Ambiguous Energy Suppression in Encryption Derived Pseudo-Random BPSK Radar Signals

by

Luke J. Kamrath

A thesis submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Auburn, Alabama
December 11, 2021

Keywords: Radar, BPSK, Ambiguous Energy Suppression, CLEAN, Range Ambiguity, Encryption, Random, Pseudo-Random

Approved by

Michael Baginski, Chair, Associate Professor of Electrical and Computer Engineering
Scott Martin, Co Chair, Assistant Research Professor of Mechanical Engineering
David Bevly, McNair Endowed Professor, Department of Mechanical Engineering

Abstract

In this thesis, a pseudo-random binary phase shift keying (BPSK) radar signal is developed using Advanced Encryption Standard (AES-192). The primary objective of this encryption based BPSK (E-BPSK) signal is to provide a fast user controlled means of generating a secure a-periodic radar signal which presents several desirable characteristics. These include virtually no ambiguous range interval, high noise tolerance and spoofing security through unpredictability. Statistical analysis of a simulated data model of the E-BPSK signal is performed to verify the randomness of the encryption based sequence. A comparison signal of identical transmit properties with a different modulation code is used for a detailed comparative analysis. The standard matched filter response of E-BPSK has a sharp main lobe peak at a real target location. The random nature of the signal due to the encryption also causes a significant amount of ambiguous side-lobe energy in both the range and Doppler axis of the matched filter. A method of suppressing this side-lobe ambiguous energy is required to enable multi-target identification.

This thesis covers mitigating the ambiguous energy in the proposed E-BPSK signal with a modified CLEAN type algorithm specifically designed for an a-periodic signal. CLEAN involves identifying targets and reprocessing the signal after extracting the identified target energy. CLEAN algorithms can become hardware intensive and are sensitive to the target model accuracy. Fitness functions for optimizing the CLEAN target model parameters are included to increase model accuracy. In simulation the modified CLEAN algorithm successfully reduces the ambiguous side-lobe energy in the E-BPSK matched filter response by up to -30 dB. CLEAN processing applied to a discrete random signal is shown to effectively mitigate the ambiguous lobes in the matched filter while preserving the range and Doppler ambiguity mitigation characteristics.

Acknowledgments

The time I have spent pursuing my Masters in Electrical Engineering at Auburn University has been one of my most rewarding experiences. I want to specially thank the two most influential friends who convinced me to continue my education in graduate school, Dylan Stewart and Patrick Smith. Talking with Dylan helped me decide on what I wanted to do and Patrick introduced me to Dr. Bevly and the GPS and Vehicle Dynamis Lab (GAVLAB) which set me on the path to graduate studies.

While pursuing my degree I had the opportunity to build the MIT coffee can radar as a class project with Casey Fendley. Seeing real world measurements from the stack of circuit boards and components we assembled was a truly satisfying experience, sparking my interest in the world of radar.

I also want to thank members of the GAVLAB past and present who shared their knowledge with me. The opportunities I have had in the GAVLAB allowed me to work on many projects in a variety of research topics. Ethan Edwards who helped me get started on one of my first research projects involving FPGA programming. Houston Cleveland who as a fellow electrical engineer in a lab full of mechanical engineers helped with class advice and research. The many discussions on research and other topics with my coworkers Tanner Ray and Robert Brothers made every day working in the lab enjoyable.

I want to thank my family for helping in many ways. My mom who took time off of work to help me find an apartment in Auburn and get ready for living alone for the first time in my life. My dad who supported my exploration in of the world of engineering with many garage projects while teaching me many skills. My younger brother who also continued to graduate school at Auburn University and who helped convince my older brother to attend graduate school as well. Our strong bond and common interests in engineering topics has allowed the three of us to stick together. Our crazy discussions and occasional arguments have enriched my time in Auburn.

Finally, I would like to thank the professors on my committee. Dr. Baginski has been a constant source of input on radar topics and I am truly thankful for his dedication to helping me with work on research and my thesis. I am thankful to Dr. Bevly for providing me with a position in the GAVLAB where I can pursue research I am passionate about. Lastly, I want to thank Dr. Martin for his continued advice and mentorship through his role managing my GRA work in the GAVLAB.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

BPF	Band Pass Filter
BPSK	Binary Phase Shift Keying
CDMA	Code Division Multiple Access
CPI	Coherent Processing Interval
CSAC	Chip Scale Atomic Clock
DSP	Digital Signal Processing
FOV	Field of View
IBH	Ipatov-Barker Hybrid
IF	Intermediate Frequency
LFM	Linear Frequency Modulation
LO	Local Oscillator
LPF	Low Pass Filter
MLR	Main Lobe Reduction
OFDM	Orthogonal Frequency Division Multiplexing
PRF	Pulse Repetition Frequency
PRI	Pulse Repetition Interval

PSK Phase Shift Keying

QPSK Quadrature Phase Shift Keying

RCS Radar Cross Section

RPB Random PRI BPSK

SLR Side Lobe Reduction

Chapter 1

Introduction

1.1 Motivation

Two of the most important attributes of a radar are its ability to accurately measure the relative range and velocity to a target based on the reflected signals delay and Doppler frequency shift. Typical pulsed radars transmit and receive periodic ranging signals and have a limited range and Doppler frequency shift that they are able to measure unambiguously. Methods to extend the maximum unambiguous range and eliminate ambiguities have been developed. One method applies a modulation code across multiple pulses (inter-pulse code), and modulation within single pulses (intra-pulse code) on the base-band transmitted signal which directly extends the ambiguous range by the inter-pulse code length [1]. The range becomes ambiguous when the reflected (received) signal from a target returns after two or more pulses have been transmitted, thereby making it impossible to determine which transmitted pulse was reflected. A non-periodic random sequence can eliminate range ambiguity by making each transmitted pulse uniquely identifiable. The signal reflected by the target will therefore be a time-delayed version of the transmitted signal. When a matched filter is used to compare the transmitted and received signal, the matched filter's maximum output will occur at the round-trip delay time associated with the relative range to the target, thereby eliminating any range ambiguity. The Doppler ambiguity can be eliminated in a similar fashion by randomizing the duration of the pulse repetition interval (PRI). Additionally, transmitting unpredictable random signals eliminates the possibility of spoofing and jamming the transmitted signal by conventional methods that require a prior knowledge of the signaling used.

In the past, there have been many methods used to the generate random sequences required for random base-band modulation. The work presented here investigates a method that relies on an encryption algorithm to quickly generate a random and virtually infinite discrete random sequence, which can then be used to modulate the transmitted radar signal.

The use of a finite and band-limited random radar signal to obtain target location and velocity is a much greater technological challenge. Probably the most difficult is the aspect is correctly implementing the necessary signal processing to eliminate any artifacts (false targets) that appear in the matched filter response due to noise and inexact signal correlations in the received signal and bandwidth limitations of both the transmitter and receiver hardware. This problem is compounded when multiple targets exist in the region of interest, causing the artifacts to appear as possible targets or eclipsing actual targets.

The ability of a radar to distinguish true targets from noise and system created artifacts is of upmost importance. This typically means increasing the length of the Coherent Processing Interval (CPI) until the required Signal-to-Noise ratio is achieved. However, when random signals are used, the self-noise produced by the signal's ambiguity creates a noise-like floor that may mask a true target. In fact, this noise can be greater than the ambient noise in the received signal.

This ambiguous noise can be reduced using several methods including "mismatched" matched filters and specially optimized codes that reduce the ambiguous signal noise [2–5]. These noise reduction methods assume the radar transmission is repetitive (cyclic) over some finite time. However, for signals that are truly unique from pulse to pulse, the prior methods would not be effective or they would require additional computations for every pulse transmitted.

A more efficient means of removing the ambiguous signal energy from the matched filter response is required for random inter/intra pulse signals to become practical for commercial radars. This work addresses that problem and presents a method to create a unique, non-cyclic random signal, and remove the unwanted ambiguous signal energy from the matched filter response.

1.2 Prior Work

Research in the field of radar led to the development of many random signal modulation methods. One such method uses encryption based algorithms to generate pseudo-random sequences used for signal modulation. The use of encrypted, psuedo-random codes for signal modulation has the additional benefit of being immune to standard spoofing tactics. Shahrab and Soleimani's work in this area examined an encryption derived code that combined encrypted binary phase shift keying (BPSK) with encrypted orthogonal frequency division multiplexing (OFDM) to produced a signals that has a high resilience to jamming, even for cyclic codes [6].

The prevention of spoofing and jamming is a concern for Global Positioning Satellite (GPS) communications also. One method that is effective at identifying and removing undesired or spoofed signals is termed "Successive Interference Cancellation" [7]. In this method, a spoofed signal is identified and a model of the spoofed signal or replica is created and subtracted from the original sampled signal. This effectively removes the spoofed signal from the sampled signal and the authentic signal remains.

This method can also be used in radar signal processing. It is first necessary to identify and catalog a specific target's size and time delay, and then simulate and remove it's signature from the return signal. This process begins by identifying and removing the largest target signatures first and progressing to the smallest target signatures. The general technique is referred to as a CLEAN type algorithm [8], but there are multiple variations of CLEAN algorithms which have distinct characteristics.

