electronic warfare, electronic protection, EP, electronic attack, jamming, coherent jammer, CJ, matched illumination, noise jammer, wideband NJ, WB-NJ, transmit waveform shaped noise jammers, TWS-NJ	65
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

INNOVATIVE ELECTROMAGNETIC PROTECTION TECHNIQUES AGAINST ADVANCED JAMMING WAVEFORM THREATS

Alexandra Feltes
Lieutenant, United States Navy
BS, University of Akron, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Ric Romero
Advisor

David C. Jenn
Second Reader

Douglas J. Fouts
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this thesis, we develop electromagnetic protection (EP) receiver techniques to mitigate the false alarm probability and detection effects generated by transmit waveform shaped noise jammers (TWS-NJs) and deceptive coherent jammers (CJs). Unlike traditional wideband NJ (WB-NJ) and narrowband NJ (NB-NJ) that produce spectral densities almost uniformly distributed across their respective bandwidths, a TWS-NJ assumes apriori knowledge of a signal spectral shape, thereby utilizing the waveform dominant bands in generating jammer noise. While noise jammers produce a significant number of false targets, CJs manipulate and retransmit the received signal to generate a few false targets in the victim receiver. For illustration in this thesis, we utilize the basic rectangular and Hamming pulses as transmit waveforms to evaluate the detection performance effects of the TWS-NJ and CJ waveforms. The bandwidths of the TWS-NJs are parameterized to reflect the effect of practical narrowband constraints. The performance effect of various jammers, including the TWS eigenjammer, on detection performance is also investigated. To mitigate the TWS-NJs, we develop an adaptive matched filter and evaluate performance improvement. To mitigate the CJ, we develop a non-coherent EP matched filter and evaluate false detection rate improvement.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

AF	ambiguity function
AWG	arbitrary waveform generator
B_c	bandwidth constraint
B_{nn}	null-to-null bandwidth
CJ	coherent jammer
CST	Computer Simulation Technology
dBsm	decibel square meters
DRFM	digital radio frequency memory
EA	electromagnetic attack
EIG-NJ	eigen-noise jammer
EMOE	electromagnetic operational environment
EMS	electromagnetic spectrum
EP	electromagnetic protection
ES	electromagnetic support
ESD	energy spectral density
EW	electromagnetic warfare
FDR	false detection rate
JEMSO	joint electromagnetic spectrum operations
JNR	jammer-to-noise ratio

JSR	jammer-to-signal ratio
KB-NJ	knowledge-based noise jammers
LO	local oscillator
MC	Monte Carlo
MWS	Microwave Studio
NB	narrowband
NB-NJ	narrowband noise jammer
NC	non-coherent
NC-NJ	narrowband constraint noise jammer
NC-NJ-H	narrowband constraint noise jammer Hamming
NJ	noise jammer
NP	Neyman-Pearson
P_d	probability of detection
P_{fa}	probability of false alarm
P_{far}	receiver false alarm probability
PEC	perfect electrical conductor
pdf	probability distribution function
PSD	power spectral density
RAM	radar absorbent material
RF	radio frequency
SATCOM	satellite communication
SIR	signal-to-interference ratio

SJR signal-to-jammer ratio

SNR signal-to-noise ratio

TW transmit waveform

TWS transmit waveform shaped

TWS-NJ transmit waveform shaped noise jammer

TWS-NJ-H TWS-NJ-Hamming

TWS-NJ-R TWS-NJ-Rectangle

TWTR-MF transmit waveform target response matched filter

WB wideband

WBJ wideband jammer

WB-NJ wideband noise jammer

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

1.1 Electromagnetic Warfare Background

The desire to control the electromagnetic spectrum (EMS) originated over 150 years ago during the Civil War when the Union and Confederacy sent long-distance communications via telegraph wire. Commanders received critical orders significantly faster than was previously possible. However, soldiers soon began wiretapping and intercepting messages by removing insulation and splicing their line into the adversary wire. These events first demonstrated the importance of maintaining and protecting one's use of the EMS and laid the groundwork for electromagnetic warfare (EW) [1].

EW has matured into a principal determining factor for operational success. Modern day conflicts such as World War II, Desert Storm, and the global war on terrorism solidified the importance of effective maneuvering within the EMS as weapon superiority alone could not dictate military success. Armed forces throughout the world depend upon EMS actions, which are vital to most military activities. We often forget that while the electromagnetic spectrum is a vast resource, it does not provide an infinite supply of bandwidth. Military and civilian technological advances have created a complicated electromagnetic operational environment (EMOE) as nearly every technology we use, from keyless entries and wireless cameras to SATCOM-enabled systems and precision-guided missiles, rely on the use of the EMS to function. The growing demand for EMS resources forces users to develop technologies that can operate in this crowded environment.

Modern warfare has shaped the EMOE into a very crowded and congested environment, as shown in Figure 1.1 [2]. Forces are severely disadvantaged without the ability to navigate through the electromagnetic spectrum. For this reason, EW is a war-fighting capability on par with the more traditional capabilities associated with war-fighting in the air, land, and maritime domains.

As highly sophisticated technology becomes more affordable, competition to control the EMOE becomes even more challenging. Military and commercial entities increasingly rely

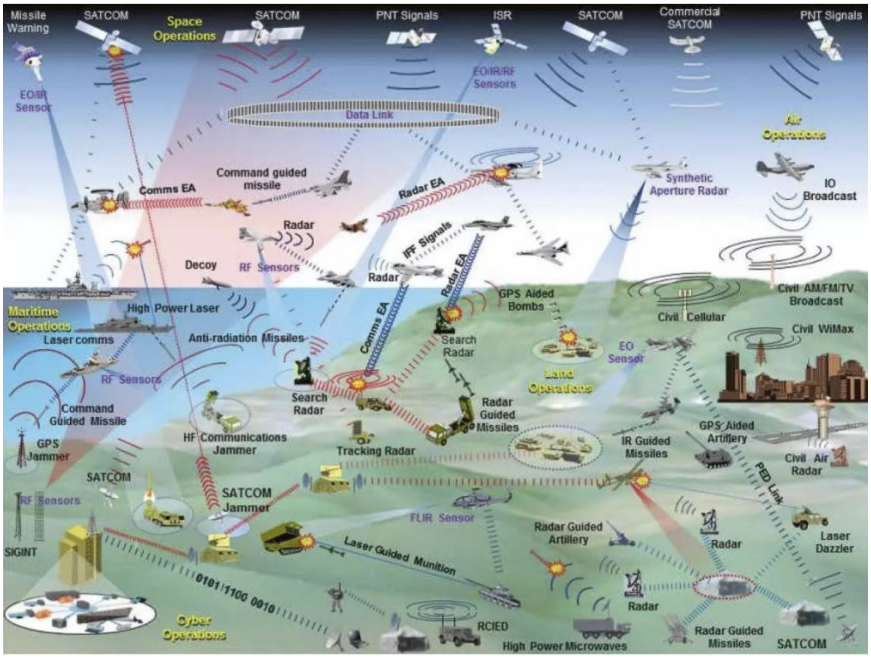


Figure 1.1. Electromagnetic warfare in the current electromagnetic operational environment. Source: [2].

on advanced technologies for navigation, information processing, intelligence gathering, and network connectivity. Such activities require use of the EMS which creates both opportunities for and vulnerabilities to EW techniques. Therefore, forces need to protect system capabilities while simultaneously developing methods to disrupt or prevent these threats. This creates a constantly evolving challenge to develop systems that can operate in emission restricted and/or congested environments.

Joint electromagnetic spectrum operations (JEMSO) involve "military actions undertaken by a joint force to exploit, attack, protect, and manage the EMOE" [3], which contains all potential and actual electromagnetic (EM) radiation within the EMS, as depicted in Figure 1.2 [3]. JEMSO actions integrate EW through various mission-related areas with the purpose of managing and achieving superiority within the EMS maneuver space. EW actions fall into three main categories: electromagnetic protection (EP), electromagnetic attack (EA), and electromagnetic support (ES) [3].

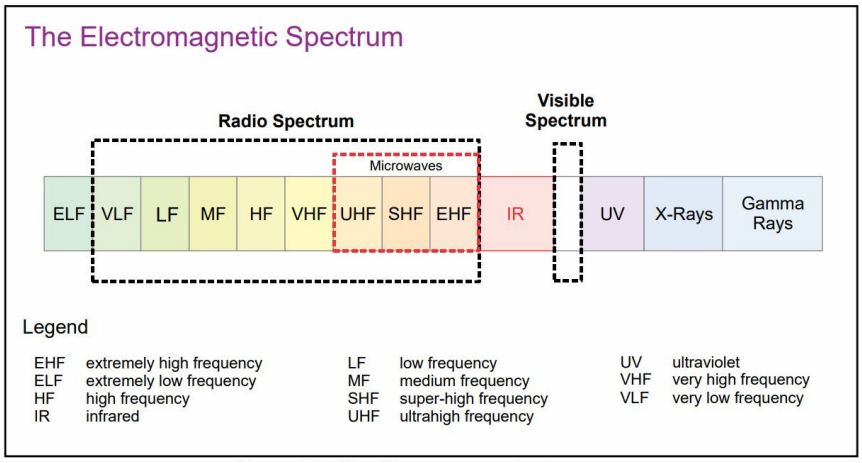


Figure 1.2. Electromagnetic spectrum overview. Source: [3].

EA uses directed or EM energy to degrade or disrupt the use of the EM spectrum. EA can be either offensive or defensive and targets either equipment, personnel, or facilities. EA actions include jamming, anti-radiation missiles, or expendables such as flares or chaff. Noise and deceptive jamming are two of the most common EA actions. Noise jamming uses EM energy to overwhelm a receiver and conceal targets, usually radiating over a wide range of frequencies. Deceptive jamming, such as jamming employed by coherent jammers (CJ), sends a few false radar returns that the receiver mistakenly identifies as real targets.

EP involves actions taken to protect friendly capabilities and personnel from adversarial EA effects. Examples include hardening systems against jamming, controlling emissions, and utilizing decoy measures such as Digital Radio Frequency Memory (DRFM) and chaff. Of note, some actions are considered both EA and EP depending on the situation. Defensive EA denies adversary use of the EMS for functions related to targeting and weapons guidance while EP protects against EA effects. The third pillar of EW is ES and involves searching, tracking, and identifying sources of EM radiation with the purpose of immediate threat recognition and avoidance [3]. This thesis focuses on EA, specifically noise and deceptive jammers, and EP techniques to counter the effects of those jammers.

1.2 Thesis Objective

In this thesis, we develop EP receiver techniques to mitigate the false alarm and detection effects generated by transmit waveform shaped noise jammers (TWS-NJ) and deceptive

coherent jammers. The TWS family of noise jammers assumes a priori knowledge of the signal spectral shape, thereby utilizing the dominant bands of the waveform in generating jammer noise. The bandwidths of the TWS-NJ are parameterized to reflect the effect of practical narrowband constraints. While noise jammers produce a significant number of false targets, CJs manipulate and retransmit the received signal to generate a few false targets in the victim receiver thereby deceiving the radar into deciding that the false targets are true. We utilize the basic rectangular and Hamming pulses as transmit waveforms to evaluate the detection performance effects of the TWS-NJ and CJ waveforms. Generalized coherent and non-coherent EP matched filters are developed for the TWS-NJs and CJs to evaluate performance improvement.

1.3 Thesis Organization

This thesis is organized as follows. In Chapter 2, we present our overall system model and discuss general radar detection theory as it relates to combating noise jammers. The development of the TWS-NJs are discussed, to include how each of the bandwidth parameterized noise jammers is generated. Additionally, we detail the adaptive matched filter techniques used to mitigate these various jammers. In Chapter 3, the TWS jammers and EP technique effectiveness are evaluated by calculating the radar detection probability and false alarm probability in the receiver. In Chapter 4, we introduce the challenge coherent jammers present and examine EP mitigation via non-coherent detection for an extended target assumption, which utilizes target impulse responses generated from computer-simulated radar cross sections of two fighter aircraft. In Chapter 5, the CJ and non-coherent EP effectiveness are evaluated utilizing impulse responses to measure the false detection rate and detection probabilities. In Chapter 6, we summarize our conclusions and discuss possible future work.

CHAPTER 2:
Development of TWS Noise Jammers and Adaptive Matched Filter Technique

2.1 Overview of Transmit Waveform Shaped Jammer Family

EA techniques against radar systems have significantly evolved since first used 150 years ago. Unsophisticated barrage jammers inundate a receiver over a wide range of frequencies to overwhelm the receiver by producing excessive false detections, which effectively blinds the system and renders it incapable of detecting true targets. However, early 20^{th} century EA methods do not produce the same desired effect against modern technologies. While high power wideband (WB) and narrowband (NB) jammers can still be effective, more complex EA methods are required to defeat the increasingly advanced receivers.

