NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CONSIDERATIONS FOR OPERATIONALIZING CAPABILITIES FOR EMBEDDED COMMUNICATIONS SIGNALS IN MARITIME RADAR

by

Jason L. Hooper

December 2018

Thesis Advisor:	Ric Romero
Second Reader:	George W. Dinolt

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2018	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE CONSIDERATIONS FOR OPERATIONALIZING CAPABILITIES FOR EMBEDDED COMMUNICATIONS SIGNALS IN MARITIME RADAR	5. FUNDING NUMBERS REM7K
6. AUTHOR(S) Jason L. Hooper	
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 work, we explore the feasibility of injecting data into an existing radar waveform. Specifically, we investigate how to embed communications signals within a navigation radar pulse to explore the potentials for a) receiving and demodulating the associated communications data, and b) identifying potential vulnerabilities/effects to maritime networks that inadvertently receive data in this manner. In this thesis, we advance previous work by utilizing a more practical, navigation-like radar waveform instead of an idealized, rectangular pulse previously studied. We utilize a particular radar system in order to calculate its actual throughput with the use of an embedded or combined signal. Considering that the radar waveform may not be detected at times due to modest radar-to-communications power ratio, we calculate the embedded communications' effective symbol error ratio. We also demonstrate the spectrum of the radar-embedded communications waveform on a carrier via signal generator and spectrum analyzer.

14. SUBJECT TERMS communications, radar, FURUNO, cyber, injection, maritime, QPSK, QAM, modulation, demodulation, bit-error-rate, bit, error, rate, symbol-error-rate, symbol, error, rate, BER, SER, maritime network, embedded communications, interpulse, intrapulse, OFDM, orthogonal, frequency, division, multiplexing, quadrature, pulse, shift, keying	15. NUMBER OF PAGES 61
	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.

CONSIDERATIONS FOR OPERATIONALIZING CAPABILITIES FOR EMBEDDED COMMUNICATIONS SIGNALS IN MARITIME RADAR

Jason L. Hooper
Lieutenant Commander, United States Navy
BS, Prairie View A & M University, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2018

Approved by: Ric Romero
Advisor

George W. Dinolt
Second Reader

Clark Robertson
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this work, we explore the feasibility of injecting data into an existing radar waveform. Specifically, we investigate how to embed communications signals within a navigation radar pulse to explore the potentials for a) receiving and demodulating the associated communications data, and b) identifying potential vulnerabilities/effects to maritime networks that inadvertently receive data in this manner. In this thesis, we advance previous work by utilizing a more practical, navigation-like radar waveform instead of an idealized, rectangular pulse previously studied. We utilize a particular radar system in order to calculate its actual throughput with the use of an embedded or combined signal. Considering that the radar waveform may not be detected at times due to modest radar-to-communications power ratio, we calculate the embedded communications' effective symbol error ratio. We also demonstrate the spectrum of the radar-embedded communications waveform on a carrier via signal generator and spectrum analyzer.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 Introduction **1**
1.1 Maritime Cyber Domain 1
1.2 Operationalizing the Integrated Radar-Communications Receiver 2
1.3 Objective 3
1.4 Thesis Organization 4

2 Signal Modeling **5**
2.1 The Radar Signal 5
2.2 Communications: The Embedded Signal 6
2.3 Combined Signal: Radar and Communications 8

3 Application of System Parameters **13**
3.1 Calculation of Effective Channel Throughput 13
3.2 Navigation Radar System Parameter Application 14

4 Effective SER for Embedded Communications and Probability of Detection for Radar **17**
4.1 Radar and Communications Waveform Development 17
4.2 Combined Signal Detection via Radar Waveform. 18
4.3 Demodulation of Embedded Signal 20
4.4 Probability of Detection. 21

5 Practical Considerations for Radar Parameter Application, Signal Transmission, and Fading Channel **29**
5.1 Simulation Utilizing Actual Radar Parameters 29
5.2 Generation of Combined Signal 31
5.3 Further Consideration of the Channel: Multipath Fading 33
5.4 Considerations within the MCD 37

6 Conclusion **39**

Initial Distribution List **45**

List of Figures

Figure 1.1 Illustration of Vast Communication in MCD. Source:[3]. 2

Figure 1.2 A Possible Scenario in Which Embedded Intrapulse Communications Could Be Used as an Embedded Communication Method. Adapted from [5]. 3

Figure 2.1 Spectrum of a Practical Navigation Radar Pulse Shape Used for Simulations. 7

Figure 2.2 Real (a) and Imaginary (b) Components of the Modeled Navigation-Like Radar Pulse. 10

Figure 2.3 The In-Phase Component of the Combined Signal Compared to the Radar Pulse, with (a)$RCR_{dB} = 0$; (b)$RCR_{dB} = 3$; and (c)$RCR_{dB} = 10$. $SRBR = 17$. 11

Figure 2.4 The In-Phase Component of the Combined Signal Compared to the Radar Pulse, with (a)$SRBR = 17$; and (b)$SRBR = 1$. $RCR_{dB} = 3$. 12

Figure 4.1 The SER Plots of Ideal QPSK vs Demodulated Embedded Signal with RCR Held Constant at $RCR_{dB} = 20$. (a)$SRBR = 1$; (b)$SRBR = 2.125$; (c)$SRBR = 17$. $P_{FA} = 10^{-5}$. 22

Figure 4.2 Probability of Detection Plots Shown for (a)$SRBR = 17$; (b)$SRBR = 2.125$; (c)$SRBR = 1$. RCR is held constant at $RCR_{dB} = 0$. $P_{FA} = 10^{-5}$. 25

Figure 4.3 The eSER Plotted Alongside Corresponding Percentage of Missed Detection with RCR Held Constant at $RCR_{dB} = 0$ and $P_{TX} = 70000$. $P_{FA} = 10^{-5}$. (a)$SRBR = 1$; (b)$SRBR = 2.125$; (c)P_D for (a); (d)P_D for (b). 26

Figure 4.4 The eSER Plotted Alongside Corresponding Percentage of Missed Detection with SRBR Held Constant at $SRBR = 17$ and $P_{TX} = 10000$. $P_{FA} = 10^{-5}$. (a)$RCR_{dB} = -3$; (b)$RCR_{dB} = -6$; (c)P_D for (a); (d)P_D for (b). 27

Figure 4.5 The eSER Plotted Alongside Corresponding Percentage of Missed Detection, Comparing the Consequences of Varying P_{FA} with Conditions: $RCR_{dB} = -3$; $SRBR = 17$; and $P_{TX} = 10000$. (a)$P_{FA} = 0.01$; (b)$P_{FA} = 0.001$; (c)P_D for (a); (d)P_D for (b). 28

Figure 5.1 A Simulated Spectrum of the Modulated Combined Signal Displayed with Carrier Frequencies (a) 500 MHz and (b)800 MHz at $RCR_{dB} = 20$. 30

Figure 5.2 A Simulated Spectrum of the Modulated Combined Signal Displayed with Carrier Frequencies (a) 500 MHz and (b) 800 MHz at $RCR_{dB} = 3$. 31

Figure 5.3 A Conventional RS Signal Analyzer and Generator Combination. Adapted from [12]. 32

Figure 5.4 The R&S FSQ Spectra of the Generated and Transmitted Combined Signal, at $RCR = 20dB$ and $SRBR = 17$, with Carrier Frequencies (a) 500 MHz and (b) 800 MHz. 33

Figure 5.5 The R&S FSQ Spectra of the Generated and Transmitted Combined Signal, at $RCR = 3dB$ and $SRBR = 17$, with Carrier Frequencies (a) 500 MHz and (b) 800 MHz. 34

Figure 5.6 Furuno FAR-2117 Radar Specifications. Adapted from [13]. . . . 36

Figure 5.7 Systems Generally Found Within Maritime Networks and some Factors that Contribute to their Vulnerabilities. Source: [17]. 37

List of Acronyms and Abbreviations

A/D analog-to-digital

AIS automatic identification system

AWGN additive white Gaussian noise

BER bit error ratio

BPSK binary phase-shift keying

BW bandwidth

CW continuous wave

DoD Department of Defense

ECDIS electronic chart display information system

eSER effective symbol error ratio

FFT fast Fourier transform

GPS global positioning system

ICS industrial control systems

I/Q in-phase/quadrature

ISI intersymbol interference

IT information technology

MC Monte Carlo

MLD maximum-likelihood detection

PRF pulse repetition frequency

PRI pulse repetition interval

PSD power spectral density

QPSK quaternary phase-shift keying

RCR radar power-to-communications power ratio

RF radio frequency

SDR software defined radio

SER symbol error ratio

SISO single input-single output

SNR signal power-to-noise power ratio

SRBR symbol-rate-to-bandwidth ratio

VHF very high frequency

VSAT very small aperture terminal

Acknowledgments

I want to offer a very special thanks to the following: My advisor, Professor Ric Romero, who did no small amount by teaching me about “symbols,” the value of hard work, enthusiasm, and effective communication(s)—pun intended. Your patience, endurance, and dedication will be a pillar of inspiration for me for years to come.

Jeff Knight, LT Sean Kennedy, Capt. Matthew Audette, LT Jon Harrell, and LCDR Tauseef Ashraf, who each offered kindness, and selflessness by devoting hours of tutelage to help create an engineer.

The Electrical and Computer Engineering Department faculty and staff, each of whom edified my knowledge and fortitude.

JET, who told me that I could "do anything" but that I do not have to "be everything."

Those who allowed me to inspire them to improve and progress, whether through my own actual or apparent strengths or by your avoidance of my real or perceived deficiencies and shortfalls. Your testimony of growth is a bulwark for my own continued will to succeed.

The call of God’s great Sea, which continued to nourish my will to return to its divine waters, and inspired my academic tenacity only that I might return to be held once again in its ever welcome embrace...

The woman of my life, my love, the mother of my children, and rock of our family, whose actions allow me to continue to be a warrior for this nation. My adoration for you can only aspire to match your willingness to continue to sacrifice for me and our family. I love you.

My children, who never cease to amaze me and who showed the pureness of their hearts by continuing to forgive Daddy for the countless nights he spent at Hotel Spanagel.

The Blessed and Mighty, True and Living, Great and Omniscient One, with His help, love, and protection may we all be blessed.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1: Introduction

The goal of this work is to continue exploration of the implications and feasibility of embedding communications in a radar waveform. In this thesis, we assume that the radar signal and communications signal may be significantly contrasted in power. Our project continues in the legacy of work that studies "weak," or low-power, communications signals in the presence of a "strong," or high-powered, radar signal. In some situations, the high power contrast may not be practical, so we also consider the case where the signals are of the same order of magnitude. We specifically consider the purposeful embedding of modulated communications within a pulsed radar or continuous-wave (CW) radar in order to discover the potential to operationalize covert communications and begin to characterize cyber implications within the maritime domain.

1.1 Maritime Cyber Domain

Many industrial, maritime, and defense technologies have been developed and fielded with security vulnerabilities. In a network of systems, any vulnerability in a particular system may present vulnerabilities to other systems within its network. As developers continue to work to create better, faster, and more powerful technologies, there is parallel competition to develop better, faster, and more robust exploitation tools. The evolution of Arpanet into the internet presents itself as a classic example of this competition [1].

Herein lies the state of the maritime cyber domain (MCD), a domain in which attacks are understood to be a growing concern [2]. The fact that the same classification of malicious internet actors can be identified within the MCD should be unsurprising. The maritime domain is, after all, a veritable network consisting of nodes that unceasingly transit across a vast physical area, in which communications occur in a variety of ways, utilizing a plethora of means, both wittingly and unwittingly, as illustrated in Figure 1.1. All of these communications channels provide a potential for a covert channel. In this thesis, we specifically discuss a covert communications channel embedded in the navigation radar pulse.

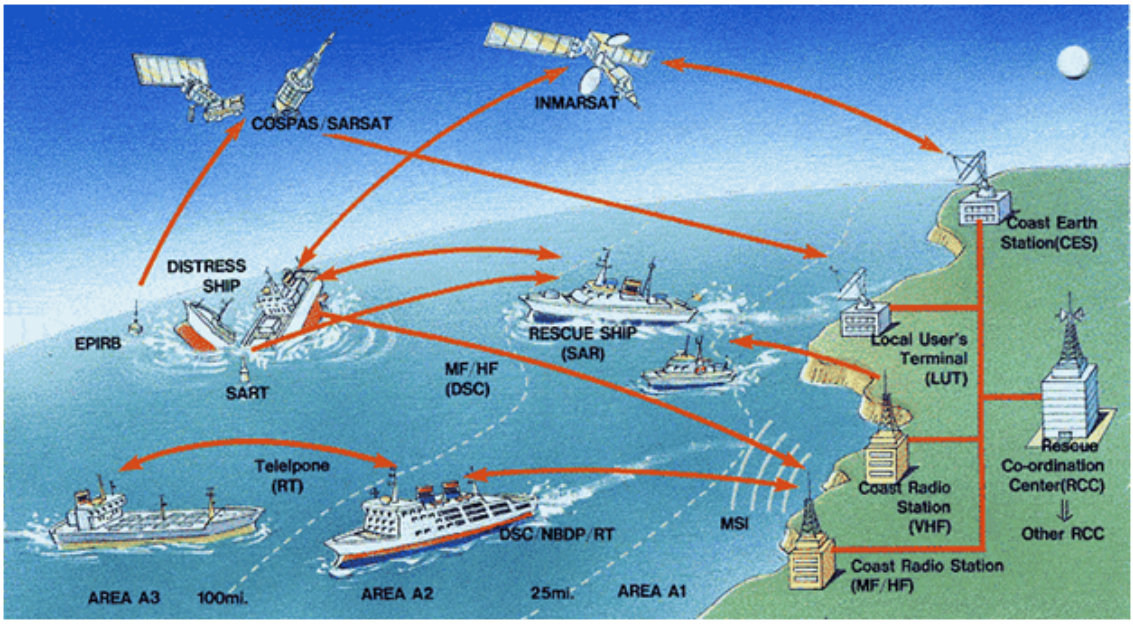

Figure 1.1. Illustration of Vast Communication in MCD. Source: [3].

Similar to the internet, operators of these "nodes," or maritime vessels, can range from Merchant Marine and naval officers to pirate-terrorists, hacktivists, and government-sanctioned cyber actors. Taking a closer look at what we identify as maritime nodes, we see the implications become more apparent and applicable to our situation: neither maritime vessels nor their associated systems are constructed with substantial consideration for the surfeit of potential cyber exploits that may be initiated from within the MCD.