There is a large body of work in the area of CLEAN processing "noisy" signals to reveal each singular source. In fact there are several variations of CLEAN for radar signal processing that include sequence CLEAN [9] and coherent CLEAN [10]. Some of these methods focus on the matched filter output while others process the actual sampled signal and identify and remove successive target replicas. Much of the research using CLEAN involves correctly obtaining accurate target size estimates in order to generate exact target replica signals for target negation. It should be noted that errors in the target model's description will cause errors in its removal.

The CLEAN algorithm is computationally intensive and increasing the algorithms efficiency and speed has become a separate area of research not considered here. It is interesting to note that a CLEAN type algorithm has been shown to reduce the ambiguous energy in MIMO synthetic aperture radar images [11]. To combat the ambiguous energy in the AES-192 based signal, this thesis uses a modified version of the CLEAN algorithm that is optimized for long, non-periodic signals.

1.3 Contributions

This research presents a unique base-band modulation method based on AES-192 encryption that, in theory, causes the unambiguous range to become infinite. In order for the method to work most efficiently, CLEAN type signal processing must be used in conjunction with the base-band modulations method, thereby eliminating the ambiguous signal energy from the matched filter response. This research presents an effective modified CLEAN algorithm that removes the unwanted and ambiguous target energy.

Much prior work in radar that investigated random and pseudo-random encryption based methods tend to focus on the auto-correlation functions output for limited times. Presenting the output data in this manner, without the entire time history shown, hides a significant drawback that plagues most non-periodic random modulation methods - the creation of repetitive and ambiguous noise that exist over multiple pulse repetition intervals. This ambiguous noise is likely to prevent weaker target signatures from being observed.

Since the radar return's signal power $P_R \sim 1/R^4$ fourth, small differences in range have large effect on the received power. Therefore, to minimize power fall off with range a logarithmic time-range axis is used. The auto-correlation function of a pulse train consisting of non-perodic pulses examined on a log scale reveals a large amount of ambiguous energy observed as range and Doppler side lobes. This is observable over all the matched filter range and Doppler bins. The ambiguous energy may be described as self-noise, and is the result of an inexact correlation of the random signal with itself. It is worth noting however, that the main matched filter signal peak is always larger than the ambiguous side-lobes.

This ambiguous side lobe energy can be decreased by increasing the number of code chips, phase states, or other modulation methods that effectively increases the bandwidth of the signal. If both the code rate and bandwidth are limited, another technique must be used to reduce the ambiguous energy. Fortunately, the matched filter responses to random transmit/receive signals have a single large peak associated with the round trip time to the target. This allows for a CLEAN type algorithm to extract the target parameters and generate and subtract a target signature replica and search for other secondary targets that could be hidden in the side-lobes. The specific contributions of this research are focused on allowing random modulation schemes to be used in radar by mitigating the ambiguous sidelobe energy using an optimized CLEAN algorithm.

The specific contributions are as follows:

i) Overview of signals based on encrypted discrete random sequences.

ii) Introduction of a hybrid discrete random signal with range and Doppler ambiguity suppression properties.

iii) Development of optimizer functions for obtaining refined CLEAN target parameters.

iv) Optimized CLEAN applied to an discrete random signal to enhance target identification.

1.4 Thesis Outline

Chapter 2 covers the necessary background of radar concepts related to target identification and processing. Chapter 3 introduces various methods of randomizing components of the radar signal and provides analysis of each. Chapter 4 is an overview of CLEAN and the required processing to mitigate ambiguous energy in radar matched filters. Chapter 5 provides a comprehensive simulation of an ideal cyclic radar signal and a hybrid encryption derived random signal with CLEAN processing to mitigate the ambiguous energy in each. Chapter 6 covers the conclusions made from the analysis and simulations and provides future work based on eliminating several assumptions currently required for CLEAN to perform optimally.

Chapter 2

Background

2.1 Radar

Sensing and detection of objects can be done in many ways. Looking at nature, the easiest is passive collection of visible electromagnetic radiation (light) in the eyes. More interesting and complex natural sensing methods include echo-location common to bats and sonar in dolphins that in both cases use reflections of sound for accurate sensing in total darkness. Radar takes the concept of listening for echoes and applies it in the radio frequency electromagnetic spectrum.

2.1.1 Radar Principals

In its most basic form, radar is a system that transmits radio-frequency (RF) electromagnetic waves and listens for echos from reflections off of objects in its region of interest [12]. The major subsystems of a radar include the transmitter, antenna, receiver and signal processor. Each subsystem varies by radar design and application. In the general case, the transmitter produces the modulated driving signal for the antenna. The antenna directs and shapes transmitted radio energy and receives reflected energy when it is not transmitting. The receiver is responsible for amplifying, demodulating and converting the reflected energy absorbed by the antenna into data for the signal processor. The signal processor extracts target information from the receiver data. In modern radar, digital signal processing (DSP) is more common place, however analog-detected voltage is sometimes all that is required. For DSP, the receiver converts the RF to an intermediate frequency and samples it with an analogue-to-digital converter (ADC). The digital samples can then be serially processed or stored in a buffer and post-processed in intervals.

2.1.2 Radar Signal Structure

Radar signals can be divided into two types, continuous wave and pulsed. Continuous wave radar transmit a signal constantly which requires a lower peak power but usually has more ambiguous correlation energy. Pulsed radar focuses the RF energy into a small "active" period with a much higher peak power. The short duration of the pulse makes it distinguishable from other signals, aiding in target identification. The pulses short duration also means that the correlation response is minimal until the pulses overlap. The most basic of pulse radar signal transmitted is created using a low frequency base-band pulse to modulate a high frequency carrier frequency. The base-band pulse is periodic over the pulse repetition interval (PRI) and active during the on-time τ. The duty-cycle of the pulse is defined as τ/PRI. Basically, the base-band pulse is used to turn the carrier oscillator "on" and "off".

2.1.3 Target Detection

A matched filter is used to identify targets in the reflected radar signal. A matched filter correlates the transmitted and received signal, causing the correlated signal to maximize at a time corresponding to the round trip time to target. This is can be done using DSP to cross correlate the transmitted and received signal. Like correlation, cross-correlation shows the similarity between two signals versus a time offset. Cross-correlation of the received signal is done by sampling the received signal and comparing it to a stored replica of the transmitted signal at varying shift intervals. The cross-correlation also maximizes at the time delay associated with the target's range [13]. Auto-correlation of a signal is the product of cross-correlating a signal with itself and provides a general idea of what to expect when a target response appears in the cross-correlated output.

A Barker-13 sequence, Figure 2.1(a) is one of the sequences used in the research and its auto-correlation function is shown in Figure 2.1(b). A large difference between the peak at zero and the amplitude of the function at any other shift is desirable. Barker sequences are known for having the best possible peak to floor performance for a BPSK code up to the length 13 [14]. Additionally, Figure 2.1(d) shows the auto-correlation function of thirteen random BPSK chips, Figure 2.1(c) with visibly higher side lobes. When codes are used for signal modulation,

peaks in the cross-correlation of the reflected and transmitted signal will correspond to the round trip delay time to the targets. The delay times are found by dividing the sample delay to peak by the sampling frequency. The range to the target R, corresponding to the sample shift Δn for a cross-correlation peak, can be calculated with Equation 2.1 using the speed of light in atmosphere c and the sampling rate F_s.

$$R = \frac{c\Delta n}{2F_s} \tag{2.1}$$

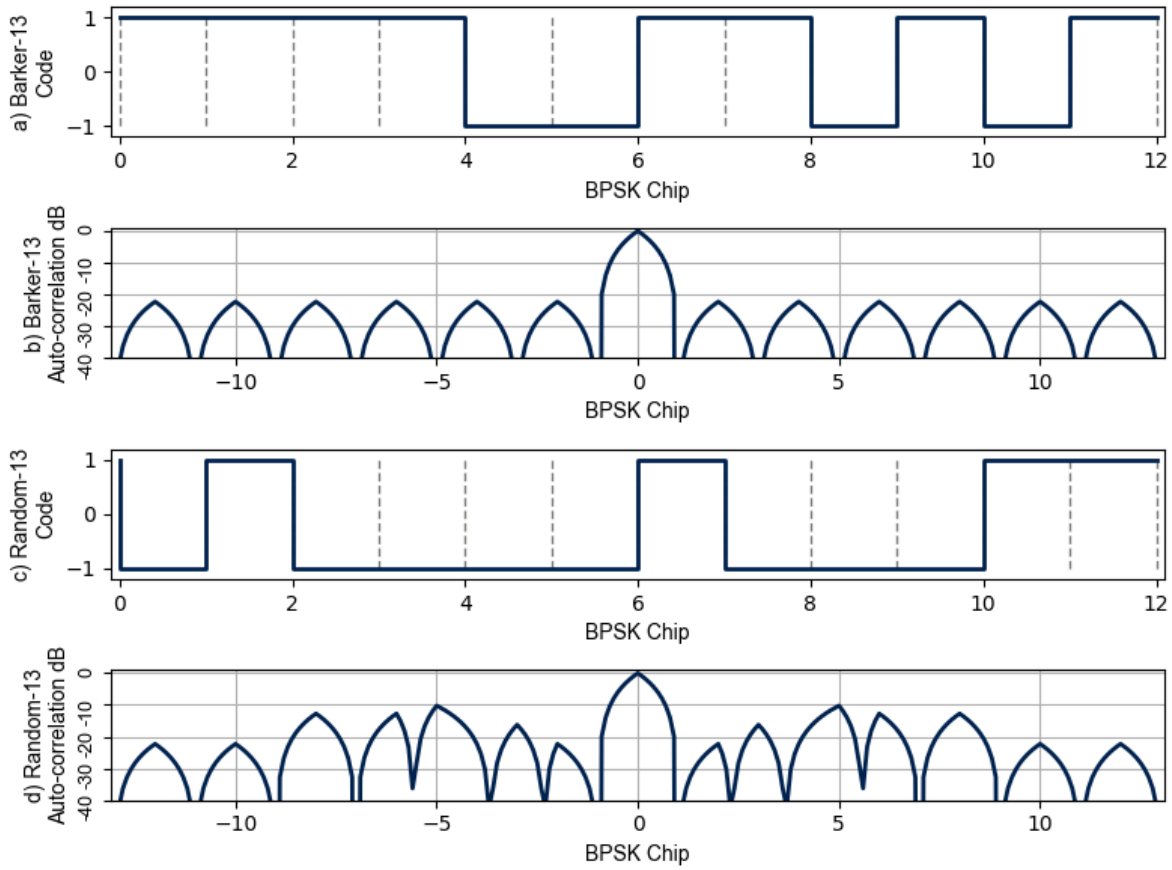

Figure 2.1: Two BPSK codes consisting of 13 chips and their respective auto-correlation functions.