Numerous texts and papers discuss conventional WB and NB noise jammers as white Gaussian noise with a uniform energy spectral density (ESD), including [4]–[7], among others. When employed against the mainlobe of the desired signal, narrowband noise jammers (NJ) effectively obfuscate the signal portion containing the largest amount of energy, which affects the receiver detection probability. With the advent of low-cost configurable arbitrary waveform generators (AWG), it is mentioned in [8] that these knowledge-based noise jammers (KB-NJ) can easily be shaped using the spectra of the transmit waveforms and proposed mitigation with the use of cognitive radar. For the first part of this thesis, we investigate the detection performance effects of TWS jammers.

TWS-NJs use the captured transmit waveform to produce a Guassian noise signal that targets the transmit waveform largest energy band in the frequency response which potentially renders the receiver matched filter incapable of distinguishing between the desired signal and the jammer. We also investigate the performance effect of varying the bandwidth (B_c) of the jammer. This accomplishes two things: a) it incorporates practical bandwidth constraints of low-cost jammers and b) it simulates a jammer that is able to place noise energy in the dominant band/s of the waveform as suggested by the KB jammer design in

an effort to increase jamming effects. KB-NJs may be formed from any transmit waveform spectrum. To demonstrate this notion, we will utilize two basic waveforms: the rectangular pulse and Hamming pulse, from which we develop a TWS-NJ-R (rect) and the TWS-NJ-H (Hamming) whose ESDs are matched to the would-be victim transmit waveform spectrum. These methods have been proven successful with various waveforms; the rect and Hamming waveforms are chosen purely for illustrative examples. To reflect practical bandwidth limitations with the use of TWS-NJ, the bandwidth constraint will be parameterized in relation to the mainlobe width of the rect and Hamming waveform spectra.

We also want to generate a noise jammer with the narrowest bandwidth constraint possible. But note that as the bandwidth constraint becomes increasingly small, the jammer approaches the trivial case of becoming a delta function in frequency, i.e., tone jammer with random phase due to the noise nature of the jammer. So, the question becomes: how do we form a very narrow meaningful NJ? Utilizing eigenwaveforms as optimum waveforms for extended targets has been well documented. While we cannot cite all relevant literature, we refer to the works in [8]–[14]. The eigenwaveform maximizes the transmit waveform-target return energy where the eigenvalue derived from the waveform-target autocorrelation function amplifies the return signal [14]. Eigenwaveforms are known to be narrowband waveforms. To that end, we can now form a very meaningful narrowband noise jammer which we refer to as an eigen-noise jammer (EIG-NJ). The EIG-NJ spectrum is based off the transmit waveform eigenfunction associated with the largest eigenvalue. Unlike the bandwidth constrained TWS-NJ, the EIG-NJ may concentrate the energy in the mainlobe, but it does not necessarily ignore the entirety of the transmit signal spectrum.

One of our objectives in this thesis is to develop EP techniques against these newly formed yet effective TWS-NJs. We assume a priori knowledge of the NJ spectra via ES such that we can form a generalized matched filter that effectively whitens the narrowband jammer. Unfortunately, the matched filter whitening action comes at the expense of effectively reducing the transmit waveform mainlobe, which is due to the knowledge-based nature of the TWS-NJ. The EP matched filter incorporates the noise jammer power spectral density (PSD) in the total interference pdf via its covariance matrix [15]. Accounting for the jammer covariance function results in colored Gaussian noise that is whitened by the EP match filter thereby reducing the TWS-NJ in the mainlobe. However, as mentioned, the waveform mainlobe is reduced as well. In other words, if the required P_{fa} is to be kept, then the threshold has to be adjusted.

2.2 System Model

The currently crowded EM environment challenges our ability to detect desired target signals. Natural and manmade objects along with thermal noise, environmental clutter, and EA techniques interfere with the ability of a receiver to identify incoming signals, particularly when the signal-to-noise (SNR) ratio is low. As such, detection theory has become an integral part in all signal processing designs.

Traditional matched filters assume a point target such that the return signal and radar waveform are nearly identical [9]. Chapters 2 and 3 invoke the point target assumption. As such, the received signal contains the echo, a realization of the jammer, and noise. Normalized sampling is assumed such that $T_s = 1$. The received signal, $\mathbf{y}$, is modeled by

$$\mathbf{y} = \mathbf{s} + \mathbf{j} + \mathbf{w} \tag{2.1}$$

where $\mathbf{s}$ is the desired target signal, $\mathbf{j}$ is the jamming signal directed at the receiver, and $\mathbf{w}$ is zero-mean, complex white Gaussian noise (CWGN) with variance σ^2. Again, for illustration, $\mathbf{s}$ is merely the rect or Hamming vector. The jammer vector, $\mathbf{j}$, decreases the signal-to-interference ratio (SIR) and degrades receiver performance thereby increasing the receiver false alarm probability and affecting the detection probability.

2.3 Development of the Noise Jammer Models

In this section, three KB-NJs are discussed for which EP techniques are to be developed. They are as follows: TWS-NJ, narrowband constraint noise jammer (NC-NJ), and EIG-NJ.

2.3.1 Transmit Waveform Shaped Noise Jammer

TWS-NJ is a KB jammer that uses the transmit waveform of the radar or system it wants to victimize. By capturing the victim-to-be waveform, the jammer can easily produce a noise jammer vector based off the victim spectrum. Another form of KB jammer is the coherent jammer. It is important to note that TWS-NJ is not the same as CJ. The purpose of an EA CJ is to create a few specific false targets in the victim receiver. In other words, the CJ acts when it actually hears a waveform is transmitted. Although it can also respond to an actual transmission, TWS-NJ does not have to wait for the victim transmission to send a noise

vector in an effort to produce a significant number of false targets to effectively 'blind' the victim radar.

To form the TWS-NJ, let $\mathbf{s}$ be the captured waveform. From the waveform convolution matrix $\mathbf{H_s}$ [10], the autocorrelation is given by

$$\mathbf{R} = \mathbf{H_s^\dagger H_s} \tag{2.2}$$

where † is the Hermitian operator. Note that $\mathbf{R}$ is the target response autocorrelation function where the diagonal contains the same energy as $\mathbf{s}$ [10]. The autocorrelation may be used to generate realizations of the noise jammer vector tailored against any transmit waveform $\mathbf{s}$. For an illustrative example, we now look at the rect waveform.

Figure 2.1(a) depicts the energy spectrum of the rect waveform and Figure 2.1(b) depicts spectra of 30 different realizations of NB jammer directed at the rect pulse. Note that TWS is inherently a wideband jammer (WBJ) which does not ignore any portion of the victim's spectrum but definitely concentrates most of its energy in the mainlobe of the victim waveform.

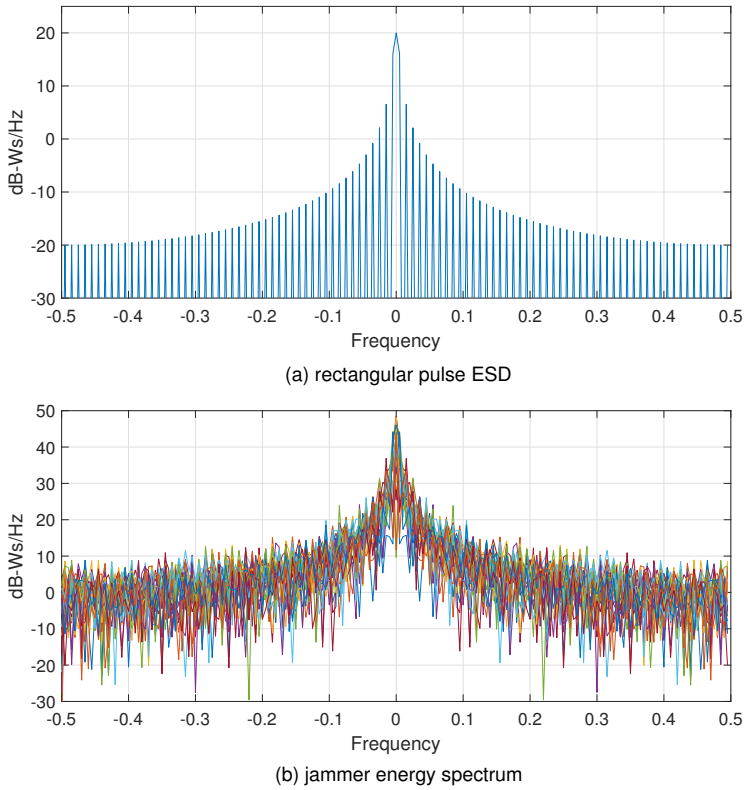


Figure 2.1. Transmit waveform ESD and 30 corresponding jammer realizations of the TWS-NJ-R with a 4 W jammer power.

2.3.2 Narrowband Constrained Noise Jammer (NC-NJ)

Practical low-cost noise jammers have bandwidth limitations. To demonstrate how a narrowband jammer can easily be formed from the spectrum of a transmit signal, we choose three narrowband constraint B_c values for illustration. A way for these KB bandwidth constrained jammers to exploit TWS methods is to concentrate the jammer power in the signal frequency response where the largest aggregate energy will be while meeting the bandwidth constraint. For the Hamming and rect pulses, these constraints will clearly capture part or all of the central mainlobe. For a transmit waveform with an arbitrary shape and spectrum, an actual algorithm is needed to ensure that the bandwidth constraint is placed at the band with the largest energy. While this is trivial in the case of Hamming and rectangular pulses,

it is not trivial in the general case of any arbitrary waveform. Thus, in this work, we develop an algorithm similar to what is described in [8].

Using the captured transmit waveform, we define a meaningful bandwidth constraint B_c in relation to the defined bandwidth of the transmit signal. For the rect and Hamming pulses, the null-to-null bandwidth (B_{nn}) is a good choice. Given a chosen bandwidth constraint, the frequency band containing the largest energy is found by producing running average totals throughout the transmit signal entire bandwidth. These energy bands are then used to develop the correlation matrix that will form the noise signal where a spectral shape is used to generate the noise jammer PSD.

For illustration in this thesis, we choose three bandwidth constraints and use a Hamming window to generate the NC-NJ spectrum. For $B_c = 2.5B_{nn}$, the jammer places the constraint (i.e., filter cutoff frequencies) beyond the mainlobe and first sidelobe of the waveform spectrum. The constraint $B_c = B_{nn}$ obstructs the entirety of the mainlobe, and $B_c = 0.5B_{nn}$ obstructs a frequency range contained within the mainlobe.

For labeling convention, the jammer occupying 50% of the mainlobe will be labeled as NC-NJ-H0.5. It follows that jammers with the other two bandwidth constraints will take on the appendices 1.0 and 2.5. Figure 2.2(a) depicts the energy spectrum of the Hamming pulse and Figures 2.2(b) - 2.2(d) depict spectra of five different realizations of narrowband constraint jammer directed at the Hamming pulse for three different bandwidth constraints.

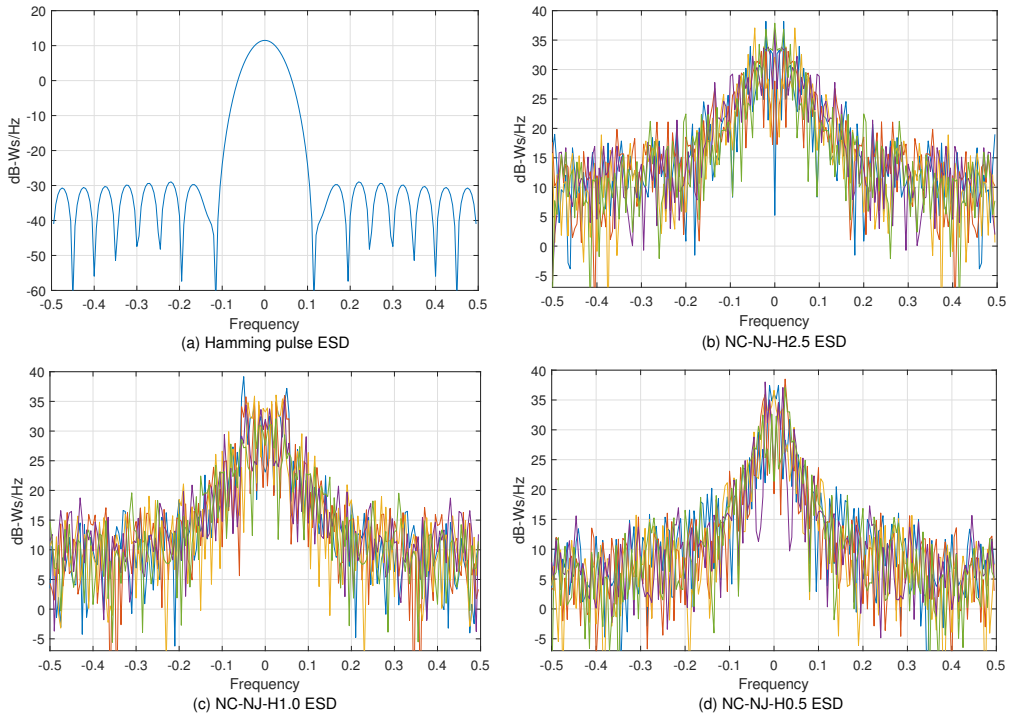


Figure 2.2. Transmit waveform ESD and five corresponding jammer realizations each with a 4 W jammer power.