1.2 Operationalizing the Integrated Radar-Communications Receiver

Throughout this thesis, we continue along the same path of previous work in expounding on embedded communications within a radar signal. In previous work, it was assumed that the radar power is much larger than the communications signal. Unfortunately, this condition is generally not true. In the case where the radar and communications receiver systems are integrated, which we assume in this work, both subsystems demand a large enough signal power-to-noise power ratio (SNR) for their performances to meet specifications. If the SNR for communications is large, and the radar power is assumed to be much larger than the communications power—as in previous work—then the radar SNR becomes impractically

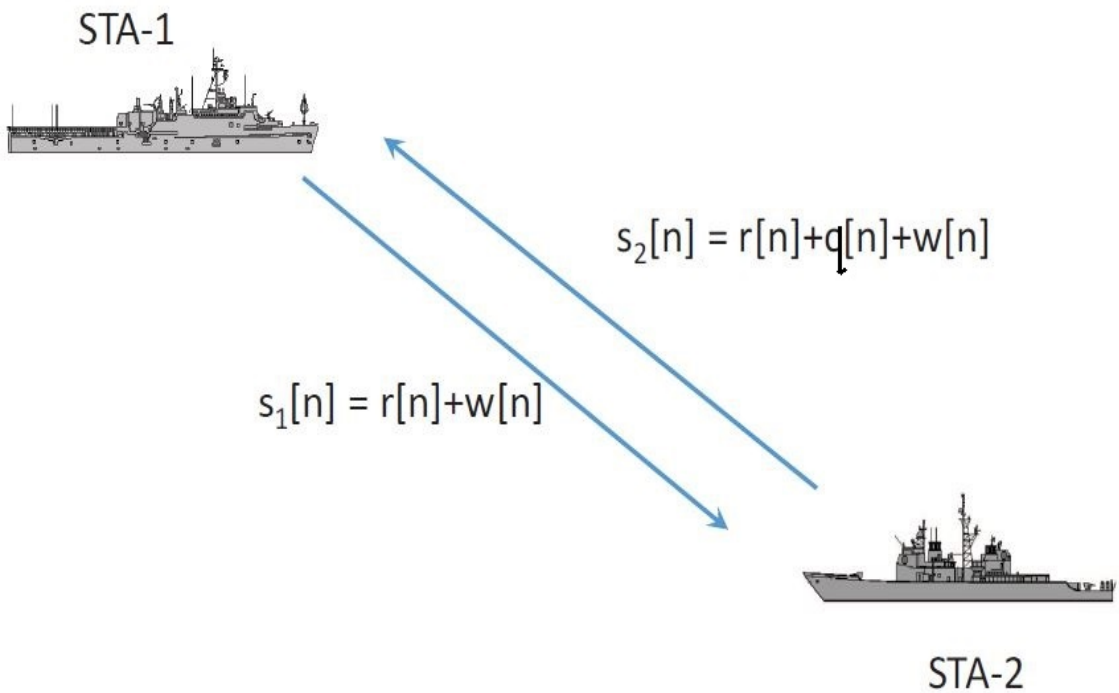

Figure 1.2. A Possible Scenario in Which Embedded Intrapulse Communications Could Be Used as an Embedded Communication Method. Adapted from [5].

large; thus, for the integrated radar-communications receiver, it is prudent to consider cases where the radar power and communications power may not be significantly different, such that the integrated SNR does not become impractically large. It is worth mentioning that, in this thesis, we assume that the radar waveform is existent, and we only design the communications waveform, unlike a "co-design" approach [4]. The term “combined signal” now refers directly to the received additive radar plus communications signal as a result of the embedding. The signal models are more aptly defined in Chapter 2; however, at this juncture, it is expedient to present our model scenario, which axiomatically follows [5] and [6].

1.3 Objective

We expound upon previous work that considers the establishment of a half-duplex communications path [6] as well as the effects of such a communications waveform on the

performance of the radar [5]. We further constrain our focus in this thesis to primarily utilize a more realistic, navigation-like radar pulse as opposed to the idealized, rectangular pulse used in [7]. We also consider the fact that the radar and communications receiver is integrated, unlike in previous works [5]-[7] where they were characterized separately. It is our intent to facilitate further research into a hardware model for a receiver that could be implemented in an FPGA that would be similar to those found in any number of navigation radars. We intend to explore the cybersecurity implications of the implementation of such a receiver into a maritime vessel's internal network. We begin to delve into those implications in this thesis. Secondarily, we discuss modulation and transmission methods for potential further covertness and increased data rate. Following the trend of previous research that influenced this work, we use software simulation in MATLAB and Simulink to support quantitative analysis [5], [6]. We then substantiate the viability of the combined signal by presenting the radar's percentage or probability of detection and the embedded communications' probability of symbol error or symbol error ratio (SER). We impose our combined signal onto a carrier and transmit. Additionally, we discuss AWGN channel parameters associated with our specific implementation.

1.4 Thesis Organization

This thesis is organized into six chapters. In Chapter 2, the signal models for the practical, navigation-like radar pulse waveform and the embedded communications signal are discussed. In Chapter 3, we apply actual radar system parameters and introduce discussion of link parameters. In Chapter 4, results are proffered for percentage of detection of the combined signal via Monte Carlo simulations, and we present a method for calculating an effective embedded signal performance. In Chapter 5, we simulate modulation of the physical combined signal and transmit the signal via hardware. We present conclusions and recommendations for potential future work in Chapter 6.

CHAPTER 2:
Signal Modeling

Relevant signal models presented and discussed in this chapter include the radar, communications, and combined waveforms. We discuss pertinent distinctions from signal representations found in previous work, such as in [5] and [6].

As is mentioned in Chapter 1, our model draws from and builds upon previous work in that we continue the use of the complex-valued baseband model with the received signal defined as $y(t) = r(t) + q(t) + w(t)$, where $r(t)$ is the radar signal and $q(t)$ is the embedded communications signal. In our model, zero-mean additive white Gaussian noise (AWGN) is represented by the $w(t)$ term. Conventional signal processing dictates the utilization of the Nyquist Theorem for analog-to-digital (A/D) sampling, which we use in our establishment of the discrete signal model with assumed normalized sampling time $t_s = 1$. We render the consequent received signal model as

$$y[n] = r[n] + q[n] + w[n], \tag{2.1}$$

where $n = 0, 1, 2, \ldots$.

2.1 The Radar Signal

The radar signal may be viewed as interference of the communications signal and the communications signal may be viewed as interference of the radar signal. Whether $r(t)$ or $q(t)$ is interpreted as interference is dependent on the subsystem being considered. As is discussed in later chapters, certain parametric attributes of the radar and communications signals may have mutually beneficial or detrimental implications for one another [8]. For the purposes of this thesis, we are more interested in the ability to successfully receive and demodulate the embedded communications signal than the coherent detection of the radar pulse at our integrated radar-communications receiver; however, we recognize a practical requirement for adequate performance of reception and detection of both signals.

For the radar waveform, we deviate from the rectangular pulse used in [5]-[7]. Instead, we

apply a practical, navigation-like, radar-pulsed waveform. Some widely-used navigation radar systems utilize magnetrons as power amplifiers for transmission. Such a device can cause significant change to the radar carrier waveform from pulse to pulse, such as slight frequency shifts within a single pulse or between multiple pulses. For convenience in this study, we simply assume the use of a traditional coherent pulse train that is transmitted at a constant pulse repetition interval/frequency (PRI/PRF) while utilizing a pulse shape that is more closely identifiable to that of the generic navigation radar pulse.

We obtained a transmission spectrum from a particular maritime navigation radar system within a reputable and widely-used family of navigation radars. From this data, a scaled representative power spectral density (PSD) was roughly modeled in MATLAB. We subsequently downconverted to baseband and downsampled the model in order to reduce computing resources for Monte Carlo simulations, producing the waveform shown in Figure 2.1. In other words, we intentionally do not use a transmission spectrum from an actual radar system for proprietary reasons. Our motivation is to simply use practical radar pulse shapes in our experiments and simulations instead of idealized rectangular pulses. Indeed, actual power and exact carrier frequencies are not shown to keep the waveform as a representative baseband navigation signal instead of a truly hardware-generated carrier waveform.

In Figure 2.2 the real- and imaginary-valued baseband representation of our unit-energy $r[n]$ pulse are plotted. Note that the time axis in this plot represents normalized time and can, thus, be easily manipulated to a desired pulse interval of any applied radar.

2.2 Communications: The Embedded Signal

For a pulse train, the embedded communications as a QPSK baseband waveform is given by

$$q[n] = \frac{A_q}{\sqrt{N}} \sum_{k=0}^{N-1} u_c[n - kT_r], \tag{2.2}$$

with scalar amplitude A_q, where N is the number of pulses transmitted, T_r is the PRI, and $u_c[n]$ as

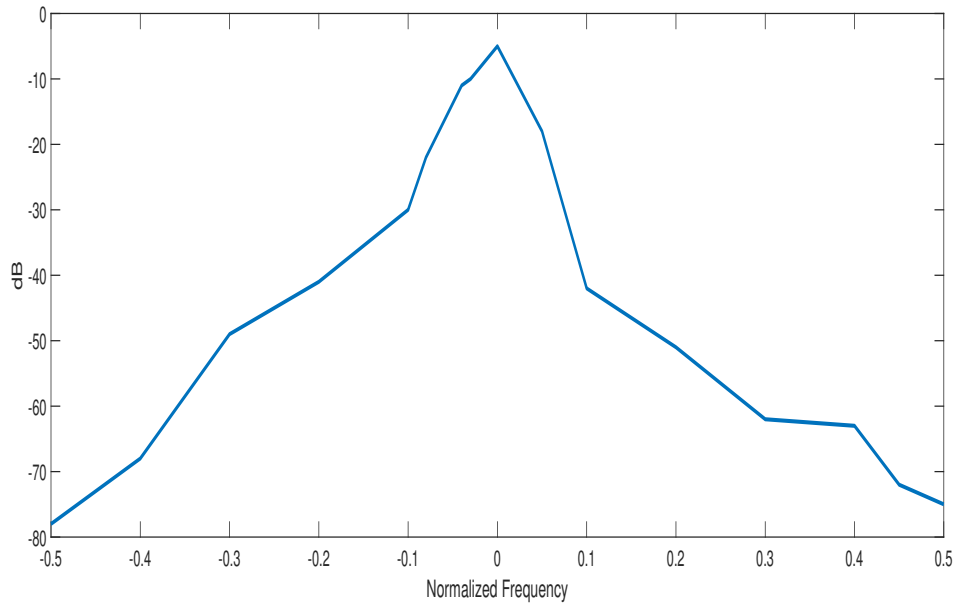

Figure 2.1. Spectrum of a Practical Navigation Radar Pulse Shape Used for Simulations.

$$u_c[n] = \frac{e^{j\phi_q}}{\sqrt{t_p}}(u[n] - u[n - t_p]), \tag{2.3}$$

where ϕ_q is the phase of the embedded signal and t_p is the radar pulse duration. We randomly appropriate symbols from the set $\phi_q \in \left[\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\right]$. Let t_q be the duration of a communications symbol. In (2.2) A_q can be adjusted to the desired energy or power. In (2.3), we assume that t_q is equal to t_p, which indicates that one symbol is embedded in one radar pulse. If more symbols are desired in the duration t_p, then the symbols must be represented by the appropriate number of samples in the radar pulse. For example, if we desire one symbol per sample in t_p, then each phase ϕ_q corresponding to each symbol in (2.3) occupies a sample duration; thus, the relation of t_q to t_p dictates the number of symbols that can be embedded in a radar pulse.

Each symbol's phase, taken from within the above defined set, is randomly chosen for each symbol for our simulations. Due to normalized time, the minimum symbol duration possible is $t_q = 1$. In our simulations, the radar pulse is 17 samples in length; thus, the maximum number of unique symbols that can be embedded in a radar pulse is 17. We can,

therefore, have various symbol rates within a radar pulse by varying symbol duration. The symbol-rate-to-bandwidth ratio (SRBR) ratio is given by

$$SRBR = \frac{R_s}{B_r}, \tag{2.4}$$

where $R_s = 1/t_q$ is symbol rate and $B_r = 1/t_p$ is the radar pulse bandwidth.

The QPSK radar-to-communications power ratio (RCR) is an important aspect for determining various factors in our simulations. We parametrize the RCR such that we can calculate the powers and/or energies of the radar and communications signal, recognizing that the communication symbols are transmitted coincident with the active time of the radar pulse. The RCR in dB is $RCR_{dB} = 10\log_{10}(P_r/P_q)$, where P_r and P_q represent the power of the radar and communication signals, respectively, such that the actual $RCR = P_r/P_q$.

Throughout this work, we use various values for SRBR. In order to put into perspective the relationship between the communications SNR and the RCR, from $RCR = P_r/P_q$ we get

$$RCR = \frac{E_r/t_p}{E_s/\frac{t_p}{SRBR}}, \tag{2.5}$$

where E_r is radar energy, E_s represents the energy in a communications symbol, and t_p is effectively the duration of the combined signal. Simplifying (2.5), we have

$$RCR = \frac{E_r}{(SRBR)E_s}, \tag{2.6}$$

from which we can see that $E_r = (SRBR)(E_s)(RCR)$. It is well known that communications $SNR = E_s/\sigma^2$, where σ^2 is noise variance. In our simulations, we set $\sigma^2 = 1$.

2.3 Combined Signal: Radar and Communications

In the example shown in Figure 1.2 we represent the signal, as transmitted by STA-1, with the equation $s_1[n] = r[n] + w[n]$, where $w[n]$ is the generic noise representation. STA-2 embeds the communications signal $q[n]$ in the radar return, or radar echo, such that the combined signal is clearly $r[n] + q[n]$, which we refer to as $C[n]$ when convenient. The received signal in STA-1 is represented by $s_2[n] = C[n] + w[n]$, where $w[n]$ is noise in

STA-1 receiver.

The effect of RCR and $SRBR$ parameterizations on the combined signal can be most expediently illustrated by presenting the plot of a single pulse of the in-phase component at baseband. In Figure 2.3, we normalize the radar pulse's energy, hold the power of the radar P_r constant, decrease the power of communications P_c, which results in an increase of RCR_{dB} to values 0, 3, and 10. The decrease in communications' energy between plot (a) and plot (c), the lowest and highest RCR values, can be clearly noted. As RCR increases to $RCR_{dB} = 10$, P_c has been substantially decreased and the combined signal is more true to the original radar pulse. The SRBR is held constant at 17 in Figure 2.3. Due to the random assignment of the embedded symbols, the communications waveform for each RCR is clearly different.