2.2 Radar Weaknesses and Vulnerabilities

The desired information reported by a radar is the range/position and/or velocity of all real targets in the field of view (FOV). Additional spurious signals in the radar's matched filter

output, whether intentional or passive, are unwanted and may lead to false target identification. Sources of these undesirable dubious signals include clutter, range ambiguity, Doppler ambiguity, and environmental/thermal noise. There is also the possibility of intentional enemy jamming directly aimed at disabling or reducing the radars performance.

2.2.1 Clutter

Spurious signals that are caused by the natural environment such as terrain or vegetation, are termed clutter. Because clutter is caused by a real reflection it can sometimes be difficult to differentiate between actual targets and clutter. In synthetic aperture radar (SAR) clutter is advantageously used to create an image of an area [15].

2.2.2 Range Ambiguity

A radar transmitting a cyclic pulsed signal will pick up reflections of those pulses at various time delays related to target ranges as seen in Figure 2.2(c). If the transmitted signal is a stream of repetitive pulses, there are time intervals where the received signal can have a delay time longer than the PRI. This means that an additional pulse is transmitted before the reflected signal is received. When this occurs it is impossible to determine which transmitted pulse caused the reflected signal and thus the true range is uncertain causing range ambiguity. Range ambiguity is generalized to when a target is farther away than a distance R_{max} calculated by Equation 2.2 [16].

$$R_{max} \leq \frac{c \cdot PRI}{2} = \frac{c}{2PRF} \tag{2.2}$$

When this occurs the detected pulse will look like it arrives at a time $\Delta T \; modulus \; PRI$. The effect is shown in Figure 2.2(d). This modulus effect occurs because the transmitted pulse looks identical to the previous pulse from PRI seconds ago, causing it to match with itself in two positions. One of the matches is ”real” and the other is a range ambiguity. One way of avoiding range ambiguity is shaping each pulse so that it is uncorrelated with the previous pulse. Analysis of the non-repetitive Encrypted Pulse Encoding will be shown in a later section. Assuming that each pulse is indeed unique there can only be one position where the output is

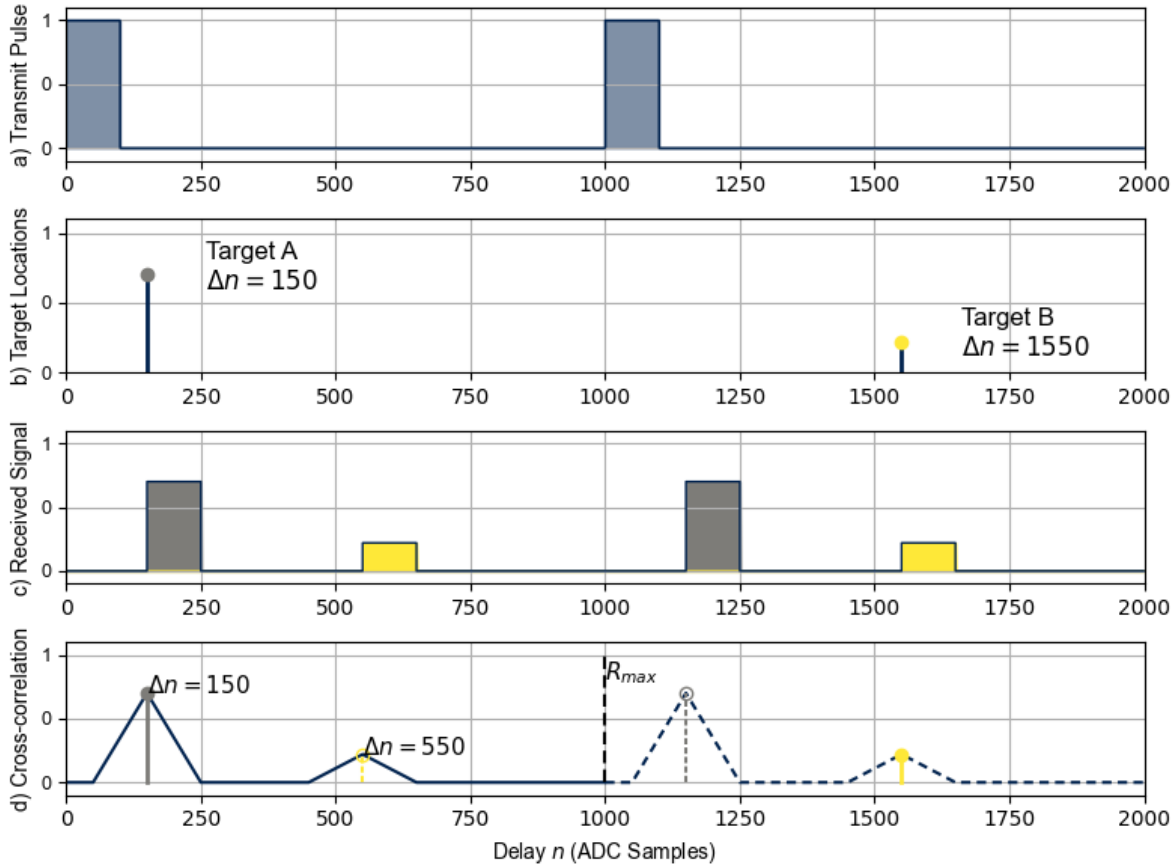

Figure 2.2: a) Two pulse repetition intervals of a base-band pulse with $PRI = 1000$ and $\tau = 100$ samples. b) Simulated target sample delay. c) Simulated targets corresponding pulse delays. d) Cross-correlation response, target B lies beyond the ambiguous range limit causing a false target at $\Delta n = 550$.

maximized. A shift of any N PRI will not produce a duplicate peak. This allows for longer integration periods if desired, as well as a virtually infinite unambiguous range.

2.2.3 Doppler Ambiguity

Measuring the Doppler frequency of a target provides an estimate of the component of its velocity in the radial direction relative to the radar. When demodulating the received signal to base-band, any frequency shift that is not the intermediate frequency is considered a Doppler shift $f_{Doppler}$. The Doppler shift in the carrier frequency f_0 caused by target radial velocity V_R is found according to Equation. 2.3[17].

$$f_{Doppler} = \frac{2 f_0 V_R}{c} \tag{2.3}$$

While obtaining this frequency shift due to a target's velocity is fairly simple, determining the target's true radial velocity is more complicated. This is best understood by considering the spectral signature of a base-band radar signal using rectangular pulses and shown in Figure 2.3. The signal is repetitive every PRI seconds causing the Fourier Transform of the transmitted pulse waveform to be repetitive every $f_{PRF} = \frac{1}{PRI}$ as shown in Figure 2.3. The reflected radar return signal will have an identical spectrum except it will be shifted by the target's Doppler frequency $\pm f_D$. Therefore, if the magnitude of the Doppler shift is greater than $\frac{PRF}{2}$, the actual frequency shift is impossible to determine since it could be due to both negative and positive Doppler shifts. For the Doppler optimization process of CLEAN, it is critical that the

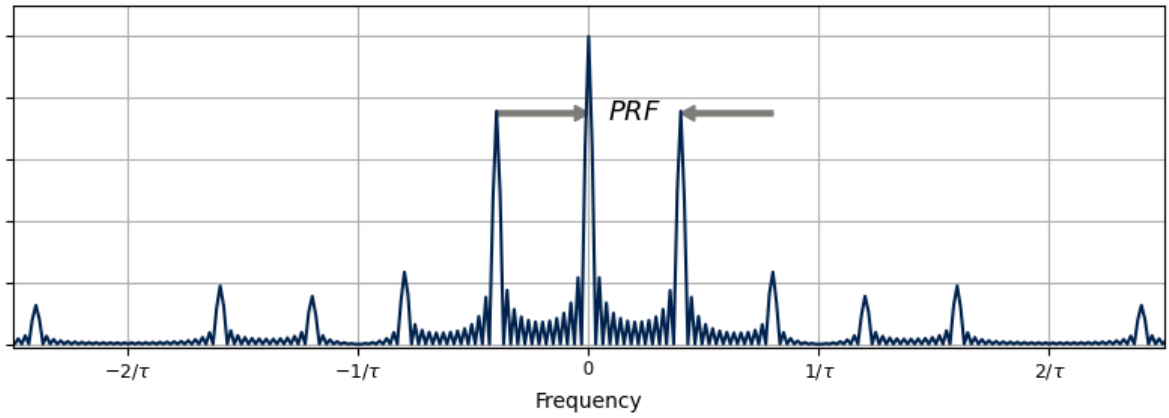

Figure 2.3: Finite radar pulse train plotted in the frequency domain.

correct Doppler frequency is used. The best signal would be one with no Doppler ambiguity, however this is usually not possible. A design constraint should be considered to minimize any additional Doppler artifacts introduced by any pulse compression or encoding used. As an example, the Ipatov sequence intra-pulse coding produces great range ambiguity reduction, but introduces many Doppler artifacts in N*PRI intervals.