2.3.3 Eigen-Noise Jammer

Let **s** be the complex-valued transmit waveform of length N whose autocorrelation matrix, **R**, is shown in (2.2). We find the eigenvector corresponding to the largest eigenvalue given by

$$\mathbf{R}\mathbf{q}_{max} = \lambda_{max}\mathbf{q}_{max} \tag{2.3}$$

where λ_{max} is the maximum eigenvalue of **R** and $\mathbf{q}_{max}$ is the eigenvector corresponding to λ_{max}. Using the eigenvector spectrum, realizations of the noise jammer can easily be produced. Exploiting the target signal characteristics, the EIG-NJ can significantly reduce SIR at the victim receiver, thereby affecting its detection probability, even for marginal jammer-to-noise ratio (JNR) values. Figure 2.3(a) depicts the energy spectrum of the eigen-waveform and Figure 2.3(b) depicts spectra of 20 different realizations of the eigenjammer directed at the receiver expecting a Hamming transmit waveform.

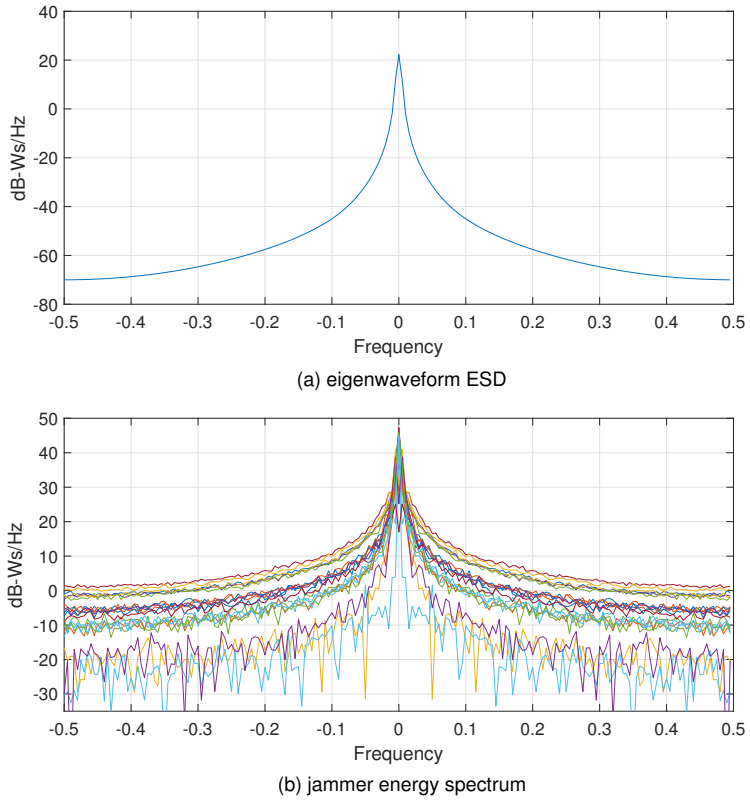


Figure 2.3. Transmit waveform ESD and 20 corresponding jammer realizations with a 4 W jammer power.

2.4 Effect of Jammers and EP Mitigation

2.4.1 Effect of Jammers on Receiver Performance

The simulations performed in this section use the Neyman-Pearson (NP) Theorem approach to signal detection. Two hypotheses exist for the received signal $\mathbf{y}$ as depicted in Equation (2.1). For a receiver unaware of the jammer, H_0 refers to when the target is absent and $\mathbf{y}$ consists of noise only. H_1 refers to when the target is present and $\mathbf{y}$ consists of the received

transmit signal and added noise:

$$\begin{aligned} H_0 &: \mathbf{y} = \mathbf{w} \\ H_1 &: \mathbf{y} = \mathbf{s} + \mathbf{w} \end{aligned} \tag{2.4}$$

Utilizing the likelihood ratio test [16],

$$L = \frac{p(\mathbf{y}; H_1)}{p(\mathbf{y}; H_0)} > \tilde{\gamma} \tag{2.5}$$

H_1 is decided if the ratio is greater than a threshold $\tilde{\gamma}$. P_{fa} refers to the probability that the radar decides a target is present when, in fact, the target is absent. P_d refers to the probability that the radar correctly detects target presence. If the jammer is not present, the traditional detection probability is given by [16]

$$P_d = Q\left(\frac{\gamma - E_s}{\sqrt{\sigma^2 E_s/2}}\right) \tag{2.6}$$

where $Q(\cdot)$ is the Q-function and E_s is the received energy of the transmit waveform. Equation (2.6) dictates the theoretical P_d when only the signal and noise are present under H_1, as depicted in Equation (2.4). The traditional matched filter threshold is given by

$$\gamma = \sqrt{E_s \sigma^2/2} Q^{-1}(P_{fa}) \tag{2.7}$$

where $Q^{-1}(\cdot)$ is the inverse Q-function and σ^2 is the noise variance. From (2.7), notice that the threshold does not account for a jammer. When a jammer is present, the received signal contains both the noise and jammer energy, potentially impacting receiver detection performance given a high enough jammer-to-signal ratio (JSR). Equation (2.7) will be used as a baseline to evaluate the effect of these jammers on the detection performance of the receiver when both signal **s** and jammer **j** are present. The effect of jammers on receiver detection performance will be discussed in more detail in the next section.

2.4.2 Electromagnetic Protection with Adaptive Matched Filters

Estimating the noise or interference covariance matrix to generate a whitening matched filter is a well-known technique in radar detection. If we are to produce an EP receiver

matched filter, the presence of a noise jammer necessitates adjusting that covariance matrix to account for the total noise, which is given by

$$\mathbf{C} = \mathbf{R_j} + \sigma^2\mathbf{I} \tag{2.8}$$

where $\mathbf{R_j}$ is the respective jammer autocorrelation and $\mathbf{I}$ is a N by N identity matrix. The jammer and noise power are contained along the diagonal of $\mathbf{C}$. It also necessitates adjustment to Equation (2.6) where $\mathbf{j}$ will be added to both H_1 and H_0. If the same P_{fa} is desired by the receiver, then adjusting Equations (2.6) and (2.7) creates a modified detection probability and threshold for the matched filter as given by [16]

$$P_d = Q\left(\frac{\gamma' - \mathbf{s}^\dagger\mathbf{C^{-1}s}}{\sqrt{\mathbf{s}^\dagger\mathbf{C^{-1}s}/2}}\right) \tag{2.9}$$

and

$$\gamma' = \sqrt{\mathbf{s}^\dagger\mathbf{C^{-1}s}/2}Q^{-1}(P_{fa}). \tag{2.10}$$

The output test statistic of the adaptive matched filter is given by

$$T(\mathbf{y}) = Re(\mathbf{s}^\dagger\mathbf{C^{-1}y}) \tag{2.11}$$

where Re is the real part of a complex-valued output that is compared to γ' for usual detection.

CHAPTER 3:
Performance Evaluation of the TWS Family Jammers and Adaptive Matched Filter

3.1 Performance Evaluation Method

To evaluate performance results, we generate complex-valued rect and Hamming transmit waveforms and perform 10,000 Monte Carlo trials per SNR to evaluate the effect of various jammer realizations have on detection probability and receiver false alarm probability. The desired P_{fa} is set to 1×10^{-3} with the noise variance set to unity. The desired P_{fa} is derived from the traditional matched filter when the receiver does not expect the jammer interference. We measure the theoretical detection probability via the adaptive matched filter derived in (2.9) for the EP matched filter.

3.2 Performance Results

Figure 3.1 presents the detection performance results for the TWS and WB noise jammer realizations where the theoretical P_d (blue) indicates when the jammer is not present. When only the reflected return signal and noise are expected, the effect of the jammer decreases the detection probability of the matched filter at high SNR as no EP is implemented. Detection performance decreases when signal-to-jammer ratio (SJR) is lowered given a fixed probability of false alarm (P_{fa}) [9]. Interestingly, the percentage of detection is increased in low SNR since the jammer effectively increases noise power such that the threshold in (2.5) is increasingly exceeded.

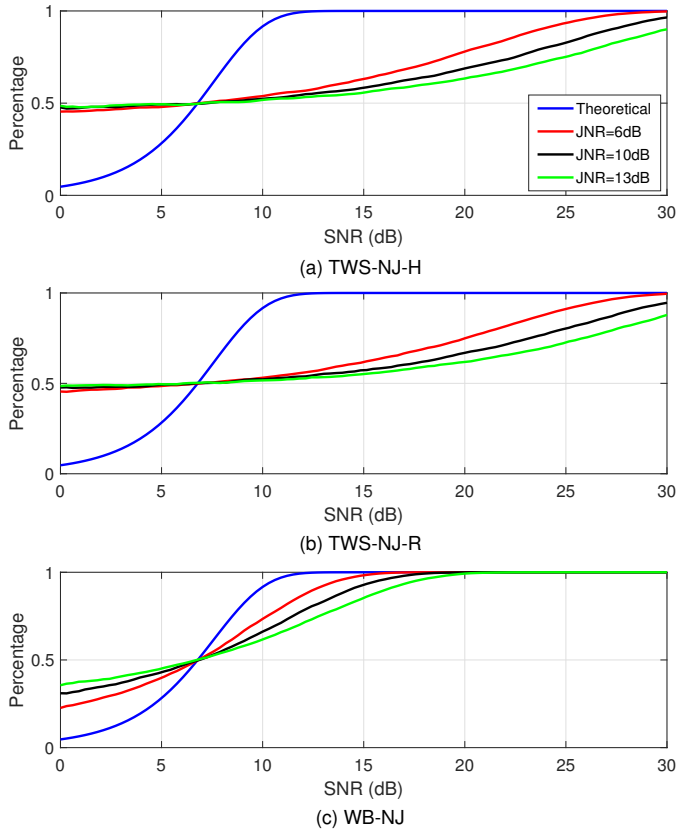


Figure 3.1. P_d comparison at 6dB, 10dB, and 13dB JNR with no EP implemented. (a) TWS-NJ-H, (b) TWS-NJ-R, (c) traditional WB-NJ.

Figures 3.1(a) and 3.1(b) illustrate how effective the TWS jammers are when no EP is implemented. In high SNR, the P_d with an actual target present is actually reduced significantly for the three JNRs investigated (6, 10, and 13 dB). Using the transmit signal ESD to shape the jammer spectrum yields jammer realizations with a strong correlation to the expected target signal. Wideband jammers evenly distribute energy across the whole frequency band resulting in a weaker correlation to the transmit waveform. The detection curves using WB-NJ confirm WB-NJs are inferior jammers compared to TWS-NJs. The detection curves using the NC-NJs are shown in Figure 3.2.