In order to examine the direct effect of SRBR on the radar pulse within its time duration, we compare the combined signal with the radar pulse by applying the values of of $t_q = 1$ and $t_q = 17$. In this thesis, the values of 1 and 17 are, respectively, the minimum and maximum values used for t_q. The RCR is held at a constant value of 3 dB. In Figure 2.4(a) we can observe a similar result as in Figure 2.3(b), with the phases of all 17 samples obviously being affected. By contrast, the effect of embedding one symbol ($t_q = 17$) throughout the duration of the pulse is illustrated in Figure 2.4(b). In the $SRBR = 1$ case, the amplitude of the real part of the combined signal can either be lower or greater than that of the in-phase of the radar pulse; however, the total effect on the whole combined signal also depends on the quadrature part of the embedded symbol.

By adjusting the symbol duration t_q, which changes the SRBR, we can effectively modify the data rate of the transmission. In this application, the communication symbols are only transmitted during the active time of the radar pulse and while the receiver receives the radar echo to maintain silence during the off time of the radar return. Specific synchronization techniques and methods of embedding are beyond the scope of this work. Symbol duration has direct bearing on the total number of symbols transmitted based on the number of pulses received. In Chapter 3, we apply operational parameters of an actual navigation radar to better conceptualize and provide context for the implications discussed here.

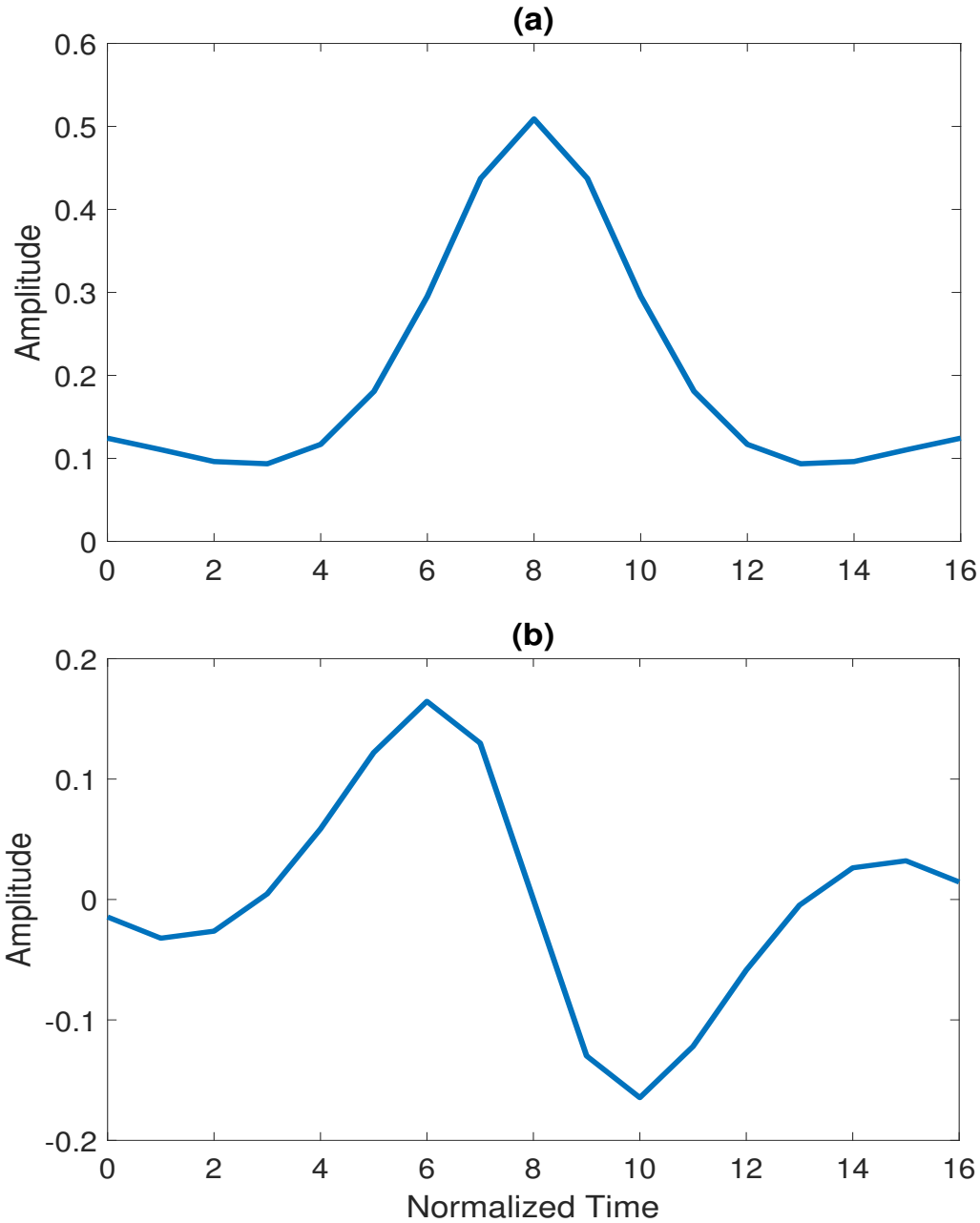

Figure 2.2. Real (a) and Imaginary (b) Components of the Modeled Navigation-Like Radar Pulse.

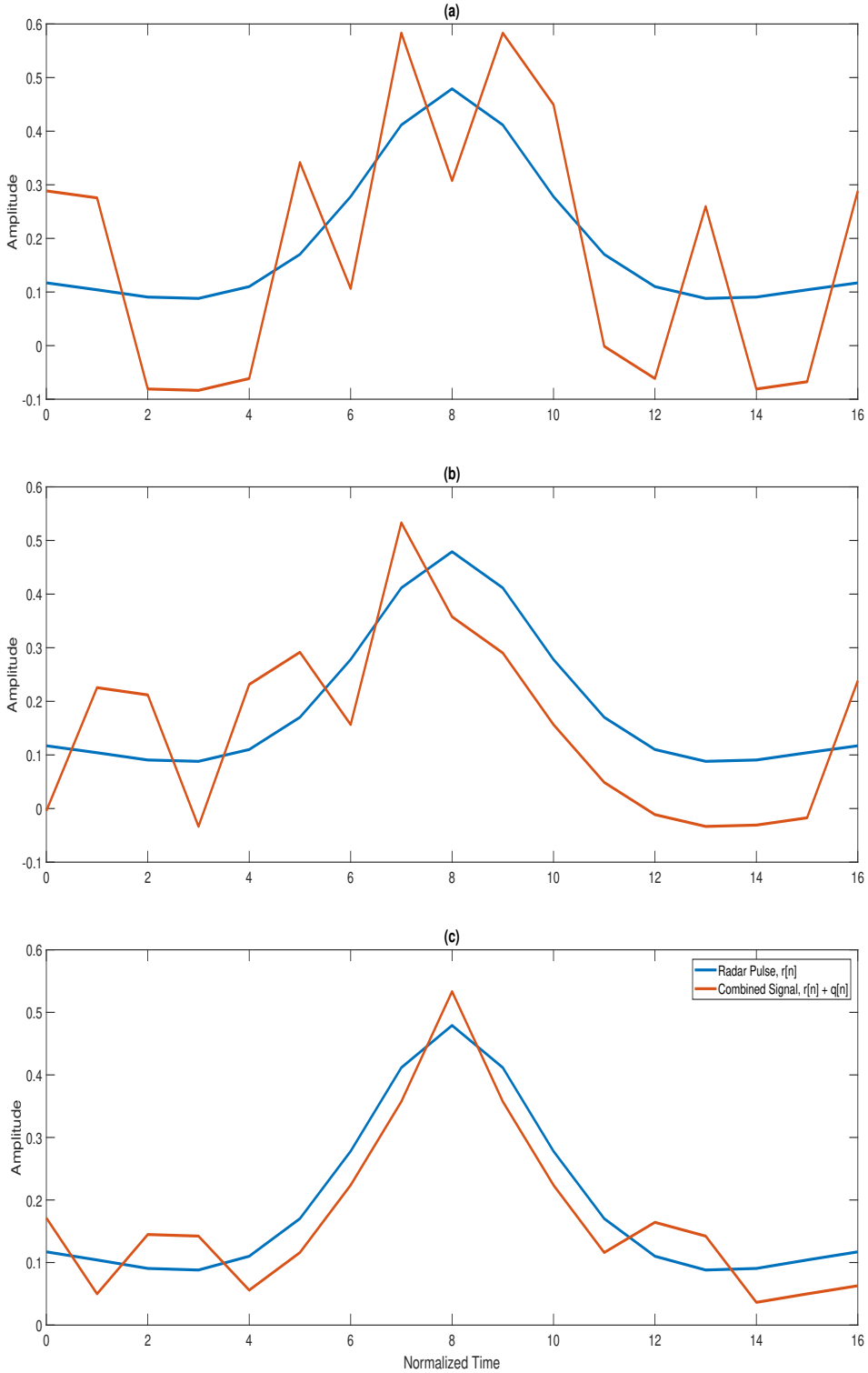

Figure 2.3. The In-Phase Component of the Combined Signal Compared to the Radar Pulse, with (a)$RCR_{dB} = 0$; (b)$RCR_{dB} = 3$; and (c)$RCR_{dB} = 10$. $SRBR = 17$.

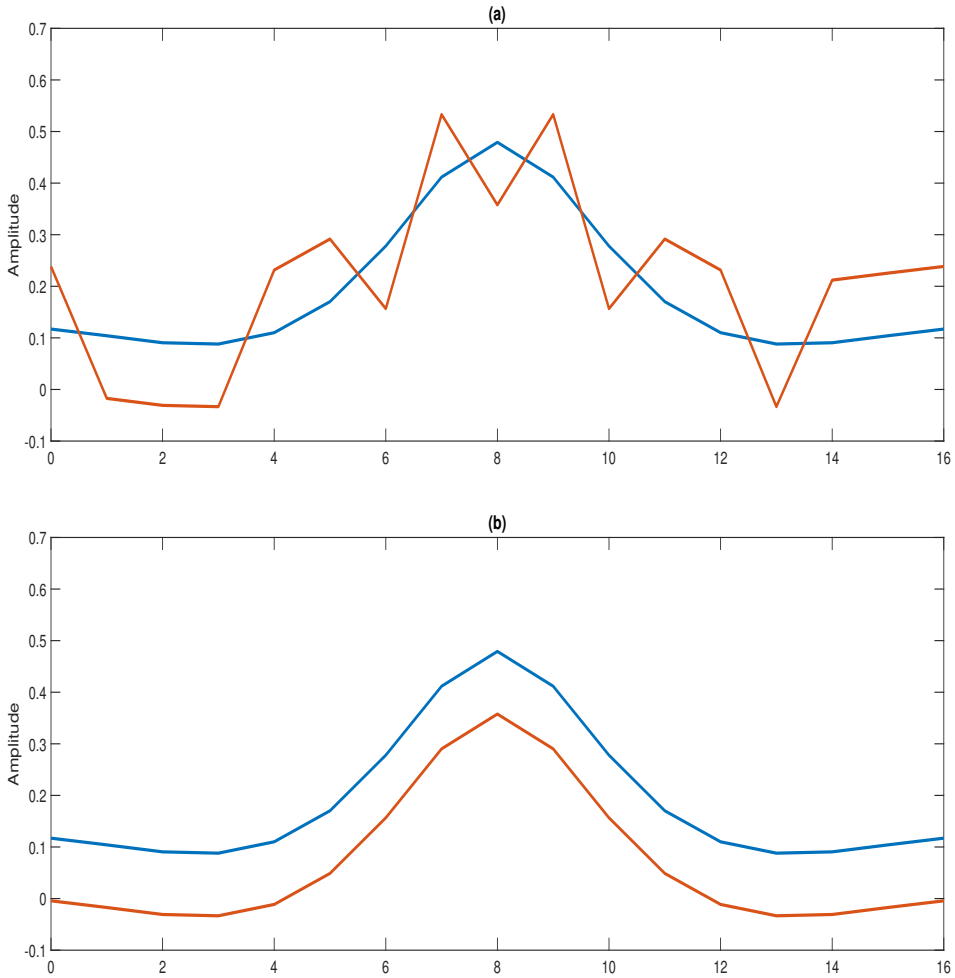

Figure 2.4. The In-Phase Component of the Combined Signal Compared to the Radar Pulse, with (a)$SRBR = 17$; and (b)$SRBR = 1$. $RCR_{dB} = 3$.

CHAPTER 3:
Application of System Parameters

Our exploration of the combined signal requires us to study the properties of the combined waveform and the integrated radar-communications receiver, along with the operative channel. The parameters to be investigated include transmit power, bandwidth, data rate, and error rate. Considering our concomitant method of transmission, we naturally expect degradation and subsequent error of the communication symbols along with degradation of the channel capacity or symbol rate throughput [8].

In the second section of this chapter, we continue our investigation by generalizing methods to calculate symbol rate throughput for our system.

3.1 Calculation of Effective Channel Throughput

The work in [9] delves into the dynamics between a rotating narrowbeam antenna and an antenna with omni-directional receive capability. We adapt this model to our application to demonstrate the characteristics inherent in this unique communication link to facilitate enhancement of the discussion in future work. A significant aspect that merits investigation within our system is how the particular beam pattern of the radar affects the communication channel capacity. There certainly exist numerous other potential impairments that pose a detriment to the channel throughput, some of which are explored in previous works, such as [5] and [9]. An example of such an impairment is the inability of the receiver to resolve paths within a sampling interval—a fading channel; however, the implications of the multipath fading environment are not thoroughly treated in this work but are briefly addressed in ensuing discussion. It is prudent to understand how the attributes of the radar can directly affect the system's ability to transmit data symbols. For example, information about the beamwidth of the transmitter can actually be utilized to gain a sense of the symbol rate throughput of the system [9].

3.1.1 Effect of Physical System Attributes to the Communications Link

The significance and implications of the two systems occupying the spectrum in a synchronous manner has already been substantially highlighted. We observe that both the existence of AWGN in the channel as well as the radar transmission impose interference upon the communications waveform. On the other hand, we also want to quantify the effect of the embedded communications to the radar's probability of detection at the receiver. In the following section, we seek to explore these considerations utilizing a specific navigation radar's specifications as projected onto the viability of embedded communications symbols in said navigation radar pulse.