2.2.4 Jamming Attacks

Attempting to disable a radar by focusing wide-band or narrow-band noise of sufficient power that it overwhelms receiver and renders it inoperable is often referred to as jamming [18]. When the receiver of a radar becomes too noisy or saturated, the real signal is buried under noise caused by the jammer. The simplest form of jamming is direct noise jamming [19].

Jamming is essentially a flood of RF noise over the same frequency band as the radar and it drowns out useful information. Countermeasures against jamming including modulation codes such as BPSK, QPSK, and frequency hopping with orthogonal frequency division multiplexing (OFDM), which can mitigate some jamming effects. Random signals tend to have wider bandwidths, making them more resistant to band-limited jamming. Much research in the area of electronic warfare jamming to disable radar is based on detection and recognition of targeted radar's repetitive signaling pattern [20–22]. Identification of the signaling pattern allows the jamming signal to be designed to disable the radar detected [23]. Many advanced jamming methods based on identified signals are actually spoofing attacks.

2.2.5 Spoofing Attacks

Direct noise jamming has several disadvantages. Probably the most significant disadvantage is that a true noise signal distributes power over a relatively wide frequency band, and it therefore requires a significant amount power power and/or a very high gain directional antenna to be effective. It has the added disadvantage that all signaling in the same frequency band will also be jammed, and this may include "friendly" communications or radar signals. A more effective method of disabling an enemy radar involves creating a seemingly "authentic" radar signal with false information. The signal power has to be sufficient to overpower any reflected power. The term used to describe this is "Spoofing". Additional details of spoofing techniques are given in [24]. Spoofing does require a detailed knowledge of the radar's transmission. Spoofing signals are difficult to distinguish from true signals, making their detection nearly impossible for unsecured periodic signaling. However, random radar signaling is very difficult to "Spoof" since the transmission is theoretically unpredictable. The only feasible way of spoofing a random signal is using "meaconing". Meaconing is the time-delayed re-transmission of the actual received signal, only with much greater power so as to overpower the actual reflected signal. This makes the target appear further away and much larger than it's actual size [25].

2.2.6 Self Interference

Most radars are designed to minimize any noise that is detrimental to their operation. In most cases this is not a significant issue. However, a type of correlation interference does occur when the modulation method creates significant undesirable range-lobes in the time domain or side-lobes in the frequency domain. This unavoidable noise is due to the signal being partially correlated with prior transmitted energy even when no target is present. A very basic random BPSK inter or intra pulse modulated scheme displays this type of ambiguous signal energy in the matched filter output. There are methods to mitigate this that include the use of mismatched coding and deconvolution. Since this effect is due to the signals correlation properties, the self interference of the signal is proportional to the target echo amplitude, meaning it is not wide sense stationary.

Chapter 3

Radar Signals with Discrete Random Properties

3.1 Modulation Control

The transmitted radar signal is created by modulating a high frequency carrier signal with a pulsed lower frequency base-band signal. Amplitude Modulation (AM) is a commonly used in radar and simply adjusts the amplitude of the transmitted radar signal. Another type of modulation is frequency modulation (FM), where the transmitted carrier frequency f_c, changes proportional to the base-band signal level. An example of an FM modulation is "Chirp" modulation [26]. A Chirp signal linearly sweeps the transmitter frequency over a frequency band during the"on" time of the pulse τ from f_1 to f_2. Chirp signals have very useful properties including improved range and Doppler resolution.

Another type of modulation uses discrete binary sequences called codes to modulate a standard base-band signal. The rate the coded signal changes is the update rate or "Chipping" frequency f_c [26]. The sampling of a coded signal in continuous time is given in Equation 3.1.

$$code(t) = code[floor(f_c \cdot t)] \tag{3.1}$$

In the case of FM, the code isn't mixed with the carrier RF and is instead used to control the the oscillator frequency generating the carrier RF. Codes that modify the phase of the carrier RF are called phase shift keying (PSK). Modulating a signal with PSK codes allow multiple transmitters with the same carrier RF to be active at the same time with minimal interference. One example of this is the binary phase shift keying (BPSK) coarse acquisition codes used by the global positioning satellite system (GPS). Each satellite transmits a unique modulation code

which enables the tracking of all satellites in view at the same time [27]. Secure modulation codes also make jamming and spoofing of signals much more difficult.

3.2 Random Phase Shift Keying

The two most common types of phase shift keying are binary phase shift keying (BPSK) and quadrature phase shift keying (QPSK). For a BPSK sequence each phase key can only have two states. BPSK is simple to implement as a positive or negative sign change making it a good baseline code for testing. A discrete random or pseudo-random sequence of binary bits, must remain constant for a very short period of time that is the inverse of the chipping frequency and referred to as a chip. Each chip state is determined by the binary data sequence and used to either maintain or negate the sign of a RF carrier. Inverting the sign of an oscillating wave is mathematically equivalent to changing its phase by 180 degrees. QPSK is slightly more complex and allows for higher code complexity at the same chipping rate. The chips of the QPSK sequence are still held constant for one chip period, but are separated into four phase states instead of two. For optimal performance, the four states are usually separated by ninety degrees consisting of zero, ninety, one-hundred eighty, and two-hundred seventy. Converting the phase shift keys to angular frequency using the carrier frequency f_0 and key code $code_{PSK}$ is shown in Equation 3.2.

$$\omega(t) = 2\pi f_0 t + code_{PSK}(t) \tag{3.2}$$

Randomizing either of these phase shift keying methods simply requires replacing the cyclic data sequence with a random number generator with the correct output states.

3.3 Random Orthogonal Frequency Division Multiplexing

Changing the center/carrier frequency of a radar offers several desirable effects. Doppler ambiguity mitigation and resistance to narrow-band jamming are two benefits. Orthogonal signals have the property that the time integrated product of two channels is zero unless the channels are identical. This prevents the channels from interfering with each other in the matched filter output. Assuming a set number of frequency choices M, randomizing the OFDM selection can

be done in a similar manner to QPSK modulation, but instead of a constant phase state over a given chip period, the center frequency is determined by the code value ($1toM$) of the current chip. Selection of the time varying carrier frequency $f(t)$ with the time dependant OFDM code chip $code_{OFDM}(t)$ is shown in Equation 3.3.

$$f(t) = f_0 + code_{OFDM}(t) \tag{3.3}$$

3.4 Random Up/Down Chirp Selection

Chirp radar has a relatively wide bandwidth and offers excellent range and Doppler resolution. A pulse that starts with a low frequency (f_L) that increases over the pulse duration (τ) to a high frequency (f_H) is referred to as an up-chirp. A pulse that starts at f_H and decreases over the pulse duration to f_L is referred to as a down-chirp. This is called linear frequency modulation (LFM) when the rate of frequency change is a linear function of time. Assuming the direction of a chirp is the state, this state can also be randomized. Each pulse can be assigned a randomly selected state of either an up or a down chirp. Equation 3.6 switches between an up-chirp generated by Equation 3.4 and a down-chirp generated by Equation 3.5 using a binary sequence $code_{U/D}$ that has a random value for each pulse.

$$\omega_U(t) = 2\pi t \left(f_L + \frac{f_H - f_L}{2\tau} t \right) \tag{3.4}$$

$$\omega_D(t) = 2\pi t \left(f_H - \frac{f_H - f_L}{2\tau} t \right) \tag{3.5}$$

$$\omega_{U/D}(t) = \begin{cases} \omega_U(t), & code_{U/D}(t) = 0. \\ \omega_D(t), & code_{U/D}(t) = 1 \end{cases} \tag{3.6}$$

3.5 Random Pulse Repetition Interval

The pulse repetition interval (PRI) is usually constant, making it one of the most predictable components of a radar signal. Randomizing the PRI would cause a sequence to have a lower number of pulse overlaps when misaligned during cross-correlation which would increase the

peak to floor performance of the matched filter. In order to maintain a controllable average power, randomizing the PRI will follow a set of rules. First an upper limit to PRI duration PRI_{max} is required to arrange all of the pulses. Each PRI is treated as a fixed size bin of duration PRI_{max} while the time between the beginning edge of a bin and the activation where the pulse will occur τ_0 varies within the range 0 to $PRI_{max} - \tau$. This produces a pulse train with an even density of randomly timed pulse activation periods. The controlled pulse shifting effect also means that a calculable rate for other modulation codes is possible.