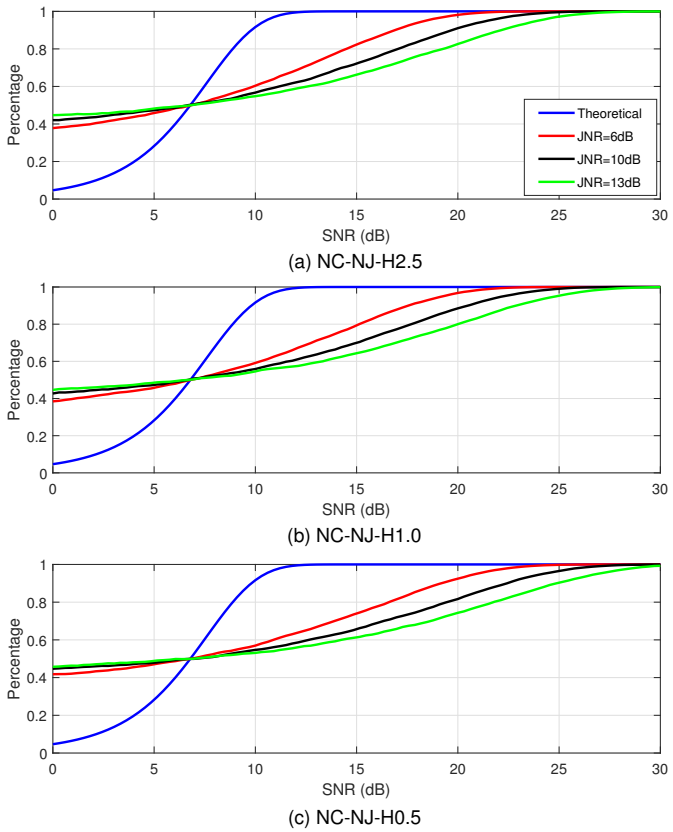


Figure 3.2. P_d comparison at 6dB, 10dB, and 13dB JNR with no EP implemented. (a) NC-NJ-H2.5, (b) NC-NJ-H1.0, (c) NC-NJ-H0.5.

From Figures 3.1 and 3.2, we observe that the TWS-NJ-H and TWS-NJ-R have the most significant negative effect on detection percentage, most likely because they are formed using the whole waveform spectra. The NC-NJ-H0.5 yields the highest negative effect among the NC-NJs, followed by the NC-NJ-H1.0 and NC-NJ-H2.5, respectively. Of course, increasing JNR further reduces detection percentage. Focusing the jammer power to target the largest energy band of the signal successfully obfuscates the transmit waveform more so than a traditional WB-NJ. While the traditional WB-NJ slightly degrades detection percentage, shaping the jammer ESD from the transmit waveform ESD clearly produces more effective noise jammers.

When it comes to transmit waveform shaped NB-NJs only, it is noted that the narrower

constraint B_c, the worse the effect of the jammer on P_d, which is a very interesting result and somewhat counter-intuitive once the constraint is within the mainlobe. This prompts us to compare Monte Carlo detection results of the narrowband EIG-NJ to the two most effective jammers thus far: NC-NJ-H0.5 and TWS-NJ-H. These results are depicted in Figure 3.3. Surprisingly, the eigenjammer outperforms both noise jammers, degrading the victim's detection probability with the worse effect for all measured JNR. And, like most jammers, it increases (false) detection percentage at low SNR. Exploiting the eigenwaveform characteristics produces a superior noise jammer which significantly reduces P_d at high SNR, even for low JNR.

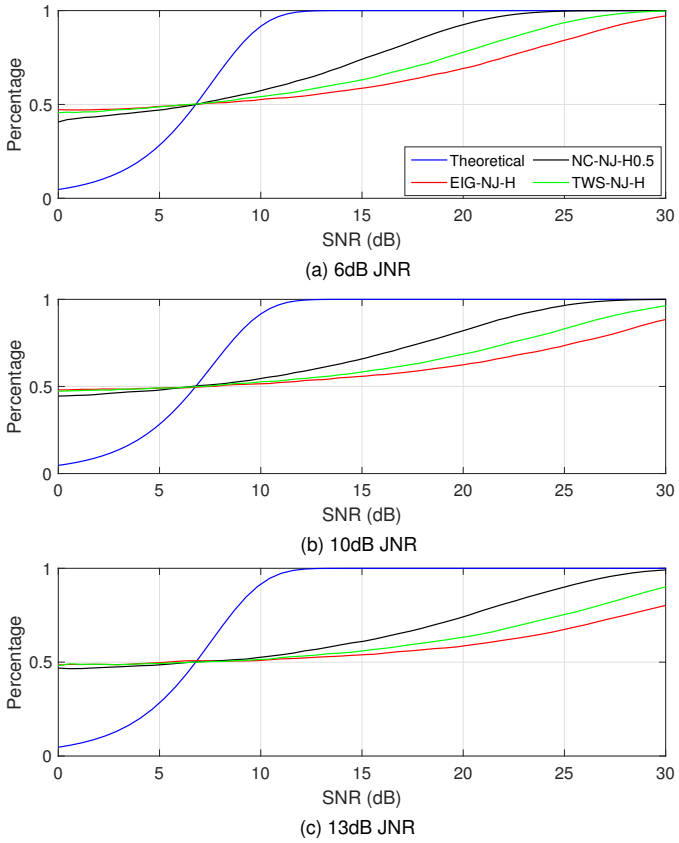


Figure 3.3. P_d comparison at 6dB, 10dB, and 13dB JNR with no EP implemented. (a) EIG-NJ-H, (b) NC-NJ-H0.5, (c) TWS-NJ-H.

In Figure 3.4, we compare the receiver false alarm probability (P_{far}) with varying JNR for all jammers to ascertain the effect on P_{fa}. The threshold is set for an expected noise

variance of unity and received transmit waveform energy value of 13 W/Hz. Increasing JNR leads to a higher P_{far}, with P_{far} increasing as the correlation between noise jammer and transmit waveform spectrum increases. WB-NJ is the least effective jammer, yielding the lowest effect on P_{far} while the EIG-NJ yields the highest P_{far}. Table I further demonstrates these results via the numerical P_{far} representation. The columns represent jammer type and the average receiver false alarm probability at a 6 dB JNR with no mitigation techniques implemented. These results concur with the aforementioned figures. EIG-NJs outperform TWS-NJs, NC-NJs, and the traditional WB-NJ in terms of both the victim's detection probability and receiver false alarm probability. Of note, all noise jammers shaped by the transmit waveform spectrum result in approximately the same P_{far} when JNR is way too high. This occurs around JNR = 30 dB when, again, defining a threshold for an expected E_s of 13 W/Hz and noise variance of unity.

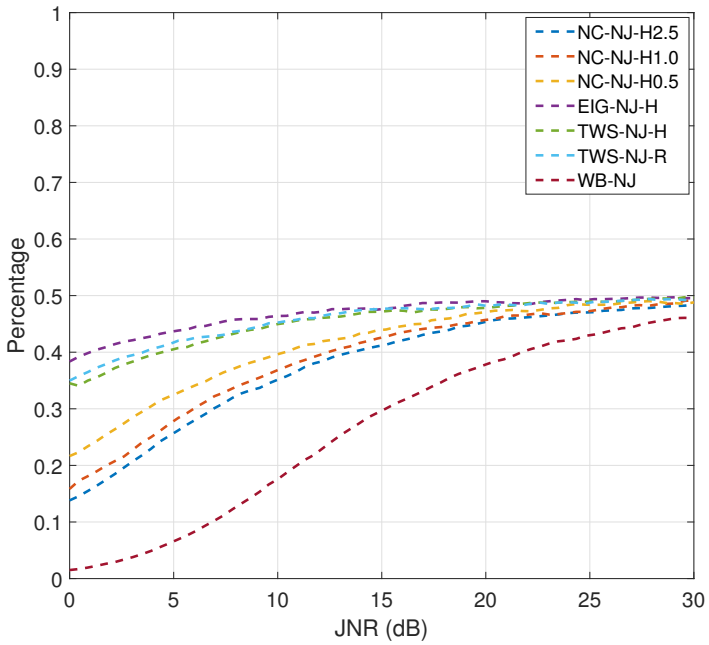


Figure 3.4. P_{far} comparison of the TWS-NJs, EIG-NJ-H, and all bandwidth constrained narrowband NJs for varying levels of JNRs.

Bandwidth constrained noise jammers do not obscure the whole waveform spectrum; only that frequency band which contains the largest response energy. While the eigenjammer also

Table 3.1. Receiver false alarm probability comparison at 6dB JNR

Jammer Type	Without EP
WB-NJ	0.0837
TWS-NJ-H	0.4155
TWS-NJ-R	0.4248
NC-NJ-H2.5	0.2802
NC-NJ-H1.0	0.3009
NC-NJ-H0.5	0.3431
EIG-NJ	0.4439

targets the transmit signal ESD containing the maximum energy, the EIG-NJ is shaped such that it still affects the entire waveform spectrum, thereby creating the most effective jammer. Similarly effective, TWS-NJs also interfere with the signal band containing the largest energy and produce ESDs that match the entire target frequency response, effectively obfuscating the spectrum. Note that at 0 dB JNR, the TWS-NJs already produce high probabilities of false alarm in the receiver thus suggesting that even a negative dB JNR value could potentially produce a relatively high P_{far}. In other words, the TWS-NJs are effective with a minimal amount of power.

Finally, we implement the adaptive EP matched filter against three of the best performing noise jammers: EIG-NJ-H, TWS-NJ-H, and NC-NJ-H0.5. The required P_{fa} to be met remains 1×10^{-3}. The design of the adaptive matched filter effectively whitens these jammers but unfortunately at the expense of effectively reducing the transmit waveform mainlobe, which is due to the knowledge-based nature of the TWS noise jammers. In Figure 3.5, the resulting P_d curves are shown for various JNRs. SNR required to reach a respectable P_d (i.e., 90%) increases with JNR. Therefore, if we are to keep the desired P_{fa}, the SNR must be greatly increased to reach a 90% detection probability. We can reduce the SNR required to reach this percentage, but then must accept a higher P_{fa}.

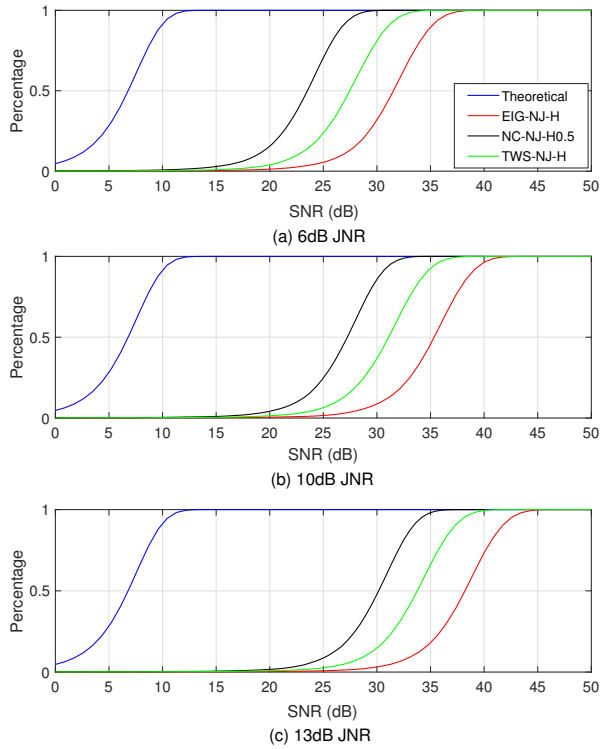


Figure 3.5. P_d comparison at 6dB, 10dB, and 13dB JNR with EP implemented. (a) EIG-NJ-H, (b) NC-NJ-H0.5, (c) TWS-NJ-H.

The EIG-NJ decreases detection probability the most, necessitating the largest SNR required to produce a desired P_d. For example, at P_d = 0.9, the SNR required at JNR = 6 dB are 27, 31, and 35 dB for NC-NJ, TWS-NJ, and EIG-NJ, respectively. The greater negative effect a jammer has on P_{fa}, the larger the SNR is required in order to reach the desired detection probability. The EIG-NJ yields the largest effect on P_{fa} thereby requiring the highest SNR to reach P_d = 0.9, followed by the TWS-NJ and NC-NJ, respectively. We observe that while these TWS-NJs can be successfully mitigated via an adaptive matched filter, this comes at the cost of requiring a significantly higher SNR (possibly 50 times or more) for the receiver to still effectively detect targets, which may require much more power than the corresponding transmitter can generate.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Deceptive Jamming Mitigation via Non-Coherent Integration

4.1 Coherent Jammer and Non-Coherent Detection Introduction

The aforementioned results demonstrate that simple adaptive filters successfully combat noise jammers, but at the cost of requiring high SNR to maintain the desired P_{fa}. However, EA has become more sophisticated in recent years, implying that filters alone may not be sufficient to maintain a desired detection rate. Combing various EP techniques such as frequency hopping, adaptive array antennas, power control, and sidelobe reduction may be required to minimize the EA effectiveness.