The embedding of communications symbols into the radar pulse requires modifications to the radar system if it were to receive the communications transmission (i.e., the integrated receiver) or the use of an additional communications receiver, which can potentially be implemented separately for the sake of not modifying the legacy radar receiver. Development of the communications channel must account for physical operating characteristics of the radar relative to the communication link, especially that of the navigation radar's tendency to employ a rotational antenna. This attribute complicates our channel such that the communications link is essentially not closed when the receiver is not in the communication path of the transmitter, i.e., when the radar is not illuminating the target receiver.

3.2 Navigation Radar System Parameter Application

It is crucial to have some sense of the data rate throughput limitations of a given radar system in order to realize the potential as well as the ramifications of system implementation. The approach presented here represents an initial and basic treatment of fundamental radar system knowledge combined with parameters for an actual navigation radar that were acquired from specifications (later shown in Figure 5.6). The choice of this system is solely for illustration. The analysis here should also apply to other navigational radar systems. The model of navigation radar selected for this experiment is the Furuno FAR-2117BB, which is a pulsed-wave radar with medium PRF. We consider the aforementioned rotational antenna and use the term dwell time to refer to the radar time on target, which we define as

$$t_{ot} = \frac{\theta_B}{\dot{\theta_S}}, \tag{3.1}$$

where θ_B represents half power beamwidth and $\dot{\theta_S}$ represents beam scan rate in degrees. We, therefore, have

$$\theta_B \approx \frac{\lambda}{D}, \tag{3.2}$$

where D represents the diameter of the transmitting radar antenna aperture and $\lambda = c/f$ is the carrier wavelength.

We can now define the number of pulses that hit the target as

$$n_B = t_{ot} f_p, \tag{3.3}$$

where f_p is the radar PRF, which is the reciprocal of interpulse period T_r. The beam scan rate $\dot{\theta_S}$ can be represented in revolutions per minute (RPM) as ω_s.

Finally, an example scenario can be calculated utilizing the FAR-2117 specifications. For X-band, $\omega_s = 24$ RPM, which we convert to $\dot{\theta_S} = 144$ deg/s. Applying (3.1), we have

$$t_{ot} = \frac{1.9\,\text{deg}}{144\,\text{deg/s}} 13.19\,\text{ms}. \tag{3.4}$$

Now, the number of pulses that will hit the target can be calculated as

$$n_B = (t_{ot})(3000\,\text{pulses/s}) = 39.582\,\text{pulses}. \tag{3.5}$$

The pulse duration for the FAR-2117 is given as $t_p = 0.07\mu$s, and we have previously established our normalized, simulated pulse duration of length 17. We can, thus, calculate the required time of the symbol duration as

$$t_q = \frac{t_p}{17} \approx 4.118\,\text{ns}. \tag{3.6}$$

At maximum capacity, our system transmits at a throughput of 672.92 symbols per illumination, which equals 51000 symbols per second.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4: Effective SER for Embedded Communications and Probability of Detection for Radar

The SER results for the embedded communications and radar's percentage or probability of detection are presented in this chapter. Our radar signal is created by developing the model of a practical navigation radar pulse, which we subsequently implement in MATLAB and Simulink. To accomplish the Monte Carlo simulations needed to produce SER results, the QPSK symbols are randomly generated to simulate the transmission of data via the embedded signal. The objective of this chapter is to parameterize RCR and SRBR and observe their effects on SER and P_D.

4.1 Radar and Communications Waveform Development

We first develop a radar pulse that can be implemented for our application as described. As we have mentioned, previous work had implemented an idealized rectangular-shaped pulse for simulations. Considering that the intent of this work is dedicated to the realization of operational implementation of the topics discussed herein, it is expedient to model our waveform based on a practical navigation radar power spectrum.

To review, we form a more realistic radar waveform by utilizing an actual power spectrum from a particular navigation radar system. Actual navigation spectral plots from a particular system may be deemed proprietary, so we simply developed a rough estimate of the spectrum. A further modification was to sample the spectrum to reduce the number of samples in a pulse to perform Monte Carlo simulations with reasonable duration. It is rather important to highlight that this first step of progress merely scratches the surface of the additionally intense investigations that can be explored in order to fully get a sense of how maritime communications can be operationalized and improved by utilizing these methods. Indeed, it should be noted again that the waveform pulses produced by a magnetron, which is used by some navigation radars, actually slightly vary from pulse to pulse since the magnetron is a non-coherent device that causes a slight shift between the instantaneous phase of each pulse. Phase noise, or deviations due to the magnetron, is beyond the scope of this work;

hence, we allow identical duplication for each radar pulse in the combined signal. The effect of phase noise on SER is also beyond the scope of this work.

To form a pseudo-navigation radar pulse inspired by a true magnetron spectrum, we estimated the data points of the power spectrum; moreover, the spectrum is downconverted to baseband so as not to reveal actual radar carrier frequencies. As mentioned, we further modify the waveform by downsampling the spectrum in which the resulting waveform spectrum is shown in Figure 2.1. It is important to note that the resulting pulses used in our experiments are obviously not exact copies of downconverted magnetron pulses. Our motivation is simply to use practical pulse shapes rather than the rectangular pulse shapes used in previous works. The radar pulses used in this thesis are at least inspired by practical radar spectra for the operational considerations mentioned in this work. The result of these operations is the baseband representation of our designed radar pulse $r[n]$.

The QPSK symbols that form the embedded communications signal $q[n]$, along with AWGN signal, were expounded upon in previous sections. It is sufficient to mention that, for the embedded signal, the number of total symbols transmitted in the simulated experiments is a function of the number of radar pulses transmitted and $SRBR$.

4.2 Combined Signal Detection via Radar Waveform

The discussion in Chapter 3 alludes to the necessity of detection of the radar signal in order for communications between the transmitting and receiving stations to be successful. This is because using maximum-likelihood detection (MLD) for QPSK does not work for the combined signal because of the radar interference with modest or large RCR. In other words, the communications receiver has to detect the radar pulse first to deem that there is embedded communications. Modest or even large RCR does not guarantee 100% detection. When a radar pulse with embedded communications is missed, then the whole symbol sequence is lost. Here, we derive an "effective SER" that intrinsically relates the error rate of the embedded signal with that of the probability of detection of the combined signal.

In order to meet this objective, other specifications must be considered. In the following sections, the factors considered are probability of false alarm P_{FA} and the corresponding radar receiver threshold. For simulations, the percentage of detection is given by

$$P_D = \frac{D_P}{P_{TX}}, \tag{4.1}$$

where D_P represents number of detected pulses and P_{TX} represents the total number of pulses transmitted.

The theoretical probability of detection is given by [10]

$$P_D = Q\left(Q^{-1}(P_{FA}) - \sqrt{\frac{2E_r}{\sigma^2}}\right), \tag{4.2}$$

where σ^2 represents noise variance, E_r is the energy contained in the radar signal, and $Q^{-1}(\bullet)$ denotes the inverse Q-function [10].

An appropriate threshold γ' is calculated by [10]

$$\gamma' = \sqrt{\frac{\sigma^2 E_r}{2}} Q^{-1}(P_{FA}). \tag{4.3}$$

Thus, we observe that P_{FA} is linked to P_D by the particular, chosen value of the threshold.

4.2.1 Discussion of Radar Matched Filtering

A matched filter detection method is implemented, wherein we match exclusively to the radar pulse since the communications component of the integrated receiver, by definition, does not know the embedded signal a priori. This is the most practical assumption in an operational environment, where the receiving station is assumed to have a priori knowledge of the radar pulse. It goes without saying that the embedded communications waveform will have an effect on performance of the radar. We note, as [6] discusses, that the embedded signal slightly degrades the probability of detection with this implementation of matched filtering. In this way, the embedded signal is precisely an interference to the radar signal. Consequent to this perspective, it behooves us to investigate how the reduced P_D bears directly on $q[n]$ at the receiving station.

Clearly, the matched filter is matched to the pseudo-navigation radar pulse shown in Figure 2.1. By convention, it should be understood that radar signal-to-noise ratio is not fully

maximized due to the embedded signal. If the received signal is $S_2[n] = C[n] + w[n]$, where we recall $C[n] = r[n] + q[n]$, then the filter output [11] is given by

$$y[n] = \sum_{k=-\infty}^{\infty} r^*[n-k]S_2[k], \tag{4.4}$$

where $*$ denotes the conjugate operation.

4.3 Demodulation of Embedded Signal

If the radar pulse is detected, then we deem that there is embedded communications. Then we can subtract the radar signal from the received signal in (4.4) to get an estimate of the communications and noise signal designated with $q'[n]$. If the radar pulse is missed, then the communications symbols are also missed. Due to noise and subtraction, we expect that $q'[n] \neq q[n]$. The MLD approach to demodulation is utilized to detect which symbol is transmitted to generate SER curves in terms of SNR. The MLD reduces to a bank of four filters, with each filter matched to a particular QPSK symbol. The MLD assumes knowledge of the modulation of the embedded signal as in practice.

Each filter is assigned an index $X \in \left[1, 2, 3, 4\right]$ corresponding to $\phi_q = \left[\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\right]$. Thus, each filter returns an output value after the received signal passes through the filter bank. The detector chooses the symbol index corresponding to the matched filter that returns the maximum output, where the index 1, 2, 3, or 4 (i.e., one of the possible phase states ϕ_q), indicates the symbol decision by the receiver.

The standard metric for measuring and comparing performance of communications signals is SER. We calculate SER such that the number of symbol errors is divided by the total number of symbols sent. As mentioned, SER results are obtained by performing Monte Carlo (MC) simulations. We can easily derive a general formula to determine total number of symbols Q_{tot} in our simulation

$$Q_{tot} = (P_{TX})(SRBR). \tag{4.5}$$

For example, in the case of $SRBR = 17$ with 10,000 pulses transmitted, the number of total of symbols transmitted is 170,000.

In Figure 4.1, we present SER results while varying SRBR with $RCR_{dB} = 20$ (for the large RCR case). Note that SER closely follows the theoretical QPSK SER regardless of SRBR used. We recall that such high RCR is impractical for an integrated radar-communications receiver. For example, if we require a SER corresponding to E_s/N_0 of 13 dB (where N_0 is the noise PSD), then the radar-to-noise power ratio needed is 33 dB! Thus, we have to investigate modest RCR from an integrated receiver to be implementable.

4.4 Probability of Detection

The performance metric in terms of the detection of the radar signal and, consequently, the combined signal, is the probability/percentage of detection P_D. From the perspective of the radar, it is only concerned about the effect of the embedded communications on P_D. The communications receiver, however, is interested in both P_D and SER since it effectively uses the radar pulse in order to determine if embedded communications symbols are present. In other words, the communications receiver is eventually interested in demodulating the embedded signal rather than to simply detect a target.

Just like SER, P_D is determined by performing MC trials. As previously discussed, the total number of symbols transmitted in our simulations is a function of the SRBR and P_{TX}. The P_D (corresponding to $P_{FA} = 10^{-5}$) results as a function of decreasing SRBR is shown in Figure 4.2, where the number of symbols transmitted ranges from 10,000 to 170,000 and RCR is held constant at $RCR = 0$ dB. At $SRBR = 17$, P_D is clearly higher at 13 dB as compared to the lower $SRBR$ values in (b) and (c). We also see that P_D in all three cases is reduced by the embedded communications but is mitigated by increasing $SRBR$. When SRBR is increased, the bandwidth of the communications signal is increased. The increase in bandwidth actually reduces the spectral overlap with the radar, which results in P_D improvement.

Notice in Figure 4.2 that P_D is close to unity for high radar SNR (16 dB or greater) as is expected since 16 dB means that the radar power is 40 times greater than the noise power in the receiver. It should be noted that P_D plots represented in Figure 4.2 do not depict detection error rate or percentage of missed detections P_{MD}. In other words, more insight can be gained and performance comparison can be investigated by plotting P_{MD}. We show these results as complement to the SER plots, shown adjacently in Figures 4.3-4.5. As

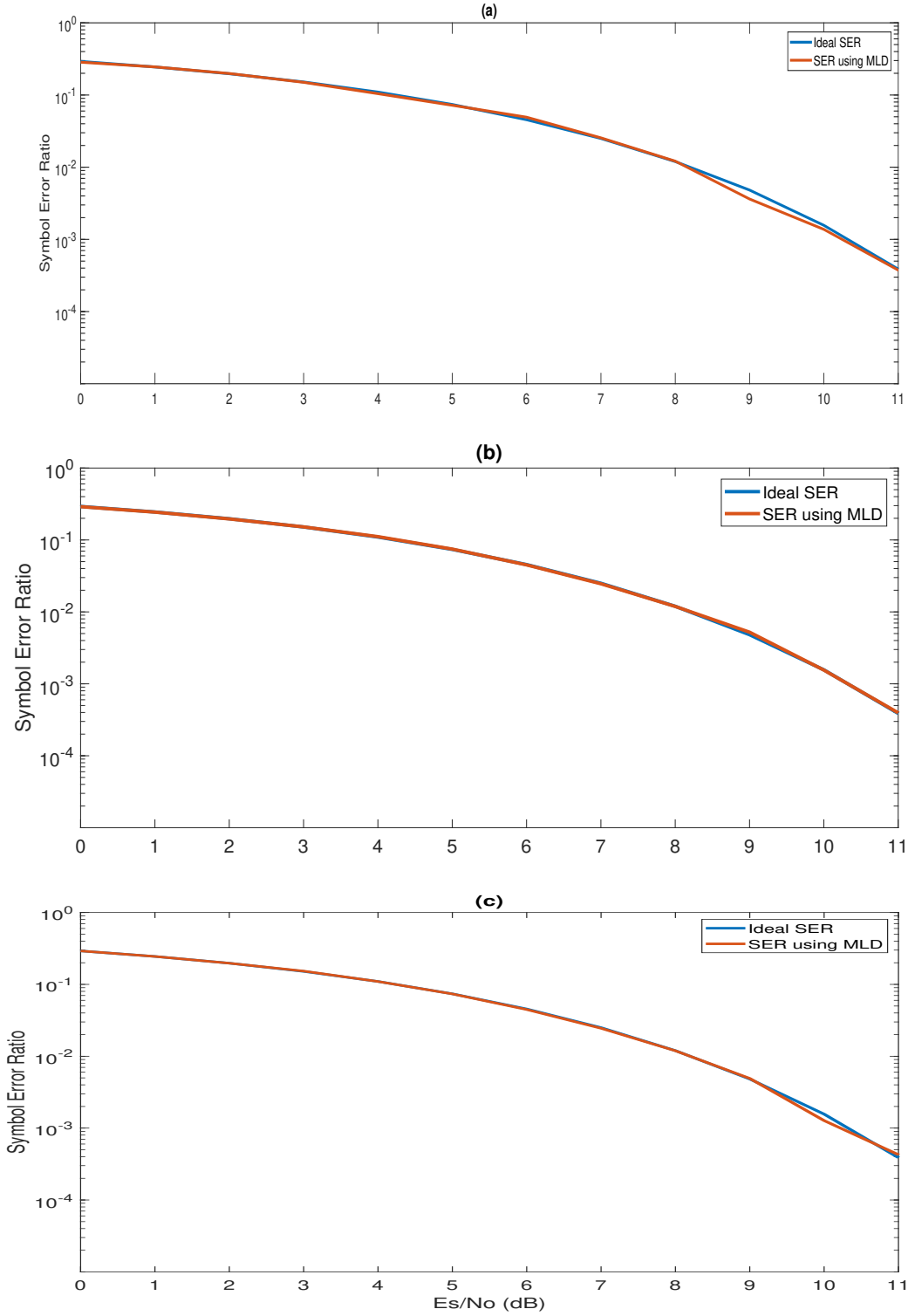

Figure 4.1. The SER Plots of Ideal QPSK vs Demodulated Embedded Signal with RCR Held Constant at $RCR_{dB} = 20$. (a)$SRBR = 1$; (b)$SRBR = 2.125$; (c)$SRBR = 17$. $P_{FA} = 10^{-5}$.

previously stated, the P_D for higher $SRBR$ is greater than the P_D for lower $SRBR$ as seen in 4.2; however, we must clarify that the P_D of the radar pulse interfered by the embedded signal is actually degraded in relation to the theoretical P_D. This is easily observed in the P_{MD} plot. This can be observed in Figure 4.3(b), where $SRBR$ is increased from $SRBR = 1$ to $SRBR = 2.125$. In spite of the fact that embedding communications degrades the P_D, we see that this degradation is mitigated by increasing $SRBR$.