3.6 Hybrid Random Signals

Combinations of the previous methods are possible and serve to further increase the randomness of a signal. Discretely randomizing multiple components of a signal simplifies the signal's creation and correlation, given the generation scheme. The added complexity from multiple methods makes spoofing the signal much more difficult. The random nature of the signal also reduces the range and Doppler ambiguity.

One such hybrid signal is based on AES random coding used to create hybrid BPSK and OFDM sequences of varying lengths. These coding showed a high resistance to jamming/spoofing attacks [6]. A hybrid signal that combines a random PRI with a random BPSK code (RPB) is used in this research and presented in the testing section.

Figure 3.1 shows the ambiguity function resulting from the RPB signal at the zero crossing (middle left) and at the PRI_{max} interval (middle right). The RPB signal has a single central peak and mitigates the ambiguous Doppler peaks seen in the top and bottom figure. The (bottom left) and (bottom right) subplots are generated using the identical random BPSK chips but using a constant PRI set to the PRI_{max} of the RPB signal. In the bottom subplots, the ambiguous Doppler peaks due to the constant PRI are clearly visible. The first pulse interval shown in the bottom right subplot has higher range and Doppler lobes than the RPB signal (middle left and right) however they are concentrated in a 2τ range band instead of being spread over the whole (pulse) range axis. The (top left) and (top right) subplots are not a random signal and instead show the Ipatov-13 Barker-13 hybrid signal (IBH). The zero Doppler slice of the IBH ambiguity function has virtually no range lobes, but when the Doppler axis is extended to equal

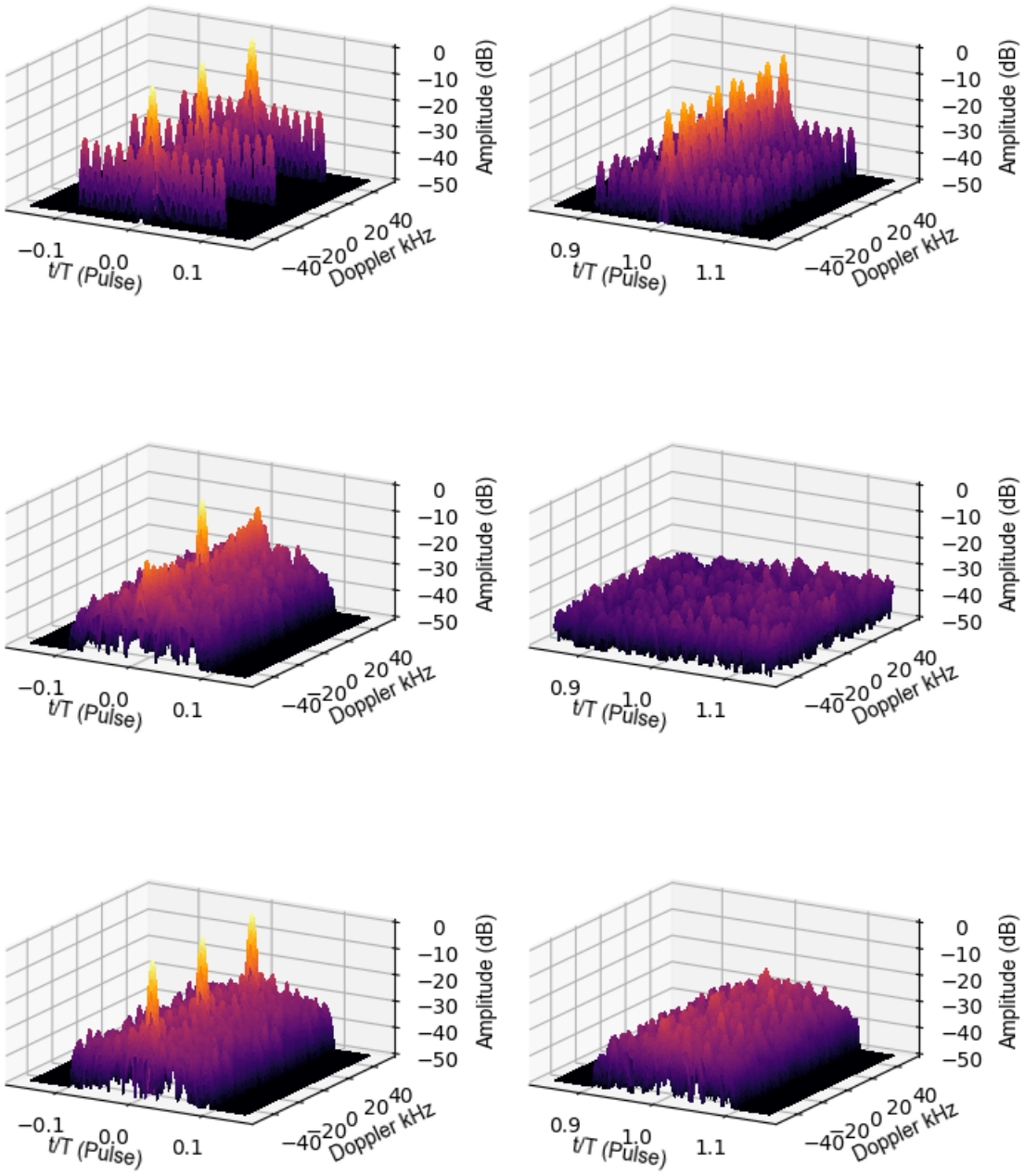

Figure 3.1: Ambiguity functions, view at zero (left column), view at first PRI (right column), Ipatov-Barker Hybrid (top), Random PRI BPSK Hybrid (middle), Random BPSK (bottom).

limits as the RPB subplots, significant ambiguous peaks are visible. From the two views of each of the three signals, the RPB signal is shown to have the highest Doppler and range ambiguity mitigation qualities.

3.7 Selected Random Signal

A binary phase code and random PRI were chosen as the components for the random hybrid signal used for testing for several reasons. First, limiting the complexity of the signal makes simulation and processing easier. A signal that can be represented in two parts, base-band and carrier, multiplied together reduces the complexity of equations. The frequency modulation based methods require a different and more complex form of the CLEAN algorithm. When comparing the random modulation methods using similar bandwidths, all demonstrated similar pulse compression and peak to floor performance. The binary phase code was chosen since it produced similar performance with an easier to model sequence. Using a binary phase code allows for a one to one mapping of the encrypted bits from the AES-192 algorithm covered in Chapter 5.1.2. Adjusting the PRI is simple and yields Doppler ambiguity mitigation properties that aid in target identification for CLEAN processing.

Chapter 4

Optimized CLEAN Algorithm

4.1 CLEAN

Methods that help distinguish individual targets in the matched filter response are especially important when pseudo random coding is used. The reason this is important is that each target's response appears to have a repetitive 'ringing' in the matched filter output. This 'ringing' will be referred to ambiguous or spurious noise. The CLEAN type algorithm is highly effective in reducing this type of unwanted noise and will be used in this research. The CLEAN algorithm begins by identifying, cataloguing, and then removing each source's signature from the response [8, 10]. CLEAN is a multi step process and it's speed is dependant on the number of targets observed in the response.

The effectiveness of a CLEAN algorithm depends entirely on it's ability to correctly identify each target's contributing signal and extracting the necessary information to produce a replica capable of removing it's contribution from the received signal. In practical applications it is impossible to perfectly remove the signal, and instead CLEAN aims to reduce the signal's presence as much as possible. By doing this targets that were hidden in the ambiguous energy are visible. The complete CLEAN process is shown in a block diagram format in Figure 4.1. For every target identified with side lobe levels above the processing noise floor, a single iteration of CLEAN is done. On the first iteration, the target with the strongest peak is identified, catalogued, and removed. On every subsequent iteration of CLEAN the largest remaining target signature is identified, catalogued, and removed until all targets are identified. The special improvements made to the CLEAN algorithm used in this work are discussed next.

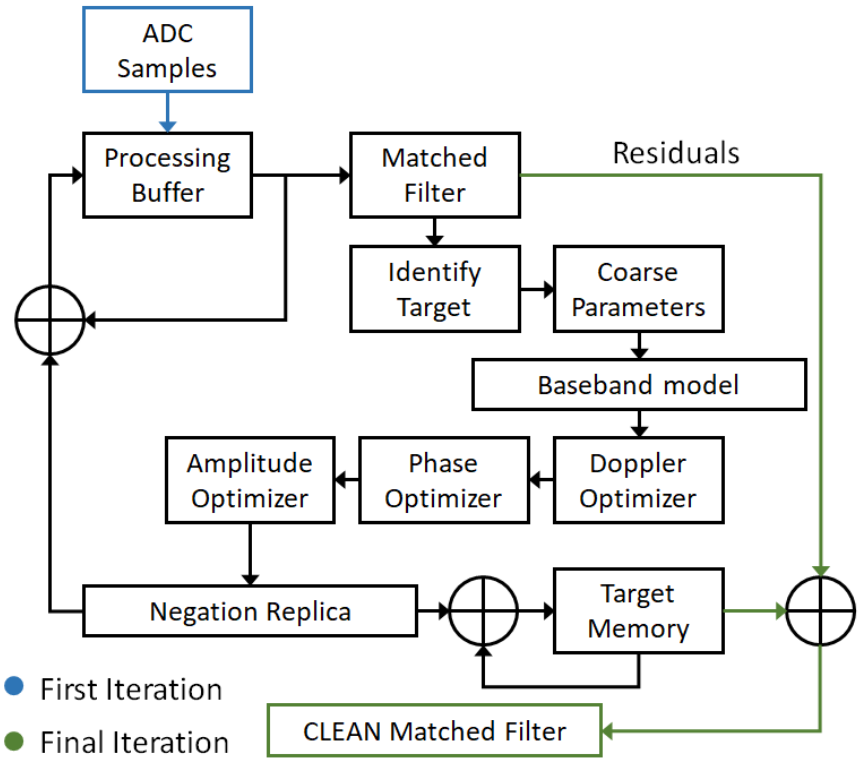

Figure 4.1: Block diagram of the iterative CLEAN process.