Deceptive jamming involves injecting false target information such as range, azimuth, or velocity into a victim-to-be receiver to trick the radar into interpreting the incorrect information as coming from a valid target. Unlike the TWS-NJ, deception jammers act only when a waveform is transmitted while trying to inject a few specific false targets in the victim receiver. Specifically, a coherent jammer (CJ) manipulates Doppler shift, range, and return gain of the transmit signal to generate fake targets in the victim radar. The manipulated waveform received by the radar produces false target returns which are nearly indistinguishable from the desired return. The modified and retransmitted CJ emission is highly correlated to the transmit waveform thus deceiving the radar display and operator who may react based on the false target, potentially leading to fatal consequences. CJs cause significantly increased false detection rates, thus presenting an extremely difficult problem to solve.

Coherent jammer suppression techniques detailed in [15] and [17] implement coherent detection via a transmit waveform target response matched filter (TWTR-MF). While traditional matched filters assume a point target, the TWTR-MF expects the received signal to be a convolution of the target response and transmit signal, which occurs if the transmit waveform bandwidth is much narrower than the target RCS [10]. Therefore, the CJ expects

the radar to receive an echo return of the transmit waveform only. In actuality, the received signal is a convolution between the transmit signal and target response; thus, the TWTR-MF yields a significantly reduced false detection rate (FDR). In this work, we expand the previous work in [15] and [17] to implement a non-coherent (NC) TWTR-MF to mitigate the false target returns generated by CJs. Coherent detection requires knowledge of both the amplitude and phase of the received signal. In other words, matched filter detection via coherent systems requires receiver phase alignment with the reference (transmit) signal.

Recovering the transmitted signal via coherent detection typically begins with multiplying the received signal with a sinusoidal wave generated by a local oscillator (LO). The LO is assumed to be synchronized in phase and frequency with the carrier wave used in the modulation process. Once the multiplication occurs, the product is sent through a low-pass filter to recover the baseband signal [18]. However, these received signals often experience a phase shift due the round-trip distance that the signal travels. This unknown phase-shift makes the ability of the system to recover the transmitted signal more difficult. One way to resolve this problem is to implement a non-coherent receiver which compares only the received signal energy or magnitude against a threshold thereby disregarding the received signal phase.

Legacy envelope (or energy) detectors utilize a combination of low pass filters and resistor-capacitor circuits to remove high frequency oscillations and recover the signal. Modern non-coherent systems implement analog-to-digital conversion in place of an RC circuit and split the converted digital signal into the in-phase and quadrature sequences. Each sequence passes through a LPF before being summed. The magnitude of the filter output summation is then compared against the threshold.

Non-coherent detection systems are typically less complex than coherent systems but yield slightly worse performance results since the non-coherent integration process discards some of the received signal information. Coherent integration allows M number of signal pulses to be summed in-phase with each other, increasing the total single-pulse SNR to MSNR. Averaging only the signal amplitude via non-coherent integration yields a gain less than MSNR but greater than $\sqrt{M}$SNR [9].

4.2 Modified System Model

The signal model needs to be modified when faced with an extended target since the received signal is the convolution of the transmit waveform and target response. Thus, the received signal is given by

$$\mathbf{y} = (\mathbf{x} * \mathbf{h_t})\, e^{j\Phi} + \mathbf{w}, \tag{4.1}$$

where $\mathbf{x}$ is the transmitted signal, $\mathbf{h_t}$ is the target impulse response, and $\mathbf{w}$ remains CWGN with a variance of σ^2. We include an unknown phase shift, Φ, which is modeled as a uniform random variable between 0 and 2π. The coherent jammer alters and retransmits $\mathbf{x}$ in an effort to deceive the victim radar. While the CJ can be located at various positions relative to the radar, it can also be located on the target from where it may direct the manipulated transmit signal back to the victim-to-be receiver.

4.3 Computer-Aided-Design Modeling

Successful operation under the extended target assumption requires that the target be electrically large enough for the convolution between the transmit waveform and target response to occur. To obtain target responses to be used in our experiments, we generate target radar cross sections (RCS) and corresponding impulse responses using Computer Simulation Technology (CST) Microwave Studio (MWS) software. CST MWS is an EM simulation software that enables analysis through various solvers, such as frequency/time domain, integral equation, eigenmode, and asymptotic. Electrically large targets require a high-frequency solver to reduce the number of computations associated with modeling targets that are thousands of wavelengths long [19]. Therefore, we use the asymptotic solver to generate RCS responses from the simulated far-field measurements produced via ray-tracing techniques. The asymptotic solver measures the far-field backscatter generated when an impinging signal hits a target, thus providing very accurate monostatic scattering analysis [20].

MWS offers a range of import options to choose when running EM simulations. Computer-aided-design (CAD) models are virtual objects that may potentially possess the same properties as the actual physical target. Engineers employ these models to test how objects would likely react and perform in reality which is an extremely useful technique that enables faster workflow and reduced manufacturing costs. Two open-source aircraft CAD models, as shown in Figures 4.1 and 4.2, are imported into MWS and scaled to their approximate phys-

ical size. Since these are digitally created models, they likely contain overlapping triangles or gaps from which some MWS solvers cannot generate a continuous error-free mesh. The asymptotic solver ignores these errors.

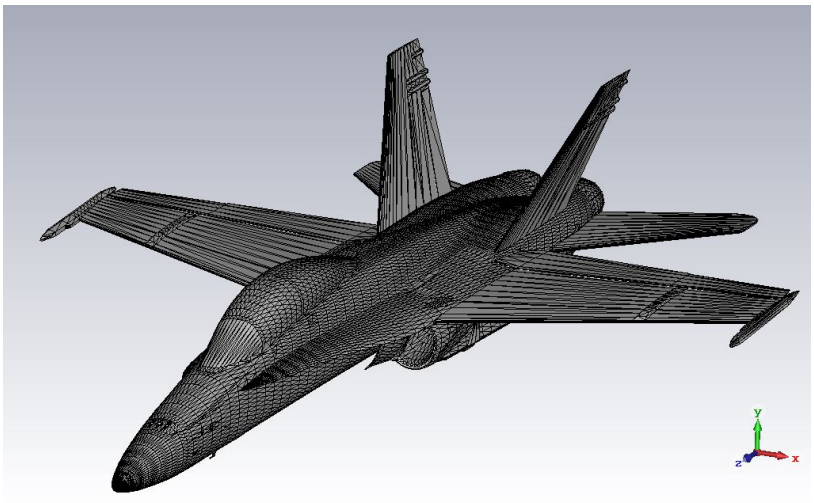


Figure 4.1. F-18 target CAD model.

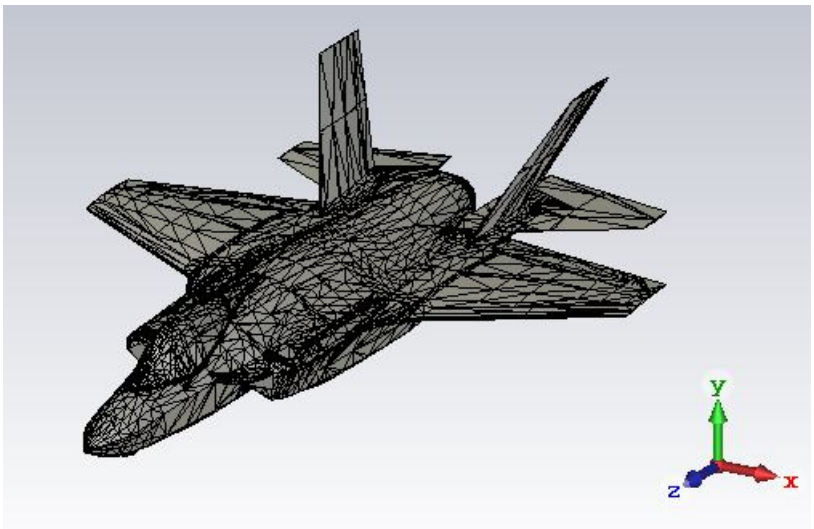


Figure 4.2. F-35 target CAD model.

4.3.1 RCS and Target Response Simulations

Airborne radar receivers typically operate in X-band between 8 - 12 GHz as shorter wavelengths provide increased resolution for target identification. Therefore, this thesis utilizes RCS responses from 8 - 9 GHz illuminated by an impinging signal at a constant elevation angle, $\phi_{el} = 0°$, across two azimuth angles, $\theta_{az} = 0°$ and $\theta_{az} = 45°$. A maximum of three reflections are used with horizontal E-field polarization for each azimuth and elevation orientation angle, which are displayed in Figure 4.3.

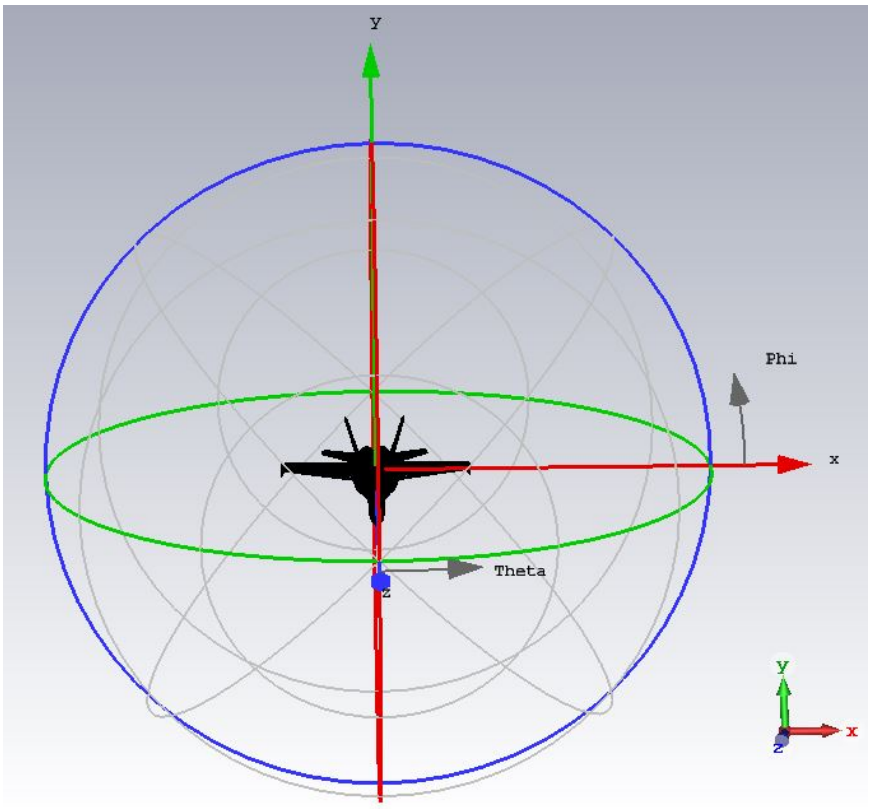
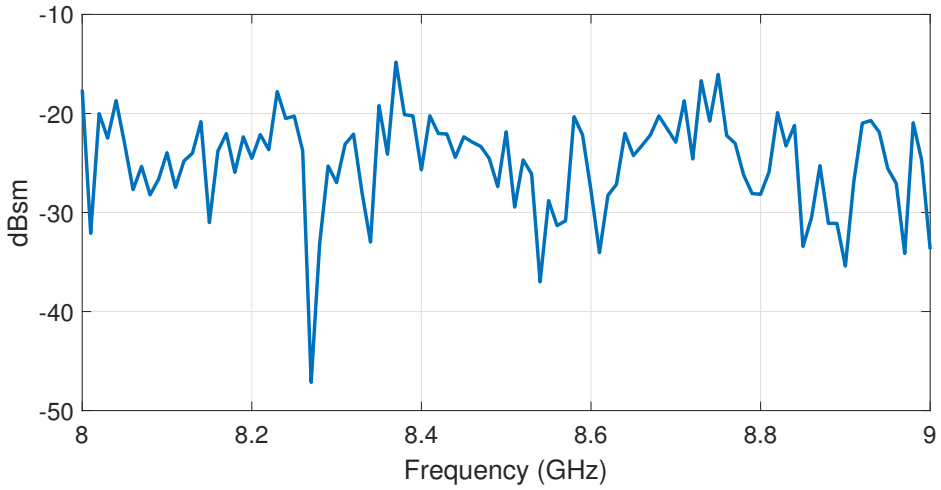
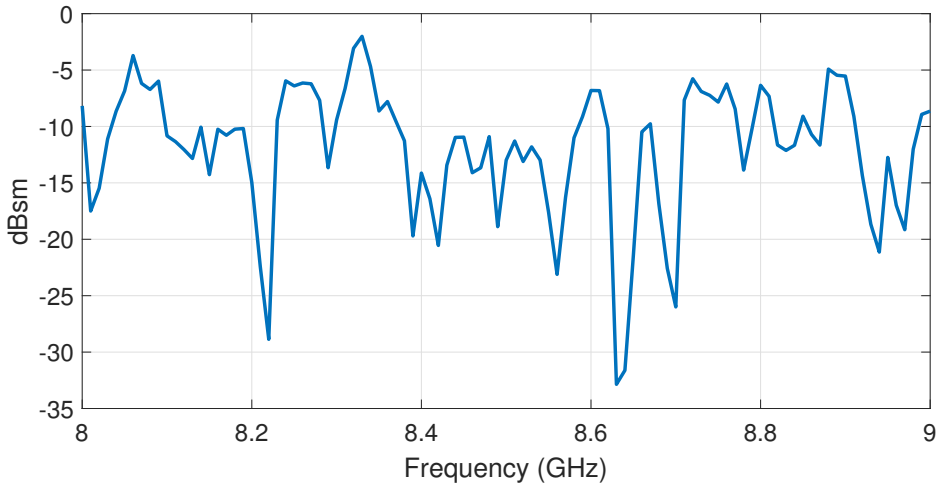


Figure 4.3. Azimuth (θ_{az}) and elevation (ϕ_{el}) angle orientation.