4.4.1 Derivation of Effective Symbol Error Rate

A key addition to our performance results is to include those symbols that are lost in undetected radar pulses within the calculation of embedded signal SER performance. We refer to the metric as "effective SER (eSER)." In our results, we calculate eSER from

$$eSER = SER + \frac{(1 - P_D)Q_{tot}}{Q_{tot}}, \tag{4.6}$$

where Q_{tot} is the total number of symbols transmitted, P_D is the probability of detection of the combined signal, and SER is the calculated SER of the transmitted communications signal. The resulting $eSER$ accounts for the communications symbols lost due to missed detection of the combined signal by the radar matched filter due to the specified P_{FA} constraint; thus, we have developed a performance metric suitable for our application.

Recall that in our simulations $SRBR = 1$ means that the number of samples for one symbol equal the number of radar samples in one pulse. Due to the high number of samples needed for $SRBR = 1$, we are only able to produce 10^{-4} error ratio at $P_{TX} = 10,000$. With $SRBR = 1$, we found that any error rate less than 10^{-4} takes an inordinate amount of time – on the order of hours or even days. So any subsequent error rate results presented in this chapter for $SRBR = 1$ do not go beyond 10^{-4}.

4.4.1.1 Vary SRBR

The results of varying the SRBR, with RCR held constant at $RCR_{dB} = 0$ for $P_{FA} = 10^{-5}$, are shown in Figure 4.3. We again note that the increase in SRBR directly improves the performance of the combined signal. Recall that this is due to the fact that the increased symbols actually increase the communications bandwidth, which lessens the radar's effective interference since the radar's bandwidth remains constant. For the same reason, this

benefit extends to the radar's P_D as well; it also increases proportionally with SRBR, as we observed in Figure 4.2. As we previously discussed, $r[n]$ and $q[n]$ suffer from mutual interference, but this interference is mitigated by increasing SRBR (as the modest RCR is held at a constant value). As we return our attention to Figure 4.3, observe that the increasing the SRBR causes the eSER curve of the embedded communications signal to more closely follow the theoretical QPSK curve. As the communications SNR increases to 10 dB, when the $SRBR = 2.125$ as shown in Figure 4.3(b), our eSER converges to the theoretical QPSK SER.

4.4.1.2 Vary RCR

Although not shown in Figure 4.3, we can already generalize that higher SRBR (such as $SRBR = 17$) produces higher quality eSER. We already know that high RCR (with a correspondingly large SRBR) also produces sufficient eSER, as shown in Figure 4.1. Since our receiver is now fully integrated, we are interested in modest (or even low) RCR, which would be practical, in order to see the effect on eSER with high SRBR. In Figure 4.4, the eSER and corresponding P_{MD} at $SRBR = 17$ for $RCR_{dB} = -3$ and $RCR_{dB} = -6$ are shown. Notice the increase in SER performance for an effective 3 dB increase in communications signal as RCR decreases from −3 dB to −6 dB. It should be noted that the case of $RCR_{dB} < 0$ indicates the power of the communications overpowers that of the radar, that is $P_c > P_r$. This explains the increase of SER performance and the simultaneous decrease in the P_D of the combined signal. In other words, a great deal of trade-off exists between SRBR, RCR, SER, and P_D, given a P_{FA} specification.

4.4.1.3 Vary P_{FA}

Taking $SRBR = 17$ and $RCR_{dB} = -3$ from above, we investigate the eSER results for $P_{FA} = 10^{-2}$ and compare the results to $P_{FA} = 10^{-3}$. The results for this experiment are displayed in Figure 4.5, where the effects of large SRBR are shown to offset the decrease in RCR as well as the decrease in P_{FA}. The result of sufficient SRBR and RCR is necessary in an environment where P_{FA} is decreased, as this factor has subtle repercussions on the P_D and, thus, the eSER. Notice that as P_{FA} improves, P_D slightly lowers. This result is expected because of the missed radar pulses due to effectively raising the receiver threshold value γ' as a result of improving P_{FA}. Similarly, the eSER is slightly degraded because of the communications symbols missed in those lost radar pulses as a result of the higher γ'.

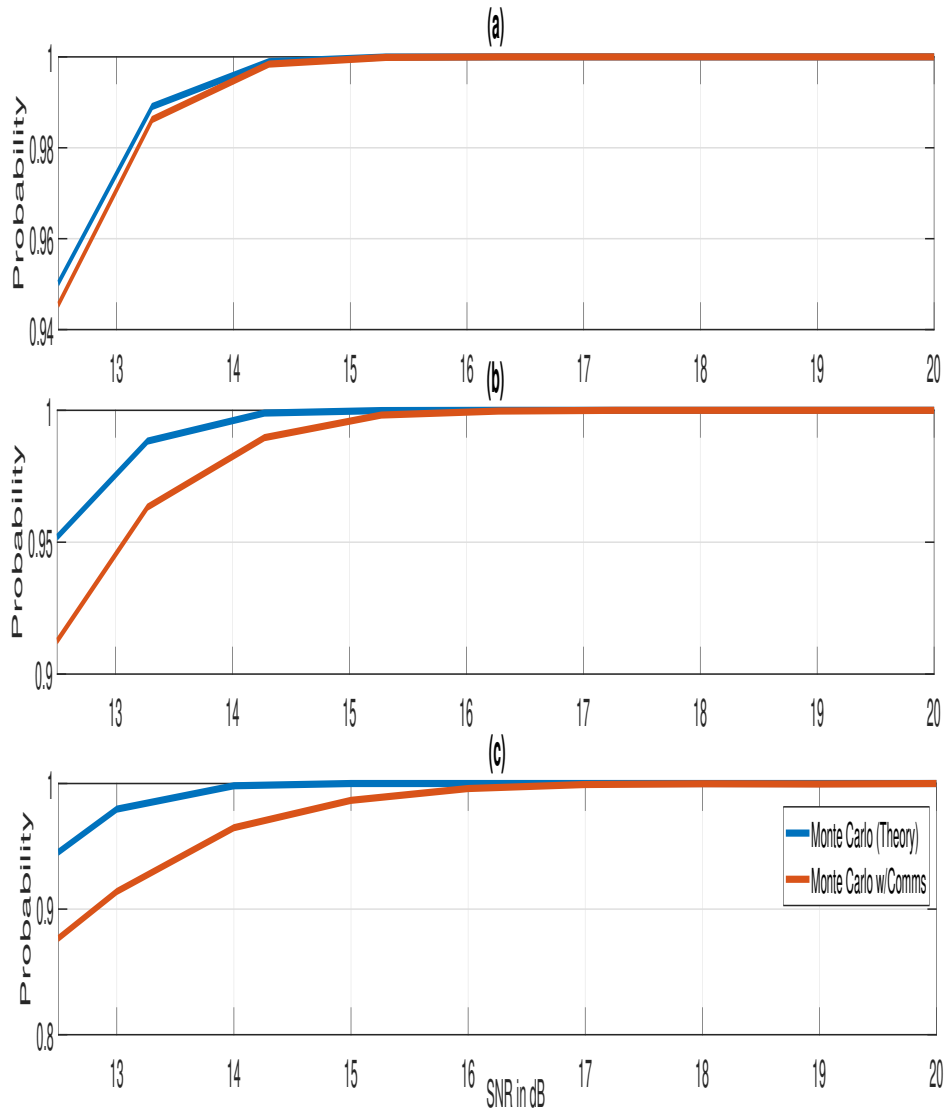

Figure 4.2. Probability of Detection Plots Shown for (a)$SRBR = 17$; (b)$SRBR = 2.125$; (c)$SRBR = 1$. RCR is held constant at $RCR_{dB} = 0$. $P_{FA} = 10^{-5}$.

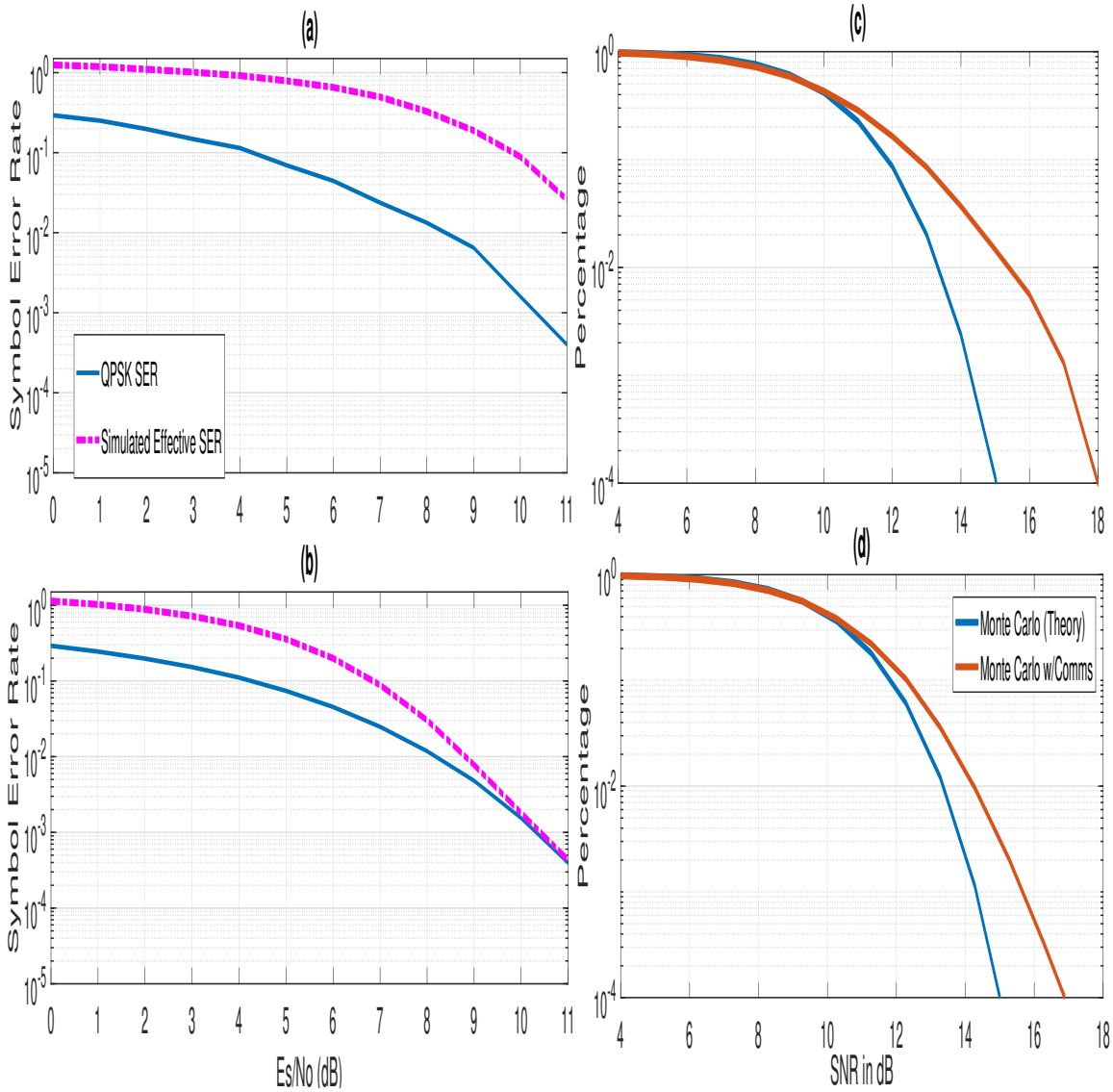

Figure 4.3. The eSER Plotted Alongside Corresponding Percentage of Missed Detection with RCR Held Constant at $RCR_{dB} = 0$ and $P_{TX} = 70000$. $P_{FA} = 10^{-5}$. (a)$SRBR = 1$; (b)$SRBR = 2.125$; (c)P_D for (a); (d)P_D for (b).