4.2 Sampling

All the algorithms used in this work are based on digital signal processing. The simulation of sampled signals is designed to be as accurate as possible. To help reduce the computational intensity of the code and memory required, the signals are demodulated down to an intermediate frequency or base-band before sampling occurs. This is discussed in detail in Chapter 5 Section 2. The signal processing has a bandwidth of F_B Hz and is centered at an intermediate frequency of F_{IF} Hz. A local oscillator (LO) downshifts the carrier signal frequency to one quarter the sampling frequency. The frequency of the LO used for quadrature demodulation, f_{LO}, is given as $f_{LO} = f_0 - f_s/4$. After quadrature demodulation, a low-pass filter with a cutoff frequency of $f_s/2$ is used to remove any high frequency components before sampling [28]. The quadrature is then sampled and saved to a buffer for processing.

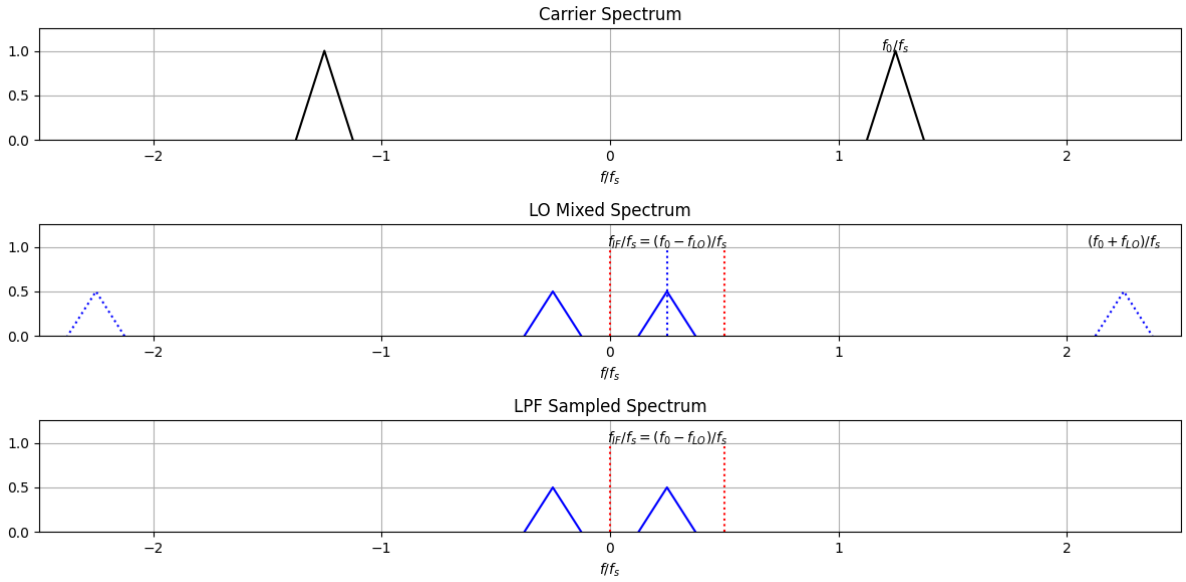

Figure 4.2: Carrier modulated bandwidth (Top), Demodulated Bandwidth (middle), Low-pass filtered demodulated band to be sampled by ADC (Bottom).

4.3 Target Identification

The first step of CLEAN is selecting the largest target signature to be catalogued and removed. Assuming a sample buffer contains N samples of the signal labeled x[n], various Doppler bins for each range sample can be formed using the intermediate frequency as the zero Doppler shift reference. Each bin's in-phase (I) and quadrature (Q) channel are cross correlated with the transmitted base-band replica created at the system sampling rate. The output of a cross correlation in a Doppler bin produces all range bins at the given Doppler frequency with a range resolution of one sample. The square root of the sum of squares of the I and Q cross correlation channels produces the magnitude of the matched filter output associated with each Doppler bin. This response can be represented as a three-dimensional surface with the x-axis corresponding to the range index n, the y-axis corresponding to the Doppler bin k, and the z-axis representing the values stored at the two-dimensional matrix index in $I[n,k]$ and $Q[n,k]$.

$$I[n,k] = \sum_{i=0}^{N-1} x\left[(i+n) \mod (N)\right] \cdot b[i] cos\left(\frac{i}{f_S}\left(\omega_{IF} + \omega_{dop}[k]\right)\right) \tag{4.1}$$

$$Q[n,k] = \sum_{i=0}^{N-1} x\left[(i+n) \mod (N)\right] \cdot b[i] sin\left(\frac{i}{f_S}\left(\omega_{IF} + \omega_{dop}[k]\right)\right) \tag{4.2}$$

Where:

n	range bin index
k	Doppler bin index
ω_{IF}	Intermediate frequency in radians/sec
$\omega_{dop}[k]$	Doppler bin frequency in radians/sec at index k

With a complete range/Doppler bin set, the first target can be selected for the parameter optimization step of the CLEAN algorithm. It is assumed that the largest signal peak is caused by the dominate target and it's range/delay, carrier phase, Doppler, and amplitude reconstruction parameters are determined.

4.4 Target Replica Approximation

To create an accurate target reflection signal, several parameters need to be identified. The most significant parameters are the target's Doppler frequency, the carrier phase change, the range and delay time to target, and amplitude. The coarse values for all of these are obtained from the location of the selected $[n_0, k_0]$ index peak in the I and Q channels of the matched filter response. The coarse Doppler frequency is simply obtained by identifying the Doppler bin k_0 with the highest output that corresponds to the target location n_0. The coarse amplitude A_0 is obtained with Equation 4.3. The duty cycle τ/PRI is used to scale the result to obtain the correct amplitude for the replica. After obtaining the coarse target parameters from the matched filter response, the next step is to develop a model of the samples for only that target. The optimization process helps to increase the accuracy of the model developed.

$$A_0 = \frac{\sqrt{I[n_0,k_0]^2 + Q[n_0,k_0]^2}}{N}\frac{PRI}{\tau} \tag{4.3}$$

The coarse phase is a simple relationship between the I and Q magnitude shown in Equation 4.4. The carrier phase can also be used to extract sub sample target delay which represents the time between two ADC samples where the target response actually peaks [28]. The whole

sample index and float sub-sample delay can be combined to get a more accurate signal delay measurement.

$$\phi_0 = arctan(Q[n_0, k_0], I[n_0, k_0]) \tag{4.4}$$

The target sample delay can be converted to target delay using 4.5.

$$t_0 = \frac{n_0}{f_s} \tag{4.5}$$

4.4.1 Doppler Optimization

Since Doppler search bins have a limited step size, the coarse Doppler from the index k_0 can be off by $\pm$ half the Doppler bin step size. A simple gradient ascent optimization initialized by the coarse reconstruction parameters allows for a Doppler frequency with a lower straddle loss to be obtained. The Doppler optimization function is part of the matched filter processing. Instead of performing the full cross correlation, only a match at previously obtained target shift position, n_0 is computed. This operation which consists of an element multiply and sum will be referred to as an in-place correlation represented by Equation 4.6.

$$X(a, b, n_0, N) = \sum_{n=n_0}^{N-1} a[n] \cdot b[n - n_0] \tag{4.6}$$

Centered at the coarse Doppler frequency obtained from the k_0 index, a smaller step size is used to generate a high and low test point which can then be used to calculate the gradient and choose the next set of test points. After a few iterations the amplitude of the Doppler optimizer will maximize. The Doppler frequency at which the output of Equation 4.7 maximizes is kept as the fine Doppler which is required for the next set of equations.

$$Opt_d{}^2 (\omega_d, n_0) = Opt_{Id}{}^2 (\omega_d, n_0) + Opt_{Qd}{}^2 (\omega_d, n_0) \tag{4.7}$$

Where:

$$Opt_{Id} (\omega_d, n_0) = \sum_{n=0}^{N-1} x [n] \, b [n - n_0] \, cos (\omega_d n / f_s) \tag{4.8}$$

$$Opt_{Qd}\left(\omega_d, n_0\right) = \sum_{n=0}^{N-1} x\left[n\right] b\left[n - n_0\right] sin\left(\omega_d n / f_s\right) \tag{4.9}$$

4.4.2 Carrier Phase Optimization

With the fine Doppler frequency, the fine carrier phase is obtained from a gradient ascent. The carrier phase optimizer is another function that iteratively determines the best phase value that maximizes the in-phase component and minimizes the quadrature out of phase component. A range of test phases are iteratively generated, and the function will converge at the maximum peak.

$$Opt_{\phi}\left(\omega_d, n_0, \phi\right) = \sum_{n=0}^{N-1} x\left[n\right] b\left[n - n_0\right] cos\left(\omega_d n / f_s + \phi\right) \tag{4.10}$$

In Equations 4.8, 4.9 and 4.10, $x[n]$, $b[n]$ and n_0 do not change. The $x \cdot b$ component can be cached and reused for all evaluations of all three equations. The phase optimization maximizes the in-place correlation response by adjusting the phase offset ϕ.