A target RCS depends upon various factors such as surface reflectivity and conductivity, size/shape of the platform, and incident angle of impinging signal. For simplicity, each target is modeled as a perfect electrical conductor (PEC) and the background is modeled as a vacuum. The RCS responses for the F-18 and F-35 are shown in Figures 4.4 and 4.5.



(a) $\theta_{az} = 0^{\circ}$, $\phi_{el} = 0^{\circ}$



(b) $\theta_{az} = 45^{\circ}$, $\phi_{el} = 0^{\circ}$

Figure 4.4. F-18 RCS response.

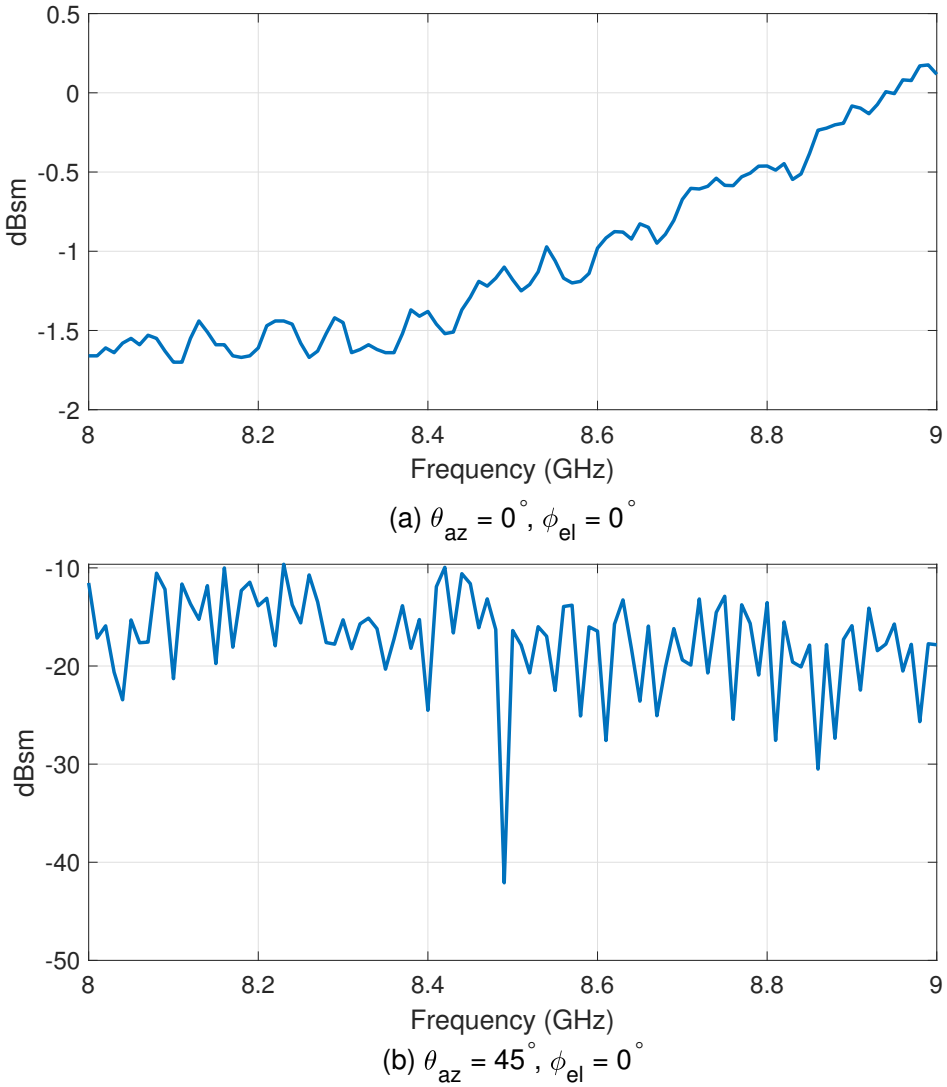


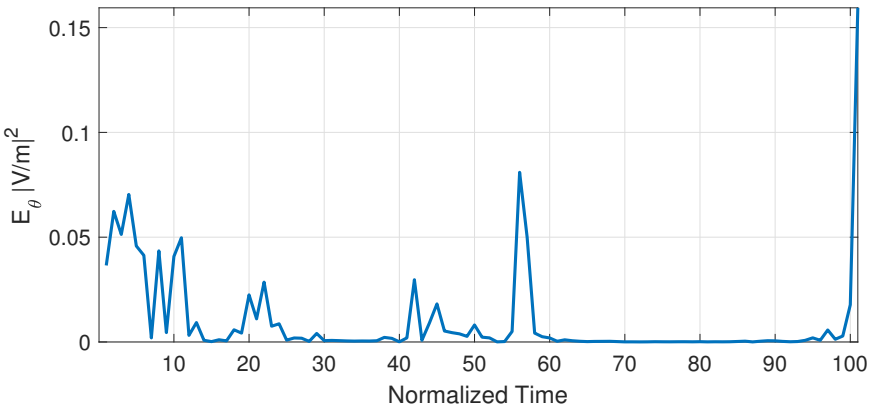
Figure 4.5. F-35 RCS response.

Stealth capabilities were incorporated into the two actual aircraft designs, however, increasing survivability of the F-18 was a higher priority than RCS reduction technology. Unlike the F-18, stealth capabilities were a significant factor when constructing the F-35 as engineers sought to design a next-generation fighter aircraft with very low observability. Techniques such as edge and engine inlet alignment, removal of unnecessary gaps, and radar absorbent material (RAM) reduce RCS, thus lowering the probability a target will be detected. Most

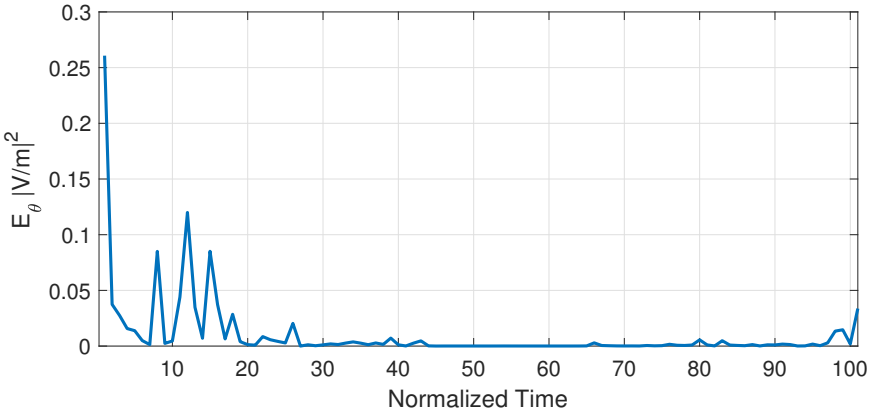
of these RCS reduction methods are beyond the scope of this thesis. However, observe that the shaping of the two aircraft influence the RCS simulations.

RCS responses also depend upon the incident angle of an impinging signal as non-uniform objects present different target patterns based upon the angle at which they are illuminated. For a head-on incident angle, the F-18 yields an average RCS of -24.92 dBsm while the F-35 yields an average RCS of -1.05 dBsm. The lower F-18 RCS is likely due to the narrower fuselage and lack of engine inlets on either side of the nose. A smaller, smoother surface area causes less backscatter thus generating a lower RCS. An impinging signal located at $\theta_{az} = 45^{\circ}$ results in average RCS values of -11.87 dBsm and -17.31 dBsm for the F-18 and F-35, respectively. We observe that the F-35 RCS reduction techniques such as internal carriage of weapons/sensors and alignment of edges reduce the number of scattering mechanisms at this azimuth angle and therefore, produce less signal reflected back towards the receiver.

The target impulse response magnitudes displayed in Figures 4.6 and 4.7 are generated using inverse Fourier Transform methods on the RCS response where sampling time is normalized. We also normalize the target response energy such that $E_t = 1$. Coherent jammers attempt to replicate the exact waveform and are, therefore, unaware that the receiver uses a priori knowledge of the RCS response. Therefore, when the CJ intercepts and retransmits the modified waveform, it assumes the receiver will detect it as the target return. However, the target response is more complex than the point target response which yields a favorable advantage to a receiver operating under the extended target assumption. This presents an opportunity to mitigate the CJ emission at the filter output.

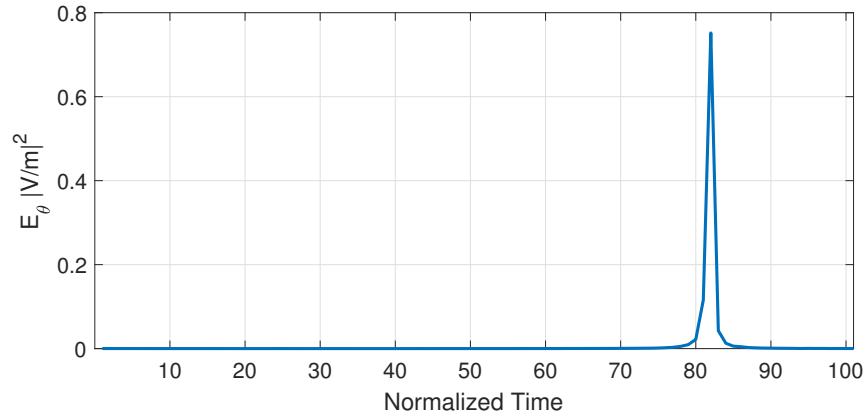


(a) $\theta_{az} = 0^\circ$, $\phi_{el} = 0^\circ$

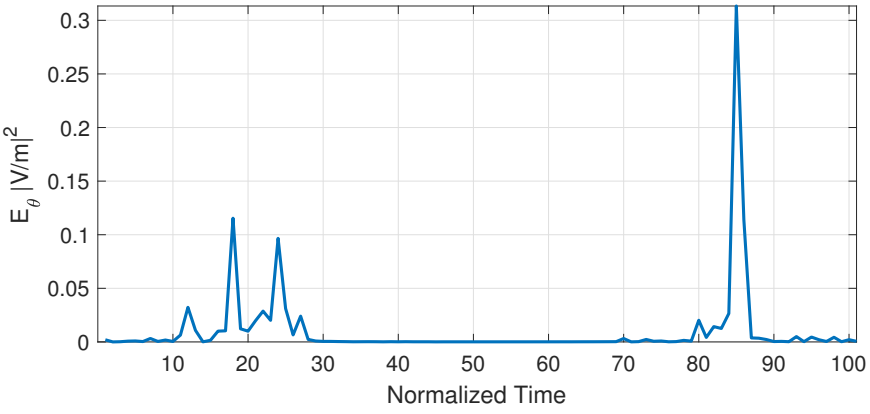


(b) $\theta_{az} = 45^\circ$, $\phi_{el} = 0^\circ$

Figure 4.6. F-18 target impulse response magnitude for $\theta_{az} = 0°$ and $\theta_{az} = 45°$ with zero elevation.



(a) $\theta_{az} = 0^\circ$, $\phi_{el} = 0^\circ$



(b) $\theta_{az} = 45^\circ$, $\phi_{el} = 0^\circ$

Figure 4.7. F-35 target impulse response magnitude for $\theta_{az} = 0°$ and $\theta_{az} = 45°$ with zero elevation.