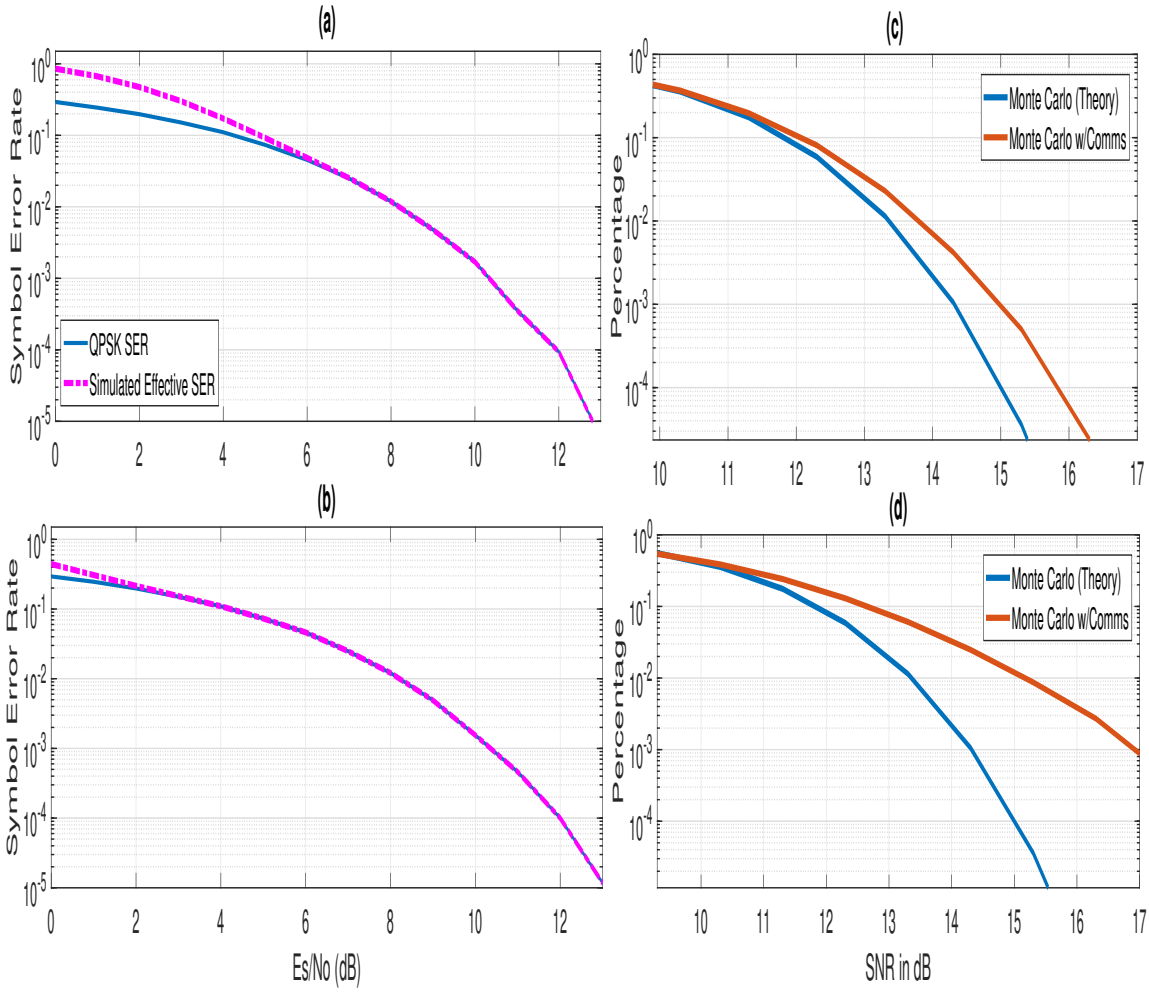

Figure 4.4. The eSER Plotted Alongside Corresponding Percentage of Missed Detection with SRBR Held Constant at $SRBR = 17$ and $P_{TX} = 10000$. $P_{FA} = 10^{-5}$. (a)$RCR_{dB} = -3$; (b)$RCR_{dB} = -6$; (c)P_D for (a); (d)P_D for (b).

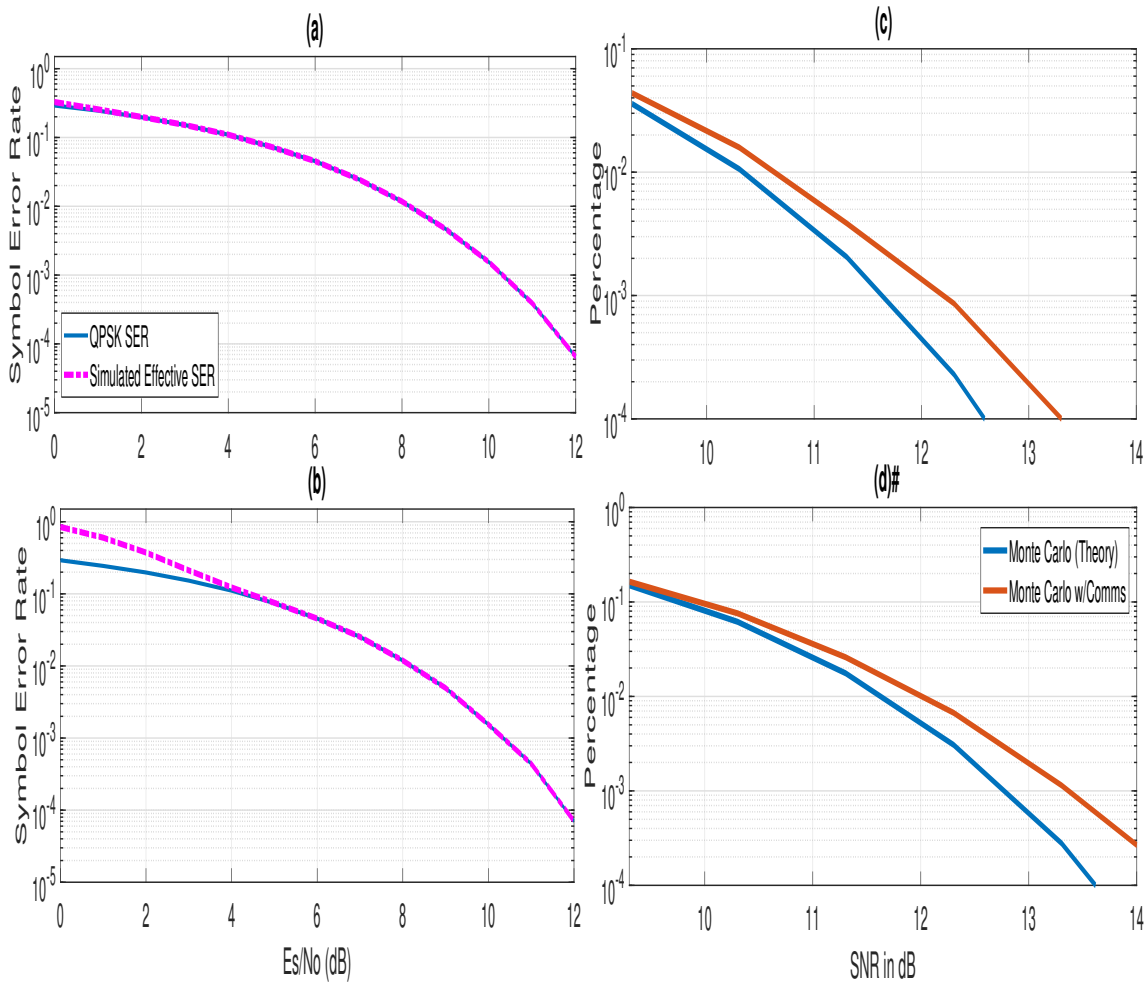

Figure 4.5. The eSER Plotted Alongside Corresponding Percentage of Missed Detection, Comparing the Consequences of Varying P_{FA} with Conditions: $RCR_{dB} = -3$; $SRBR = 17$; and $P_{TX} = 10000$. (a)$P_{FA} = 0.01$; (b)$P_{FA} = 0.001$; (c)P_D for (a); (d)P_D for (b).

CHAPTER 5: Practical Considerations for Radar Parameter Application, Signal Transmission, and Fading Channel

In this chapter, generation of the combined signal on a frequency carrier for actual transmission is presented. The carrier waveform is simulated in software as well as generated and transmitted in hardware. We also include discussion from Chapter 3 and apply specific radar parameters. We conclude the chapter with a deliberation on the inherent risk of implementation based on cyber concerns and the nature of the MCD.

5.1 Simulation Utilizing Actual Radar Parameters

In order to establish the practicality of the combined signal, it is expedient to formulate a realistic modulation of the combined signal that is based upon our heretofore discussed notional waveform which invokes actual radar parameters. Furthering our discussion of channel capacity in Chapter 3, here we develop a simulation that implements specifications close to that of Furuno FAR-2117 navigation radar. The pertinent parameters considered here are PRF and pulse duration t_p. To program the signal generator, we must also calculate pulse bandwidth BW, sample time t_s, and sampling frequency f_s. The system specifications are taken from [13], as shown in Figure 5.6. The practical sample time is calculated as

$$t_s = \frac{t_q}{10}, \tag{5.1}$$

and $t_q = t_p/17$ (for maximum SRBR), where t_p is equal to the specified pulselength in μs.

We generate a combined signal with parameters of $RCR_{dB} = 20$ and $SRBR = 17$. These values are chosen to produce a waveform that is well-suited for discussion. For comparison, we also generate the $RCR_{dB} = 3$ result, with SRBR held constant at 17 in Figure 5.2. The result of imposing the combined signal on a carrier wave, with established radar specifications, is plotted and shown in Figure 5.1, wherein the main lobes at the carrier frequencies, 500 and 800 MHz, can be clearly seen. Both positive and negative frequencies are shown.

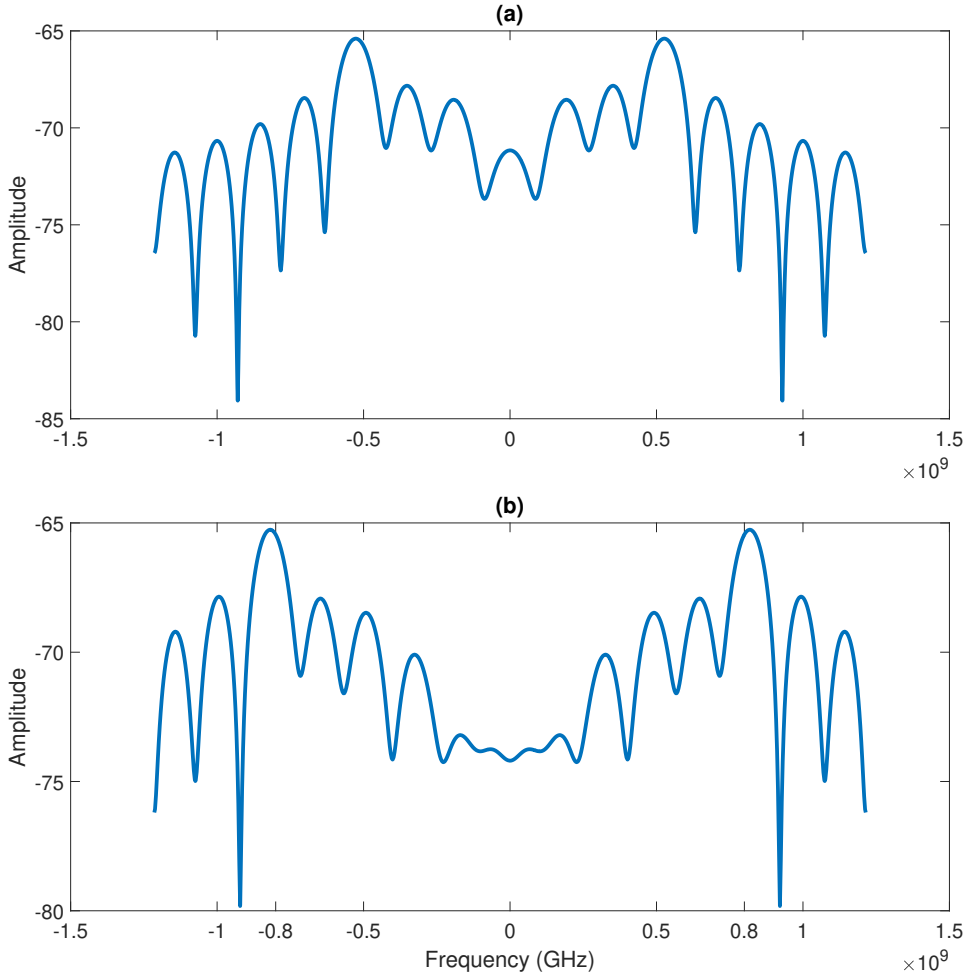

Figure 5.1. A Simulated Spectrum of the Modulated Combined Signal Displayed with Carrier Frequencies (a) 500 MHz and (b)800 MHz at $RCR_{dB} = 20$.

In Figure 5.2, the effects of utilizing a significantly smaller RCR_{dB} are also easily observed, where the lobes at carrier frequencies are notably less distinctive in both the 500 and 800 MHz cases. We can clearly observe that the lower RCR, which we recall indicates relative closeness in value to P_r and P_c, makes the mainlobe less distinguishable because of the combination of communications' increased power and the spreading of the communications bandwidth (SRBR=17).

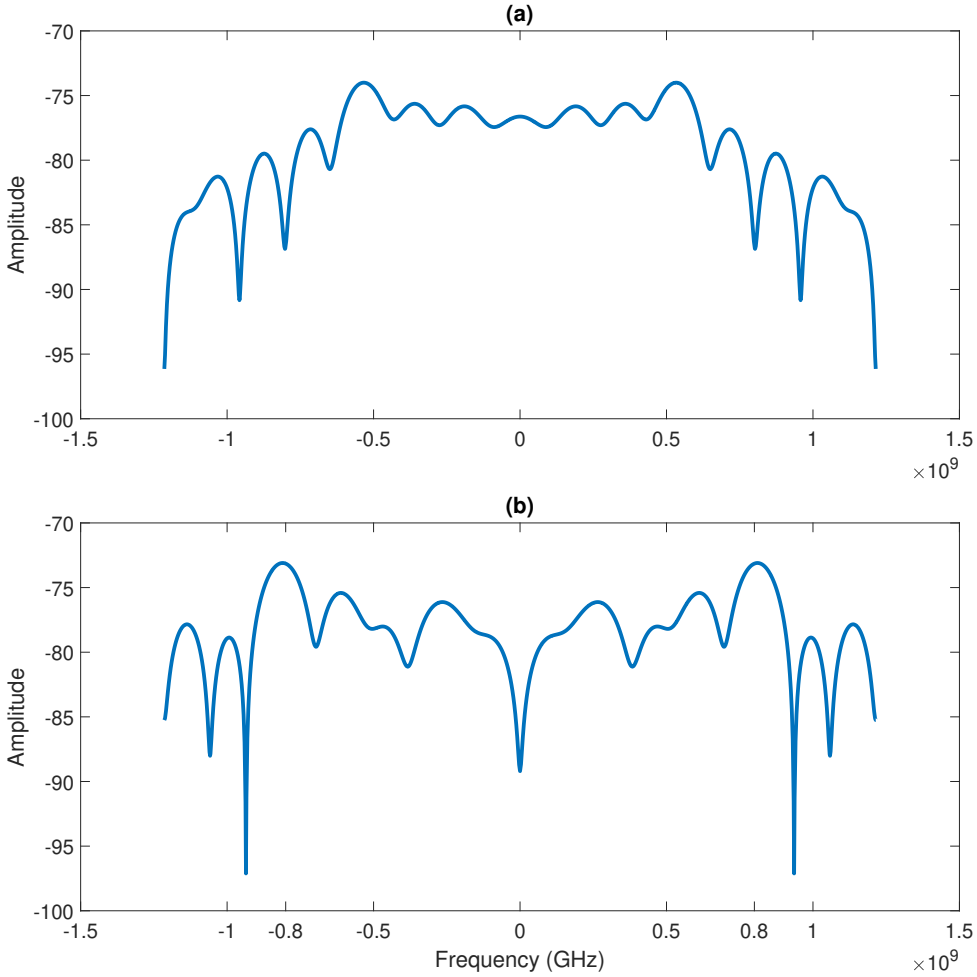

Figure 5.2. A Simulated Spectrum of the Modulated Combined Signal Displayed with Carrier Frequencies (a) 500 MHz and (b) 800 MHz at $RCR_{dB} = 3$.