4.4.3 Amplitude Optimization

The fine Doppler and carrier phase are used to obtain the replicas fine amplitude using a gradient descent method. The Amplitude optimizer is more sensitive to local minima trapping and would benefit from a more rigorous optimizer than a simple gradient descent method. Unlike the Doppler and phase optimizers, the Amplitude optimization is designed to minimize the matched filter response at the detected target location. Essentially a test replica is generated and temporarily subtracted from the samples which are then vector multiplied with the known shifted replica. The amplitude of the test replica is varied, while the Doppler, Phase, and Delay are all fixed at their corresponding fine values. This is accomplished by first generating a signal replica with a maximum amplitude of 1.0 for use in the optimization process. The process creates a replica of the target's signature at base-band sampling frequency, $b[n]$, according to Equation 4.11.

$$r_a[n] = b\left[n - n_0\right] cos\left(\omega_d n / f_s + \phi\right) \tag{4.11}$$

This replica is used for in-place signal negation and then to calculate the in-place correlation response according to Equation 4.12.

$$Opt_a\left(A, \omega_d, n_0, \phi\right) = \sum_{n=0}^{N-1} \left(\left(x\left[n\right] - A \cdot r_a[n]\right) r_a[n]\right)^2 \tag{4.12}$$

$$Opt_a\left(A, \omega_d, n_0, \phi\right) = \sum_{n=0}^{N-1} \left(x\left[n\right] r_a[n] - A\left(r_a[n]\right)^2\right)^2 \tag{4.13}$$

The value of A that minimizes the output of Equation 4.13 is the new amplitude parameter for the target negation replica. Figure 4.3 shows Equations 4.7, 4.10 and 4.13 evaluated at test points (green circles) centered on the coarse values calculated from the matched filter. They converge to local maxima/minima (red plus) when the optimal replica parameter is used. The convergence point is approximated by cubic interpolation using the test points (blue line) and the corresponding maximum or minimum coordinate is obtained from the interpolation function.

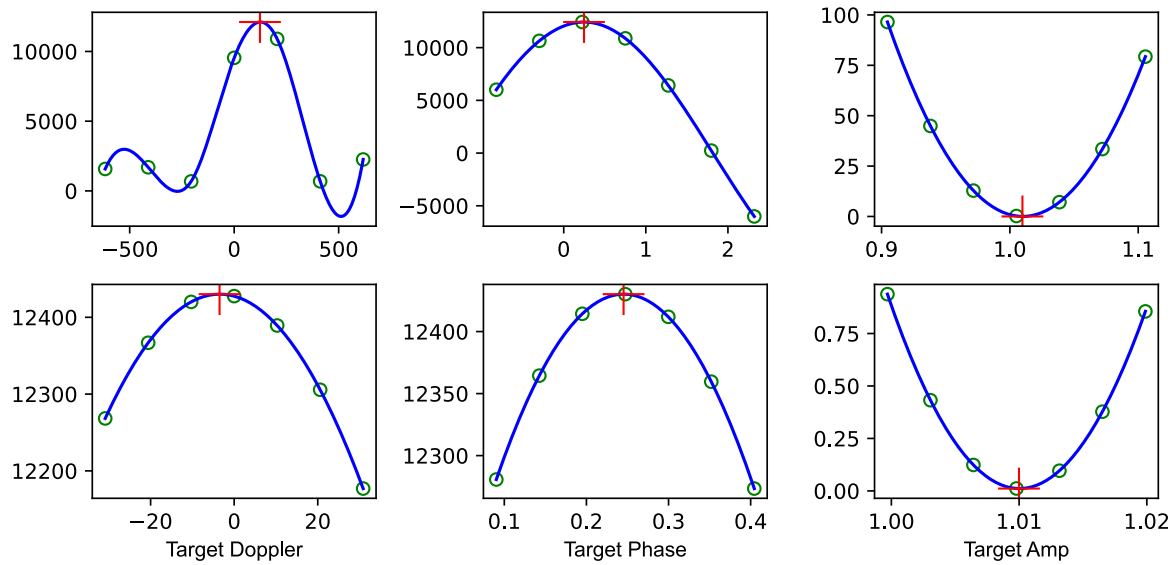

Figure 4.3: Sample CLEAN replica parameter refinement. Doppler optimizer (Left Column). Phase optimizer (Middle Column). Amplitude optimizer (Right Column).

4.4.4 Algorithm Optimization

Equations 4.12, and 4.13 are mathematically equivalent, but Equation 4.13 is slightly more optimal for checking multiple values of A. In code, Equation 4.12 consists of a multiply, subtraction and multiply that cannot be cached for reuse in the next A evaluation. Equation 4.13 consists of two multiplies a square and subtraction, but a multiply and the square sequences can be cached for reuse, meaning over multiple evaluations of A, only a multiply and subtraction are required. Simply changing the form of the equation reduces the computation cost. Another consideration for the cached sequences, any sample in the replica where $r_a[n] = 0$ will always result in zero so it can be skipped. For a pulsed radar signal, this means that after the replica is partially generated (base-band pulse activation mask), only the samples during the on-time τ need to be checked. A large portion of the optimization steps are not co-dependant meaning a parallel form could be designed for execution on a GPU. The level of accuracy can be tuned with adjustments to the number of iterations, and which optimizers are run.

4.5 Target Negation

In the first iteration, the receiver samples $x[n]$ are copied into the processing buffer $x_0[n]$. After all reconstruction parameters have been determined, the approximate replica is generated at the system sampling rate and subtracted from the processing buffer values resulting in the new processing buffer values $x_i[n]$ shown in Equation 4.14.

$$x_i[n] = x_{i-1}[n] - Ar_a[n] \tag{4.14}$$

If the approximate replica is accurate, it significantly reduces the signal contribution of the selected target including the amplitude of ambiguous energy also referred to as range lobes in the matched filter's response. Since the identified targets are effectively being processed out of the signal, memory is required for the cataloging of the identified targets. Before the first iteration, an empty matched filter response is created as the target memory. Every time a target is identified and removed from the processing buffer, a corresponding thumbtack response is added to the target memory. This is effectively the cleaned virtual matched filter response. On

the last iteration, the remainder of the processing buffer's matched filter response (residuals) is combined with the cleaned virtual matched filter response to produce the complete CLEAN matched filter response.

4.6 Reprocessing

Once an identified targets replica signal is subtracted from the data samples, the new $x_i[n]$ can be reprocessed with the quadrature matched filter. Reprocessing with the matched filter will reveal any targets previously obstructed by the ambiguous range lobes of the negated targets. The full CLEAN algorithm can be repeated for each target identified until a threshold or minimal change in the matched filter result after reprocessing is reached. When the true noise floor in the matched filter is reached, further iterations only add distortion to the signal and can not reduce any ambiguous energy due to external or processing noise sources.

4.7 Bandwidth Model

The negation replica is designed to match the detected target, but if the number of parameters of the constructed replica are limited, the base components (encoding base-band) used need to be as close to the real signal as possible. This is accomplished by approximating the filtering effects of the system as a whole and applying this filter to the negation replica in the optimization. The worst case scenario is when there is no approximation filter model used. When looking at a low-pass filtered signal, the edges of a square pulse of the EBPC, will have blurred transition edges. This effect is demonstrated in Figure 4.4. If a replica with perfect square transitions was

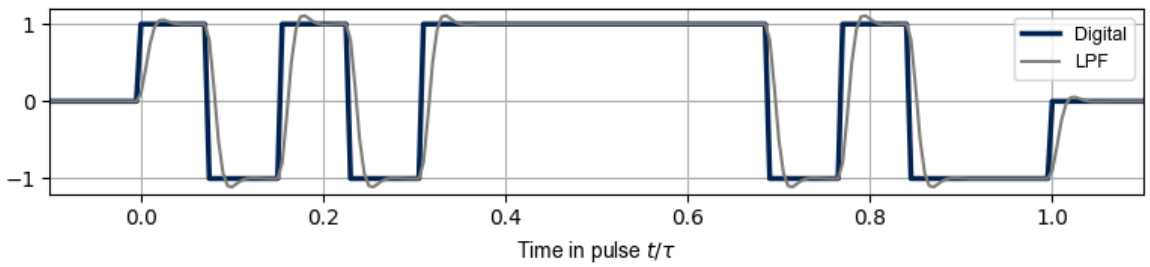

Figure 4.4: Filtering effect of band-limiting square pulse transitions.

subtracted from the real signal having smooth transitions, much of the actual target signature

would still remain. Therefore, the replica signature must include all the system effects before being subtracted from the stored signal. The example error difference between the a filtered and digital signal is shown in Figure 4.5. Errors between the negation base-band replica and

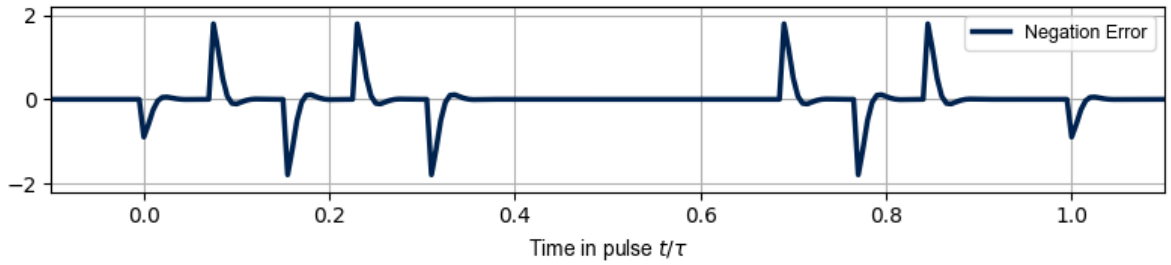

Figure 4.5: Error between a band-limited square pulse and the reference square pulse.

true base-band signal will result in artifacts generated and compounded by every iteration of the CLEAN algorithm. The artifacts limit the total amount the signal can be reduced by. This amount can be approximated by the difference of the true and modeled signal as a percentage of the matched filter peak or in dB relative to the peak before CLEAN.