4.4 Effect of Coherent Jammer and EP Mitigation

4.4.1 Target Response Convolution Process

Similar to methods previously described in Equation (2.2), we generate the normalized target response autocorrelation matrix, $\mathbf{R_t}$, from the target response convolution matrix

such that

$$\mathbf{R_t} = \mathbf{H_t^\dagger H_t}, \tag{4.2}$$

where $\mathbf{H_t}$ is the convolution matrix for $\mathbf{h_t}$. From [10], the maximum value of an extended target ambiguity function (AF) depends upon the transmit waveform and is, therefore, not constant for all waveforms. Rather, the AF peak is contingent on how strongly $\mathbf{x}$ correlates to $\mathbf{h_t}$. Maximizing this peak value is equivalent to maximizing the magnitude of the correlation between the transmit signal and target response:

$$\mathbf{D} = |\mathbf{x}^\dagger \mathbf{R_t x}| \tag{4.3}$$

where detection probability increases as the transmit waveform becomes more correlated to the target response's autocorrelation matrix.

4.4.2 Electromagnetic Protection via Non-coherent Detection

Developing a non-coherent version of the TWTR matched filter derived in [15] and [17] provides a simpler implementation option for target detection. The previous NP detection hypotheses operated under the coherent point target assumption and requires adjustment to accommodate the non-coherent extended target assumption. H_0 remains unchanged from Equation (2.4) however, the received signal, $\mathbf{y}$, contains a convolution of the transmit signal and target response with an unknown phase shift:

$$\begin{aligned} H_0 &: \mathbf{y} = \mathbf{w} \\ H_1 &: \mathbf{y} = (\mathbf{x} * \mathbf{h_t})\, e^{j\Phi} + \mathbf{w} \\ &\quad = \mathbf{z} e^{j\Phi} + \mathbf{w}. \end{aligned} \tag{4.4}$$

The distance between the receiver and the target causes a phase shift, Φ, that is unknown to the receiver and typically modeled as random. Estimating Φ requires a more complicated receiver than if we were to simply implement non-coherent detection. Non-coherent detection processes only the magnitude of the return signal and disregards the unknown phase under H_1. H_1 is decided if the LRT ratio from (2.5) is greater than a threshold $\tilde{\gamma}$.

If the jammer is not present, the detection probability for a fixed P_{fa} becomes a function of the transmit waveform and target response energy as the return echo is a convolution vice

simply a reflected version of the transmit signal [21]. When the transmit waveform is truly wideband (i.e., impulse waveform), the traditional non-coherent P_d equation given by

$$P_d = Q\left(\sqrt{-2\ln P_{fa}} - \sqrt{2SNR}\right) \tag{4.5}$$

becomes

$$P_d = Q\left(\sqrt{-2\ln P_{fa}} - \sqrt{2E_tSNR}\right) \tag{4.6}$$

where E_t is the target response energy and SNR = E_x/σ^2 is the (received) transmit signal-to-noise ratio. For this special case of a wideband/impulse transmit waveform, the traditional non-coherent threshold given by

$$\gamma_{nc} = \sqrt{-\sigma^2 E_x \ln(P_{fa})} \tag{4.7}$$

becomes

$$\gamma_{nc} = \sqrt{-\sigma^2 E_x E_t \ln(P_{fa})}. \tag{4.8}$$

Since we use a finite-time transmit waveform, Equations (4.6) and (4.8) need to be modified. In other words, utilizing the relationship from Equation (4.3) to modify the non-coherent P_d equations yields

$$P_d = Q\left(\sqrt{-2\ln P_{fa}} - \sqrt{2\mathbf{D}E_tSNR}\right) \tag{4.9}$$

and the corresponding adjusted threshold for the non-coherent TWTR-MF becomes

$$\gamma_{nc}^{'} = \sqrt{-\sigma^2 E_x E_t \mathbf{D} \ln(P_{fa})}. \tag{4.10}$$

The output test statistic of the non-coherent TWTR matched filter is given by

$$T(\mathbf{y}) = |\mathbf{z}^{\dagger}\mathbf{y}| \tag{4.11}$$

where the absolute value of a complex-valued output is compared to $\gamma_{nc}^{'}$ for usual detection. Taking the absolute value vice real part differentiates non-coherent versus coherent detection as only the filter's output magnitude is used in non-coherent detection.

CHAPTER 5:
Performance Evaluation for Non-Coherent EP against Coherent Jammers

5.1 Performance Evaluation Method

To evaluate performance results, we generate complex valued rect and Hamming transmit waveforms and convolve them with the aircraft target impulse responses produced through MWS. We perform 10,000 Monte Carlo simulations per transmit energy (or SNR) level to evaluate the non-coherent matched filter performance against a coherent jammer emission. The theoretical probability of detection in (4.9) considers only the case where noise and the true return signal are present. The detection probability expected by the jammer is given by (4.5) or (4.6) if it assumes the receiver uses a traditional non-coherent matched filter. In that case, the CJ expects that received signal is matched to the filter (but with an unknown phase shift). In reality, we calculate the FDR when the CJ emits the transmit waveform and the receiver uses the non-coherent TWTR matched filter. The desired P_{fa} remains 1×10^{-3} with the noise variance and target energy set to unity in our simulations.

5.2 Performance Results

Figures 5.1 - 5.4 display the F-18 and F-35 MC simulations for the two transmit waveforms and given azimuth angles. The expected performance of the non-coherent TWTR matched filter is shown by the simulated P_d curves in blue. The CJ expects the receiver to contain a traditional NC matched filter that assumes a point target thus generating the FDR shown in the red curves. However, the echo return is sent through the NC TWTR matched filter which accounts for the convolution that occurs vice what the CJ expects.

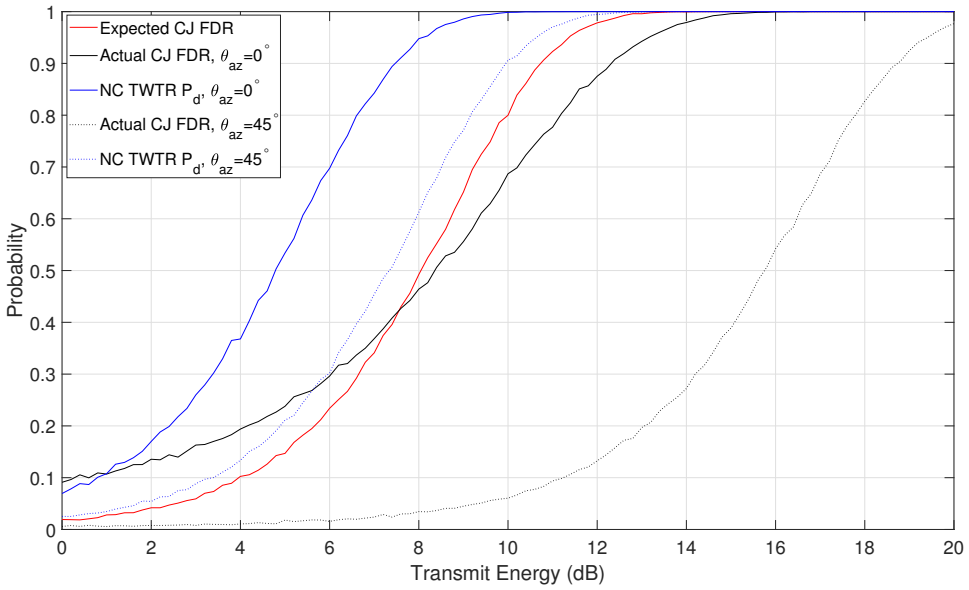


Figure 5.1. Rect TW performance results for F-18 target for $\theta_{az} = 0°$ and $\theta_{az} = 45°$ at zero elevation.

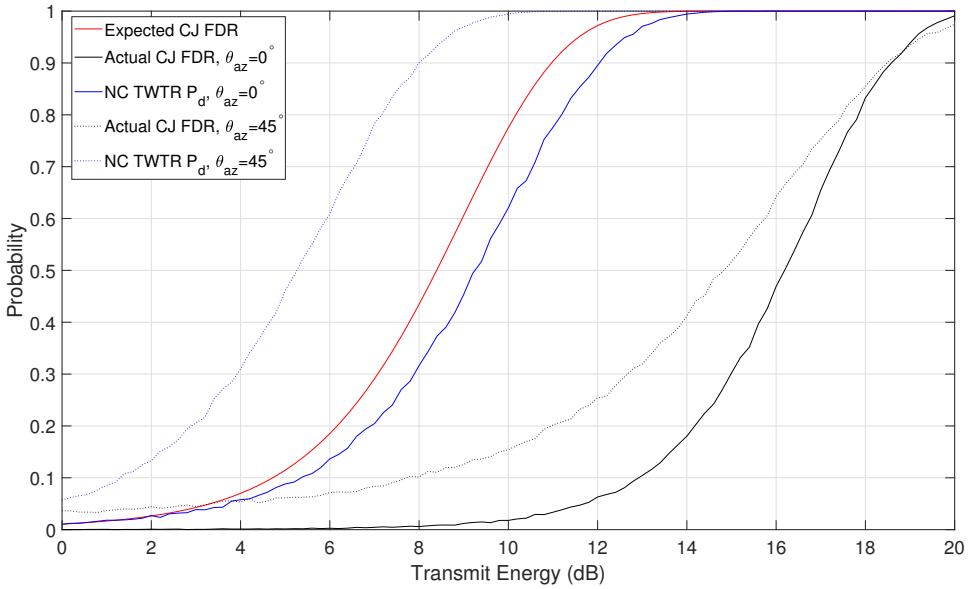


Figure 5.2. Rect TW performance results for F-35 target for $\theta_{az} = 0°$ and $\theta_{az} = 45°$ at zero elevation.

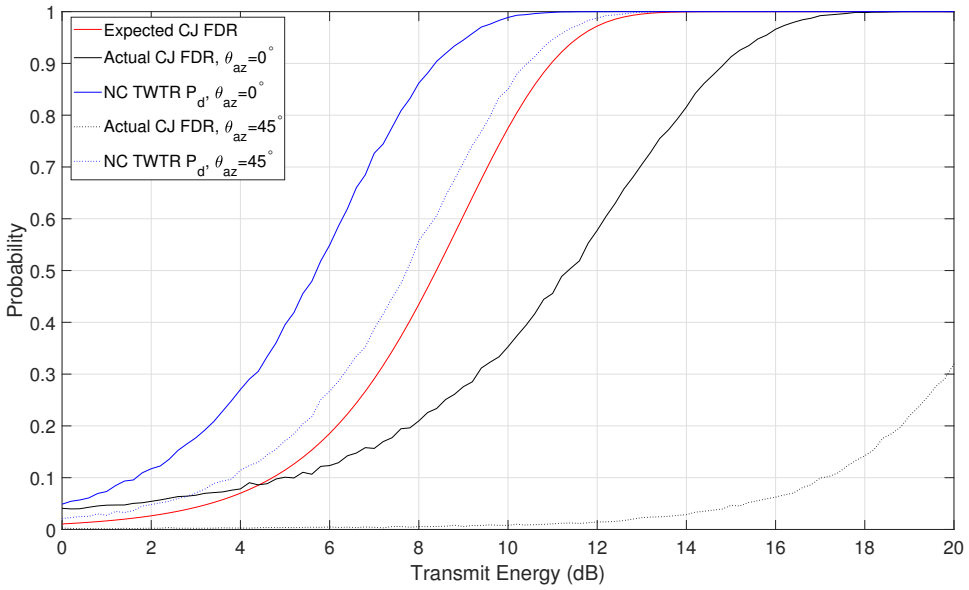


Figure 5.3. Hamming TW performance results for F-18 target for $\theta_{az} = 0°$ and $\theta_{az} = 45°$ at zero elevation.

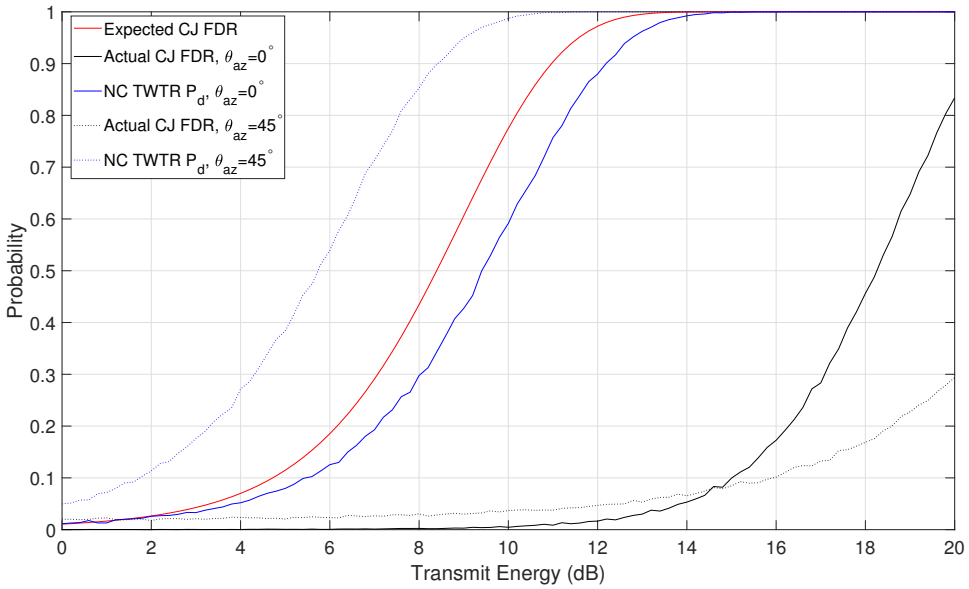


Figure 5.4. Hamming TW performance results for F-35 target for $\theta_{az} = 0°$ and $\theta_{az} = 45°$ at zero elevation.