5.2 Generation of Combined Signal

The ability for transmission of the combined signal is substantiated by radio frequency (RF) transmission with a Rohde & Schwarz (RS) FSQ Signal Analyzer (FSQ) coupled with RS SMW200A Vector Signal Generator (SMW) via the I and Q (in-phase and quadrature) modulation input/output signal paths using a coaxial cable connection. An image of the RS equipment suite is shown in Figure 5.3. The desired signal is generated by taking advantage of a combination of MATLAB scripting, file generation, and codecs. We use these techniques to convert the MATLAB-generated, combined signal $C[n]$ data from our

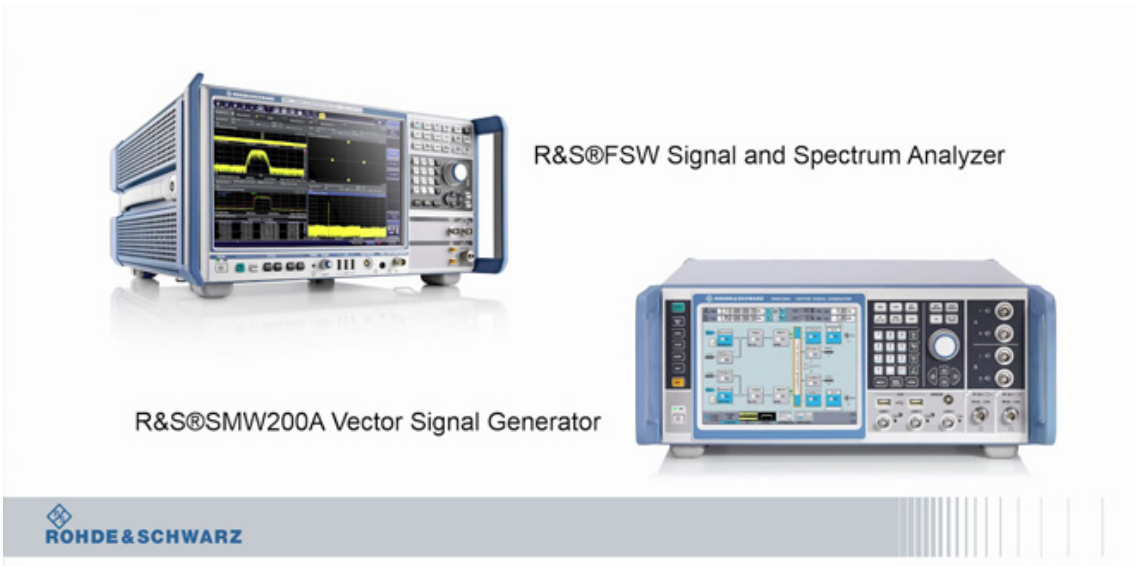

Figure 5.3. A Conventional RS Signal Analyzer and Generator Combination. Adapted from [12].

simulations into a format that can be successfully interpreted by the SMW. The converted data is then loaded into the the SMW and transmitted via the RF output to the FSQ, which yields the result shown in Figure 5.4.

To code our signal, we again use values of $RCR = 20dB$ and $SRBR = 17$ to facilitate comparison with our simulated representation. We transmit the noiseless, combined signal at carrier frequencies 500 MHz and 800 MHz, which are shown in Figure 5.4 and Figure 5.5. As is usual for spectrum analyzers, only the positive frequencies are shown. The amplitude reference levels for these plots are held constant in the FSQ so that frequency lobes can be more easily contrasted. Note the similarity of the spectra in Figure 5.1 to Figure 5.4 and Figure 5.5. The simulated spectra in Figure 5.1 are limited by our sampling time, while the figures from the spectrum analyzer are most likely re-sampled depending on the resolution and video bandwidths of the analyzer.

We also note the difference between the smooth mainlobe in Figure 5.1 and the original pulse spectrum in Figure 2.1. The mainlobe of Figure 2.1 is used to manufacture one pulse in t_p duration, while the combined signal shown in Figure 5.1 corresponds to that pulse, plus zero-padding to include the off time of a true pulsed radar waveform, which yields a smoother mainlobe.

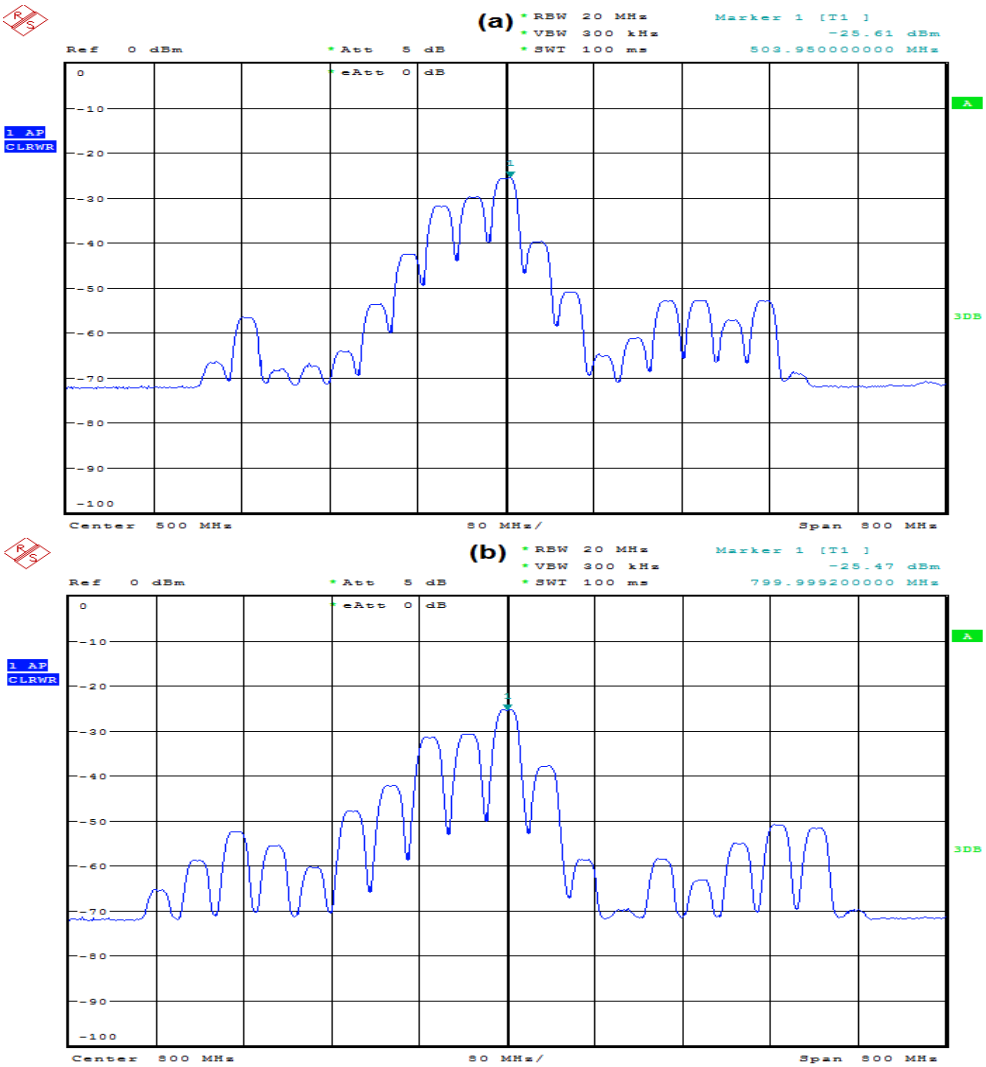

Figure 5.4. The R&S FSQ Spectra of the Generated and Transmitted Combined Signal, at $RCR = 20dB$ and $SRBR = 17$, with Carrier Frequencies (a) 500 MHz and (b) 800 MHz.

5.3 Further Consideration of the Channel: Multipath Fading

In this section, we explore the implications of the channel throughput with respect to the transmission of the combined signal in terms of the AWGN and fading channel models expressly for the purpose of generating discussion for future work. Throughout this thesis, we have considered only the AWGN channel. We add only Gaussian noise directly to the composite radar and communications waveforms both within software simulations and

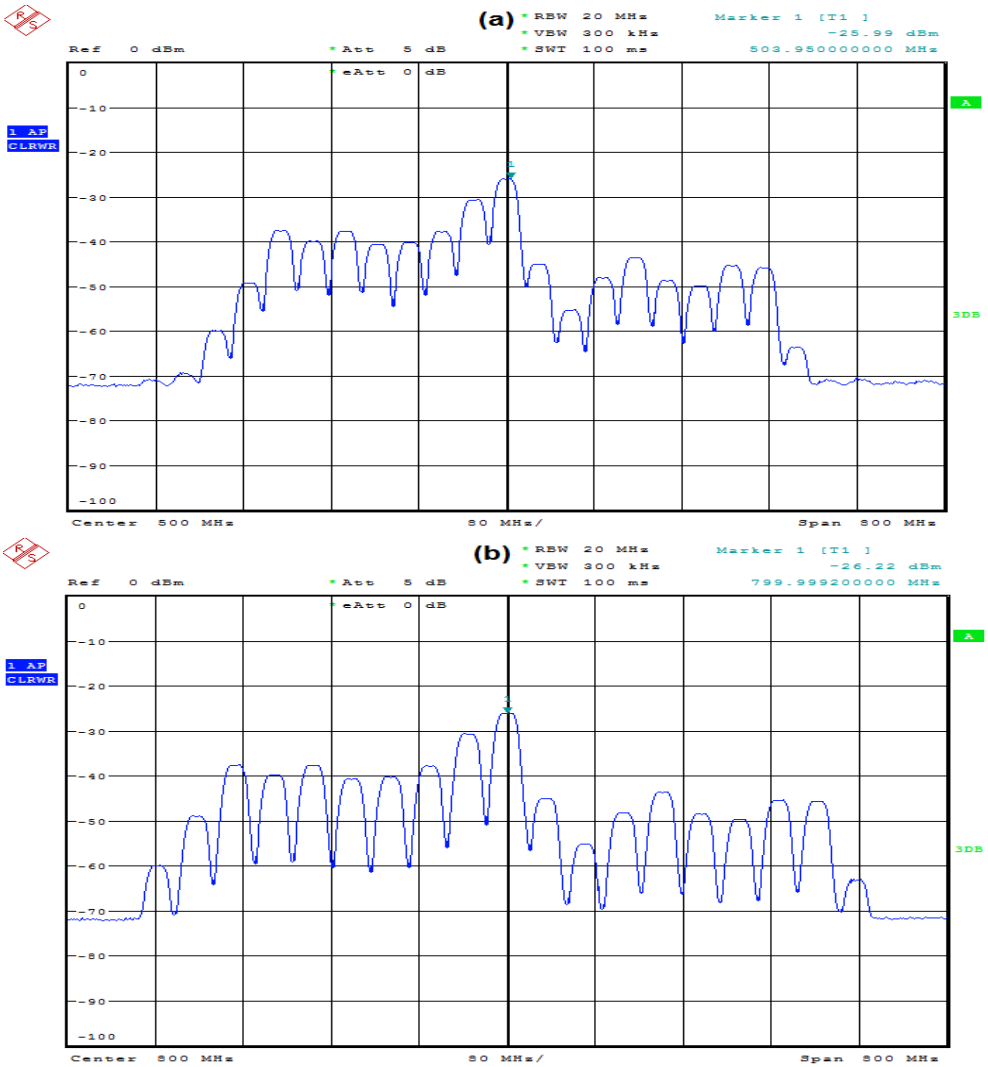

Figure 5.5. The R&S FSQ Spectra of the Generated and Transmitted Combined Signal, at $RCR = 3dB$ and $SRBR = 17$, with Carrier Frequencies (a) 500 MHz and (b) 800 MHz.

throughout hardware experimentation. As this effort progresses through successive studies, it will be interesting to eventually apply the multipath fading channel as a culminating consideration, since radar reflections from within the maritime environment are most certainly expected. Undoubtedly, these reflections from sources including terrain, other vessels, and the ocean's surface will contribute to multiple paths as well as general signal scattering and diffraction. Although we understand that Rayleigh fading is not applicable to the line-of-sight radar signal itself, it is possible that such an environment will lead to intersymbol

interference (ISI) for the embedded communications signal because of the inevitable symbol overlap caused by the multipath copies [14]. In this section, we begin to explore the potential implications of the multipath fading channel to the application presented in this work. First, we directly compare the relative feasibility of utilizing the AWGN channel against the Rayleigh fading channel utilizing a communication waveform. We consider an L-tap Rayleigh fading, multipath channel with zero mean and unity variance which has an impulse response represented by

$$h(t, \tau) = \sum_{i=1}^{L} C_i(t)\delta(\tau - \tau_i), \tag{5.2}$$

with corresponding bit error probability given in [14] as

$$P_b = \frac{1}{2}\left(1 - \sqrt{\frac{E_b/N_0}{1 + E_b/N_0}}\right), \tag{5.3}$$

where E_b is the bit energy. For our application, we can derive the Rayleigh QPSK SER with the average error probability distribution, as given in [15], from

$$P_s = \frac{1}{\bar{\alpha}} e^{-\alpha/\bar{\alpha}}, \tag{5.4}$$

where α is E_s/N_0 and $\bar{\alpha}$ is average E_s/N_0. Within our scenario, we model individual AWGN and Rayleigh channels whereby we are able to observe the respective SERs for each channel. For our preliminary simulation, we model a single input, single output (SISO) Rayleigh channel; thus, diversity order is unity and channel tap $L = 1$. After simulating transmission of our combined pulse through our modeled Rayleigh channel, we observe that we are able to implement the same technique in our simulation as in the AWGN case with identical performance. We note, however, that this is due to our assumption of knowledge of the exact radar pulse to subtract from the received signal.

In the fading channel, we offer that in order for a similar technique to be invoked, it is necessary for the receiver to develop an appropriate received radar pulse estimation procedure. Since we are not able to apply the same estimation as we accomplished for the AWGN simulation, we could not accurately calculate SER in the Rayleigh channel

RF Transceiver

1. Frequency

X-band:	9410 MHz ± 30 MHz
S-band:	3050 MHz ± 30 MHz

2. Output power

	FAR-2117	FAR-2127	FAR-2137S
Output Power	12 kW	25 kW	30 kW
Transceiver	RTR-078	RTR-079	RTR-080

3. Pulselength/PRR

Range scale (nm)	Pulselength (μs)	PRR (Hz)
0.125, 0.25	0.07	3000
0.5	0.07, 0.15	3000
0.75, 1.5	0.07, 0.15, 0.3	3000, 1500
3	0.15, 0.3, 0.5, 0.7	3000, 1500, 1000
6	0.3, 0.5, 0.7, 1.2	1500, 1000, 600
12, 24	0.5, 0.7, 1.2	1000, 600
48, 96	1.2	600

4. I.F. 60 MHz, Logarithmic

5. Bandwidth

Short pulse:	40 MHz
Middle pulse:	10 MHz
Long pulse:	3 MHz

Figure 5.6. Furuno FAR-2117 Radar Specifications. Adapted from [13].

in our simulation utilizing the technique described in this thesis. We offer that such a procedure might possibly include modifying our matched filtering technique similar to the L-tap receiver, also known as Rake receiver, to take advantage of the multipath fading environment. Such a technique will eventually recover radar energy needed for improved detection of the radar pulses. Once the multipath is mitigated in a radar pulse, we can in theory use the individual SISO receivers for the embedded communications. We also postulate that applying OFDM might possibly be a technique for mitigating the symbol overlap issue; however, we leave this and additional degradation related to more complex noise and fading environments for future work.

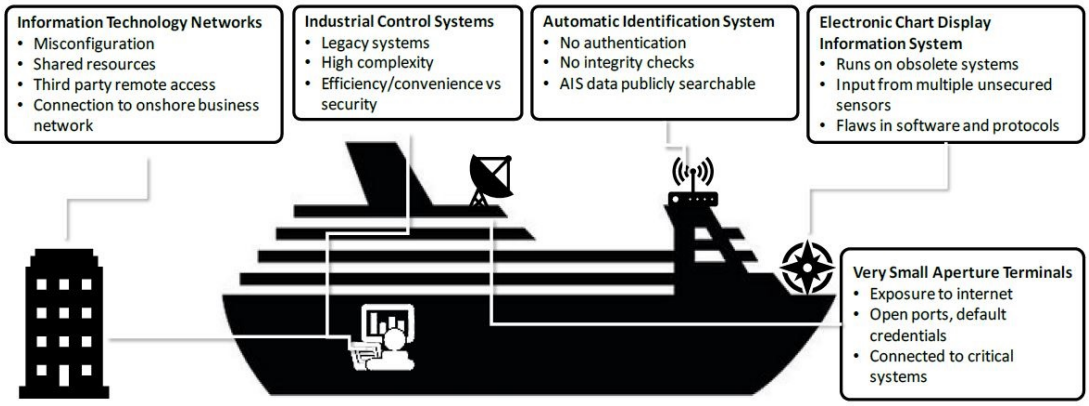

Figure 5.7. Systems Generally Found Within Maritime Networks and some Factors that Contribute to their Vulnerabilities. Source: [17].

5.4 Considerations within the MCD

One of the major implications of exploring the viability of covert communications in the context of the low-powered signal is the potential targeting of internal maritime networks with malicious intent. There exist a plethora of systems on board seaborne vessels that could be vulnerable to such malicious activity including Automatic Identification System (AIS), Electronic Chart Display Information System (ECDIS), Very Small Aperture Terminals (VSAT), global positioning system (GPS), as well as other information technology (IT) and Industrial Control Systems (ICS) that can be unique to various maritime platforms. The repercussions of the vulnerabilities of the unique IT and ICS systems can be truly destructive, especially for military and other Department of Defense (DoD)-related maritime platforms. A substantial amount of investigation, such as that found in [17], has been conducted as part of continuing efforts to foster and better understand this vastly underappreciated subject. An overview of some of the systems mentioned here, as well as important factors that contribute to vulnerabilities in each, is shown in Figure 5.7. Many of the cyber evaluations conducted on board ships may not consider the possibility of over-the-air as a medium to inject malicious data into internal maritime networks; however, taking for granted the ability to receive and decode such data, it is imperative to account for the many possible covert channels, including the possibility of radar and communications systems. In this study, a notional receiver is taken for granted, which allows for reception of such data. This notional receiver may be thought of as unlikely to exist, but if we take a case example of AIS, as presented by Balduzzi in [17] – which itself is a Very High Frequency (VHF) radio

broadcasting system – as a system that is vulnerable to Software Defined Radio (SDR) attacks, the potential for similar impropriety within our application can also be deduced.

If it is accepted that covert channels can be thus utilized to establish communications links to which maritime network administrators are oblivious, we can conclude that these networks, along with the individual systems within, can be targeted to facilitate an equally covert data exchange across different networks. That is, we can ascertain that data may be extracted and that systems within the networks can be manipulated and/or otherwise controlled. Lampson defines covert channels as those communication channels that establish links and innovate exchanges via methods and means that were not designed or intended for communication, in [18]. In light of this assertion, in tandem with our work, we agree that maritime cyber system hardening must begin by facilitating evaluations and experiments that "break new ground." Such groundbreaking experimentation has been conducted in [18] that demonstrates the ability to establish a covert communication channel between two computers utilizing audio input and output devices and subsequently extends this experimentation to a covert mesh network. Within the network, covert applications are invoked such as remote keylogging – wherein the victim's keystrokes are exploited and extricated to a separate network, and internet tunneling – collecting data on a specified server and forwarding to a remote server. The approach in these acoustical mesh network experiments were able to establish a data rate of merely 20 bits/s with a maximum range of around 20 meters between nodes. This experiment additionally established a complete path with two intermediate infected node hops for a single frame to traverse. The time for one frame to complete the path was 18 s. Taking this experimental data into account, as compared in view of the data that is presented in Chapter 3 of this work, we can posit that a comparable measure of success could be realized with our application given optimum conditions. In order to obtain such conditions, a copious amount of supplementary research must be performed as follow-on to this work to help continue breaking "new ground."

CHAPTER 6: Conclusion

In this work, we designed and applied signal models for a practical, navigation-like, radar pulse waveform for embedded communications signal that is received by an integrated communications-radar receiver. We then presented a method to calculate symbol rate throughput for a particular navigation radar which can be applied to other navigation systems. We introduced the effective SER for our system by factoring the probability of detection for the combined signal into the communications SER, illustrating how the two are intricately and intimately linked. We illustrated how varying of our system's parameters, such as RCR, SRBR, and P_{FA} directly influence the performance of the system by reducing or improving its ability to meet theoretical QPSK SER. We formed the radar embedded communications via MATLAB script and coded the combined signal on a carrier frequency in the RF signal generator. We used a vector signal analyzer to plot the output signal. The spectra produced matched the spectra from MATLAB simulations. We find that lower SRBR is not an ideal implementation of the communications system due to the fact that not enough symbols are transmitted to generate a reasonable SER. Conversely, the utilization of high SRBR mitigates the mutual interference on the elements of the combined signal $r[n]$ and $q[n]$. Specifically, we found that high SRBR results in better eSER and larger P_D. Upon modulating our combined signal, both in software and hardware, we found that high RCR results in a larger radar mainlobe.

6.0.1 Recommendations

There is an extraordinary amount of additional investigation to be carried out in order for this application to be realized. It is, however, important to realize that, although, we discuss practical implications, this entire legacy of work actually serves as a hyperbolic and theoretical platform for examining a potentially emerging direction for cybersecurity as a whole. The inclination towards utilizing spectrum-sharing applications opens up multiple possibilities for leveraging communications channels to establish links for which they were not initially intended. While the potential for covert communications will continue to increase, so will the number of potential cyber attack vectors. As this work advances, we recommend

that a range of electromagnetic/RF spectrum and cyber possibilities be thoroughly examined in tandem along with possibilities for establishing new communications links.

6.0.2 Future Work

This topic will continue to be a source of investigation for years to come due to its complex and syncretistic nature. The work has the capacity to branch across several independent topics that were discussed here: radar, communications, and cyber. We offer recommendations for future work according to each of the aforementioned topics.

6.0.2.1 Radar

From the radar perspective, we considered only the pulsed wave application. Future work could include concentration on pulse shaping, phased array and/or "stare" radar waveform type, or different system-type applications by functions such as weather, search and surveillance, or other high-resolution applications. Also, pulse trains with different radar pulse shapes, phase-coding, and duration could be investigated within the context of this work.

6.0.2.2 Communications

Considering the communications perspective, previous work started to address different communications modulation techniques for the combined signal. Comparing each of these modulations to OFDM would be valuable due to the potential for OFDM to address modulation and demodulation of the extracted communications signal in the multi-path fading environment. Exploring the fading channel, up to the Rayleigh fading channel is, in itself, a substantial endeavor to undertake for future work. Lastly, the implication of applying different error correction, error detection, and error coding techniques may be investigated. Additionally, the spectrum-sharing techniques could potentially be adapted to other mobile communications technologies outside of the maritime realm.

6.0.2.3 Cyber

Just as the author of [6] recommends, we continue to propose that the RF signal be converted into the appropriate protocol for traversing an experimental maritime data network, where the results of injecting potentially malicious data originating from external communications could be analyzed.

List of References

[1] *The Washington Post*, "A history of internet security," May 30, 2015. [Online]. Available: https://www.washingtonpost.com/graphics/national/security-of-the-internet/history/?noredirect=on [Accessed: Oct. 25, 2018].

[2] M. Ivezic, "Defeating 21st Century pirates: the maritime industry and cyberattacks," Jan. 8, 2018. [Online]. Available: https://www.csoonline.com/article/3245803/security/defeating-21st-century-pirates-the-maritime-industry-and-cyberattacks.html [Accessed: Oct. 25, 2018].

[3] *Sailing*, "Frequentis to Provide Maritime Distress Communication Solution for South Africa." [Online]. Available: http://sailing.co.za/frequentis-to-provide-maritime-distress-communication-solution-for-south-africa/. [Accessed: Oct. 20, 2018].

[4] M. Amin, "Radar as signal of opportunity, a new paradigm for wireless communications," Lecture from Center for Advanced Communications Villanova, London, UK, SSPD, December 2017. [Online]. Available: http://sspd.eng.ed.ac.uk/sites/sspd.eng.ed.ac.uk/. [Accessed: Oct. 20, 2018].

[5] A. Hunt, "Various effects of embedded intrapulse communications on pulsed radar," M.S. thesis, Dept of Elec. and Comp. Eng., NPS, Monterey, CA, 2017.

[6] E. J. Bittner, "Covert half duplex data link using radar-embedded communications with various modulation schemes," M.S. thesis, Dept of Elec. and Comp. Eng., NPS, Monterey, CA, 2017.

[7] G. Meager, "High powered radar interference estimation and cancellation for weak signal collection and demodulation," M.S. thesis, Dept of Elec. and Comp. Eng., NPS, Monterey, CA, 2017.

[8] S. Shahi, D. Tuninetti, and N. Devroye, “On the capacity of the AWGN channel with additive radar interference, ”*54th Annual Allerton Communication Control and Computing Conference*, 2016, pp. 902-907.

[9] R. A. M. Fens, M. Ruggiano and G. Leus, “Channel characterization using radar for transmission of communication signals,” *European Conference on Wireless Technology*, 2008, pp. 127-130.

[10] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory*. Upper Saddle River, NJ: Prentice Hall, 1993.

[11] S. Haykin and M. Moher, *Introduction to Analog and Digital Communications, 2nd ed.*. Hoboken, NJ: John Wiley & Sons, 2007.

[12] Rohde & Schwarz, “Testing LTE-U capable eNodeB with R&S SMW200A and R&S FSW.” [Online]. Available: https://www.rohde-schwarz.com/us/solutions/test-and-measurement/wireless-communication/wireless-5g-and-cellular/5g-test-and-measurement/mwc2016-videos/testing-lte-u-capable-enodeb_234122.html. [Accessed: Oct. 20, 2018].

[13] *Multi-color High Performance X/S-Band BlackBox Radar displaying ARPA and AIS Target Information.* Furuno., Japan. [Online]. Available: https://www.furuno.com/files/Brochure/221/upload/FAR-2107BB_E.pdf. [Accessed: Oct. 20, 2018].

[14] T. T. Ha, *Theory and Design of Digital Communication Systems*. New York: Cambridge University Press, 2011.

[15] H. Li, “Performance of modulation.” Class notes for ECE442: Communications, Dept. of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN, USA, 2013. Available: http://web.eecs.utk.edu/ husheng/ECE441_2013_files/lecture4.pdf

[16] Wireless Communication. “BER or SER for BPSK and QAM in Rayleigh fading channel.” Accessed Nov. 3, 2018. [Online]. Available: http://www.wirelesscommunication.nl/reference/chaptr05/digimod/fadserah.htm

[17] D. Bothur, G. Zheng and C. Valli, “A critical analysis of security vulnerabilities and countermeasures in a smart ship system, ”*The Proceedings of 15th Australian Information Security Management Conference*, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. pp. 81-87.

[18] M. Hanspach and M. Goetz, “On covert acoustical mesh networks in air, ”*Journal of Communications.*, vol. 8, no. 11, pp. 758-767, Jun. 2014. [Online]. doi: 2014arXiv1406.1213H

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