From these results, we see that the new non-coherent TWTR-MF successfully reduces the expected false returns from the CJ in red to the actual false detection rate in black. The CJ expects a traditional NC matched filter with a lower threshold. The NC TWTR-MF mitigates the CJ emission and thus lacks the necessary energy level to reach the CJ expected false detection rate. Note, however, that the actual CJ FDR in Figure 5.1 and 5.3 for $\theta_{az} = 0°$ is greater than its expected CJ up to approximately 7 dBW/Hz and 5 dBW/Hz transmit energy, respectively. Despite a higher-than-expected FDR, the P_d remains significantly higher when the NC TWTR-MF is implemented.

The expected CJ FDR calculated via (4.6) remains nearly fixed for each simulation. However, the transmit waveform type and target response of a given azimuth angle affect the P_d. The rect and Hamming TWs yield higher detection probabilities for all transmit energy values when compared to the expected CJ FDR, with one exception; the NC TWTR P_d for the F-35 when $\theta_{az} = 45°$ yields worse performance results. Note that while comparison to the expected FDR is interesting (such as the case just mentioned), a more useful comparison is the actual CJ FDRs versus the NC TWTR $P_d s$. In all cases the actual CJ FDRs are significantly lower than the NC TWTR $P_d s$.

If we focus on the F-18, we observe that the Hamming pulse requires approximately 8.4 dBW/Hz and 10.4 dBW/Hz transmit energy to reach $P_d = 0.9$ for $\theta_{az} = 0°$ and $\theta_{az} = 45°$, respectively, while the rect pulse requires approximately 7.5 dBW/Hz and 10 dBW/Hz transmit energy for the aforementioned azimuth angles.

While the results show a similar pattern for the F-35, we observe that the $\theta_{az} = 0°$ detection curves requires a higher transmit energy to reach a 90% P_d for the rect and Hamming pulses, but not for the $\theta_{az} = 45°$ detection curves. The Hamming pulse requires approximately 12.2 dBW/Hz and 8.4 dBW/Hz to reach $P_d = 0.9$ for $\theta_{az} = 0°$ and $\theta_{az} = 45°$, respectively. The rect pulse requires approximately 12 dBW/Hz and 8 dBW/Hz transmit energy for the given azimuth angles. Tables 5.1 and 5.2 more closely investigate these performance results, specifically for a transmit energy value of 8 dBW/Hz. The columns represent the platform, given illumination angles, the expected CJ FDR, the actual CJ FDR when the NC TWTR-MF is implemented, and the probability of detection for the NC TWTR-MF.

Table 5.1. Rect pulse detection rate comparison for 8 dBW/Hz transmit energy

Platform	Azimuth Angle	Expected CJ FDR	Actual CJ FDR	NC TWTR-MF P_d
F-18	0°	0.4924	0.4641	0.9478
F-35	0°	0.4346	0.0060	0.3165
F-18	45°	0.4924	0.0345	0.6126
F-35	45°	0.4346	0.1015	0.9010

Table 5.2. Hamming pulse detection rate comparison for 8 dBW/Hz transmit energy

Platform	Azimuth Angle	Expected CJ FDR	Actual CJ FDR	NC TWTR-MF P_d
F-18	0°	0.4346	0.2096	0.8620
F-35	0°	0.4346	0.0024	0.2977
F-18	45°	0.4346	0.0056	0.5574
F-35	45°	0.4346	0.0306	0.8528

Consider for the case of 0° azimuth angle in Table 5.1 with the use of the rect pulse. Note that P_d for the F-18 is larger than P_d for the F-35. But at 45° azimuth angle, we observe the opposite, where P_d is larger for the F-35 than the F-18. This effect is due to the fact that P_d depends on the correlation between the rect transmit waveform and the target RCS response at a specific angle as dictated by (4.9). We note the same observations in Table 5.2 with the use of the Hamming pulse, albeit with slightly less $P_d s$, which indicates that the rect is more correlated to the RCS responses than Hamming. Perhaps this is due to the fact that RCS responses are usually wideband. In other words, since a rect waveform is more wideband than a Hamming waveform, the $P_d s$ should be higher which concur with the results in the tables.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 6:
Conclusion

6.1 Summary and Conclusion

In this thesis, we used complex-valued rect and Hamming transmit waveforms to investigate the performance effects of TWS-NJs and CJs. We developed corresponding EP techniques to mitigate these threats at the expense of increased SNR. The first half of this work focused on the TWS-NJs where the bandwidth constraint relative to the width of the transmit waveform mainlobe was parameterized to generate variations of practical narrowband TWS jammers. To evaluate performance of the TWS-NJs, we varied JNR and examined detection probability and receiver false alarm probability. Shaped noise jammers significantly reduced detection performance at high SNR and increased P_{far} as they effectively were colored Gaussian noise vice WGN. Altogether, the EIG-NJ proved to be the superior noise jammer.

Assuming a priori knowledge of the NJ spectra, we developed EP techniques to mitigate the false alarm effects of the TWS jammer family. The counter-EA method successfully mitigated the negative effects of all noise jammers considered but at the expense of also filtering the desired signal energy. In other words, large SNR is needed to maintain the desired P_{fa} and P_d.

In the second half of this thesis, we developed target impulse responses generated from RCS simulations for two aircraft CAD models. The target responses were then used to create a NC TWTR matched filter utilizing an extended target assumption, which receivers exploited to mitigate the CJ signal. The simulation results demonstrated the NC TWTR-MF successfully reduced the FDR caused by coherent jammers.

6.2 Future Work

This thesis has shown that the EA jammer waveforms and adaptive matched filters can be successfully implemented through computer simulation. For more realistic applications, the feasibility of jammer transmission and subsequent matched filtering should be tested via RF transmission. Many AWGs configure in-phase and quadrature modulation of internally

or externally generated digital signals, establishing the framework to seamlessly shift from computer to RF simulations.

The EA and EP methods can be significantly expanded to investigate performance effects utilizing different simulation parameters. The rect and Hamming pulse waveforms were chosen for simplicity whereas more complex waveforms or pulse trains can be utilized to develop and test these jammers. Regarding the RCS simulations, one can vary the frequency ranges and modify the illumination angles to investigate how the NC TWTR-MF performs against CJs given different target impulse responses. More practical CAD models with better fidelity (i.e., reflecting actual materials and such) would also produce different RCS patterns, presenting expanded opportunities to explore the CJ FDR and mitigating effects of the NC TWTR-MF.

List of References

[1] M. LaMarche, "The history of electronic warfare: An overview of electronic warfare part 1," blog, September 2018. [Online]. Available: https://www.mrcy.com/company/blogs/history-electronic-warfare-overview-electronic-warfare-part-1.

[2] M. von Spreckelsen, "Electronic warfare – The forgotten discipline: Why is the refocus on this traditional warfare area key for modern conflict?" *Journal of the Joint Air Power Competence Centre*, vol. 27, pp. 41–45, 2018. [Online]. https://www.japcc.org/electronic-warfare-the-forgotten-discipline/.

[3] *Joint Electromagnetic Spectrum Operations*, Joint Publication 3-85, Chairmen of the Joint Chiefs of Staff, Washington, DC, 2020, pp. 1–13.

[4] F. Ji-ning, W. Jun, D. Zhe-jun, and Y. Xiao-bo, "Study on the effect of wideband Gaussian jamming to FLL of navigation receiver," in *2013 3rd International Conference on Consumer Electronics, Communications and Networks*, 2013, pp. 630–635. [Online]. doi: 10.1109/CECNet.2013.6 703 410.

[5] H. Paik, N. N. Sastry, and I. SantiPrabha, "Effectiveness of noise jamming with white Gaussian noise and phase noise in amplitude comparison monopulse radar receivers," in *2014 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 2014, pp. 1–5. [Online]. doi:10.1109/CONECCT.2014.6 740 286.

[6] X. Zhang and T. Chen, "Noise-linear frequency modulation shared waveform for integrated radar and jammer system," in *2007 International Conference on Communications, Circuits and Systems*, 2007, pp. 644–648. [Online]. doi:10.1109/ICCCAS.2007.4 348 136.

[7] B. Dulek, S. Gezici, and O. Arikan, "Convexity properties of detection probability under additive Gaussian noise: Optimal signaling and jamming strategies," no. 13, 2013, vol. 61, pp. 3303–3310. [Online]. doi: 10.1109/TSP.2013.2 259 820.

[8] Q. J. O. Tan and R. A. Romero, "Jammer-nulling transmit-adaptive radar against knowledge-based jammers in electronic warfare," *IEEE Access*, vol. 7, pp. 181 899–181 915, 2019.

[9] M. A. Richards, J. A. Scheer, and W. A. Holm, *Principles of Modern Radar, Basic Principles*. Edison: SciTECH Publishing, 2010.

[10] J. Nieh and R. A. Romero, "Comparison of ambiguity function of eigenwaveform to wideband and pulsed radar waveforms: A comprehensive tutorial," in *The Journal of Engineering*, 2018, vol. 4, pp. 203–221.

[11] R. A. Romero, J. Bae, and N. A. Goodman, "Theory and application of SNR and mutual information matched illumination waveforms," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 2, pp. 912–927, 2011.

[12] N. A. Goodman, P. R. Venkata, and M. A. Neifeld, "Adaptive waveform design and sequential hypothesis testing for target recognition with active sensors," *IEEE Journal of Selected Topics in Signal Processing*, vol. 1, no. 1, pp. 105–113. [Online]. doi: 10.1109/JSTSP.2007.897 053, 2007.

[13] M. R. Bell, "Information theory and radar waveform design," *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1578–1597. [Online]. doi: 10.1109/18.259 642, 1993.

[14] Y. Wu and J. Nieh, "Performance analysis of radar eigenwaveform design integrated with pulse compression scheme," in *2019 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*, 2019, pp. 99–103. [Online]. doi: 10.1109/ICRAMET47 453.2019.8 980 425.

[15] H. Albuquerque and R. A. Romero, "Coherent jammer mitigation with target signatures using LFM and Frank-coded waveforms," in *2019 53rd Asilomar Conference on Signals, Systems, and Computers*, 2019, pp. 1338–1343. [Online]. doi: 10.1109/IEEECONF44 664.2019.9 049 067.

[16] S. M. Kay, *Fundamentals of Statistical Signal Processing Detection Theory*. Upper Saddle River: Prentice-Hall PTR, 1998.

[17] Q. J. O. Tan and R. A. Romero, "Airborne target detection using dual matched filter discriminator with matched waveform illumination for coherent jammer suppression," in *2019 IEEE Radar Conference (RadarConf)*, 2019, pp. 1–6. [Online]. doi: 10.1109/RADAR.2019.8 835 694.

[18] S. Haykin and M. Moher, *Introduction to Analog & Digital Communications*, 2nd ed. John Wiley & Sons, Inc., 2007.

[19] *CST Studio Suite*, CST, 2017. [Online]. https://tespol.com.pl/wp-content/uploads/2017/10/CST-STUDIO-SUITE-2017.pdf.

[20] H. Albuquerque, "Coherent jammer mitigation using transmit waveform-target response matched filter with LFM and Frank-coded waveform," M.S. thesis, Dept. of Elec. and Comp. Eng., NPS, Monterey, CA, USA, 2019.

[21] R. A. Romero, “Detection performance of matched transmit waveform for moving extended targets,” in *2013 Asilomar Conference on Signals, Systems and Computers*, pp. 1956–1960. [Online]. doi: 10.1109/ACSSC.2013.6 810 646.

THIS PAGE INTENTIONALLY LEFT BLANK

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California