Chapter 5

Simulation, Testing and Results

5.1 Signal Selection

Two signals will be used for comparative analysis in intermediate frequency simulation and CLEAN processing. One of the signals chosen, the Ipatov-Barker BPSK Hybrid is a cyclic signal with very low range side lobe ambiguous energy. The second signal used is another BPSK hybrid that instead combines both random PRI timing and random BPSK using an AES-192 encryption generator. Both signals will have the same average power, pulse on time, and number of BPSK chips per pulse. The signals are configured to have as similar a bandwidth as possible to provide a more relevant comparison. A modulation scheme such as up/down chirp or random OFDM was not chosen because minimal complexity was one of the design goals. BPSK is much simpler to implement in simulation and in future work on hardware to obtain real world results.

5.1.1 Ipatov-13 Barker-13 Hybrid

Work by Levanon showed that Ipatov sequences used in inter-pulse BPSK extend range ambiguity by the sequence length and have an ideal correlation response when correlated with a specialized miss-matched code[1]. For a proper comparison, the signals need a similar bandwidth. To achieve this, A Barker-13 sequence is added as intra-pulse BPSK. This is important later when the encrypted signal will also use intra-pulse BPSK. The shortest possible coherent processing interval for a Ipatov sequence is double its length. In this case, a minimum of twenty-six pulses must be stored before processing can be performed on the Ipatov-13 sequence. This is due to each pulse having a phase state determined by the Ipatov-13 sequence.

Barker-13 BPSK Intra Pulse Modulation Chip States													
Barker-13	$+1$	$+1$	$+1$	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	-1	$+1$

Table 5.1: Barker-13 chip sequence, repeated inside of every pulse.

Ipatov-13 BPSK Inter Pulse Modulation Chip States													
Ipatov$_T$-13	$+1$	-1	-1	$+1$	-1	$+1$	$+1$	$+1$	$+1$	$+1$	-1	$+1$	$+1$
Ipatov$_C$-13	$+2$	-3	-3	$+2$	-3	$+2$	$+2$	$+2$	$+2$	$+2$	-3	$+2$	$+2$

Table 5.2: Ipatov-13 transmit (T) and mismatched correlation (C) chip sequences, each value corresponds to a pulse state, repeats after 13 pulses.

The generation of the Ipatov-Barker Hybrid signal requires that the BPSK chips be indexed with the correct time stamp. Both sequences are written and stored as arrays, and each chip's state is stored in array cells $[0\ to\ 12]$. The current pulse P is given by Equation 5.1.

$$P(t) = floor\,(t/T) \tag{5.1}$$

The time within a pulse p is given by Equation 5.2.

$$p(t) = t \mod (T) \tag{5.2}$$

The active portion of a pulse is determined according to Equation 5.3.

$$a(t) = \begin{cases} 1.0, & p(t) \leq \tau \\ 0, & otherwise \end{cases} \tag{5.3}$$

The number of BPSK code chips per pulse remains constant and is given by Equation 5.4.

$$P_N = floor\,(\tau f_c) \tag{5.4}$$

Where:

- τ pulse on time;
- T pulse repetition interval PRI;
- f_c BPSK code chipping frequency;

The intra-pulse modulation chip array index is given by Equation 5.5. Here M, the sequence length, is set equal to 13 yielding Barker-13 coding, every pulse on time period τ will be modulated by the same 13 chips of the Barker sequence.

$$n_B(t) = floor\left(M\frac{p(t)}{\tau}\right) \mod (M) \tag{5.5}$$

The inter-pulse modulation chip array index is given by Equation 5.6. Setting M, the sequence length equal to 13 for Ipatov-13 indicates that the modulus 13 will repeat the Ipatov sequence every 13 pulses.

$$n_I(t) = floor\left(MP(t)\right) \mod (M) \tag{5.6}$$

The hybrid signal is a combination of both inter and intra-pulse BPSK methods. The Ipatov-13 Barker-13 hybrid BPSK states are given by Equation 5.7.

$$IBH(t) = Ipatov_{13}[n_I(t)] \cdot Barker_{13}[n_B(t)] \tag{5.7}$$

The matched filter output performance is sensitive to the returned signal's sampling accuracy and phase alignment. Instability in the RF oscillator generating the actual transmitted pulse and the sampling oscillator will reduce the matched filter's ability to resolve targets using the Ipatov-Barker Hybrid coding. If ideal alignment and sampling accuracy was possible then CLEAN would not be needed. However, the floating point error in the IF simulation resulted in ambiguous (spurious) peaks of up to -65 dB.

5.1.2 AES Pseudorandom Binary Phase Encoding

AES-192 Encryption [29] is used to generate a pseudo-random sequence, which can be repeatably started at a user defined time, and if desired, it may also contain additional encrypted data. AES was chosen for its computational speed and familiarity. Other forms of encryption could be used and would likely produce similar results, but this research will only use AES-192 encryption.

Data before it is encrypted is referred to as plain-text data, and after encryption as crypto-text and used for the BPSK modulation. The AES-192 variant simply indicates that the key length used for the encryption is 192-bits long. Since the algorithm operates on 128-bit blocks of data, a buffer is required to generate a continuous stream of BPSK code bits. Essentially, in continuous mode ($\tau = T$), the algorithm generates encrypted blocks at $f_c/128$ where f_c is the chipping rate of the BPSK code. The AES-192 encryption operation is given by Equation 5.8.

$$cryptotext_{128} = AES_{192}(plaintext_{128}, key_{192}) \tag{5.8}$$

The plain-text blocks are updated every encryption to produce unique crypto-text blocks, this ensures that the sequence does not repeat. A simple method for changing the plain-text on every update is to store the update counter number in the plain-text field, and this is the method shown below. The value used as the plain-text field is represented in Equation 5.9.

$$plaintext_{128} = dec2bin(k\eta + l, 128) \tag{5.9}$$

where:

$dec2bin$	decimal to binary conversion;
k	encryption block count;
η	user specified prime number;
l	user specified fill;

Since the counter updates at a fixed frequency it can also be used as an accurate record of time of transmit. To prevent an observation brute force attack, the counter is masked with fill bits and multiplied by a prime number to increase plain-text bit variability before encryption. Assuming that both the transmitter and receiver have the same key and accurate time reference (GPS time or CSAC), an identical copy of the pseudo-random sequence can be produced for correlation purposes. The equation for obtaining the n^{th} bit from the k^{th} block is shown in Equation 5.10.

$$bit[n, k] = AES(dec2bin(k\eta + l, 128), key)[n] \tag{5.10}$$

Writing n and k as a function of t allows for bit selection as a function of t. Several prerequisite variables are required to obtain them, Equations 5.1, 5.2 and 5.4 from the Ipatov-Barker Hybrid section are used here. The current block $k(t)$ and bit $n(t)$ can be calculated from accurate time as shown.

$$n(t) = floor\left(P(t)P_N + \frac{p(t)P_N}{\tau}\right) \mod (128) \tag{5.11}$$

$$k(t) = floor\left(\frac{P(t)P_N}{128} + \frac{p(t)P_N}{128\tau}\right) \tag{5.12}$$

Note that Equations 5.11 and 5.12 only produce the correct index during the active portion of the pulse τ. Values given during the inactive period of the pulse are ignored or multiplied by zero. Table 5.1.2 shows a sample of the index states corresponding to pulse times t. Using the block and bit at any time t, the phase is obtained according to 5.13.

$$bit(t) = AES(dec2bin(k(t)\eta + l, 128), key)[n(t)] \tag{5.13}$$

Multiplication by π will produce two possible phase states of 0 and π radians at the chipping frequency f_c when the pulse is active.

$$\omega_{AES}(t) = bit(t)\pi + 2\pi f_0 t \tag{5.14}$$

Note that for correct operation, the chip width (t_{chip} = $1/f_c$) must be an integer multiple of τ.

time t	$P(t)$	$n(t)$	$k(t)$
$0-T$	0	0-12	0
$T-2T$	1	13-25	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$9T-10T$	9	117-127, 0-1	0, 1
$10T-11T$	10	2-14	1

Table 5.3: Set of bit and block index values for pulse encoding with the AES method.

In this work, the chip duration was is exactly t_{chip} = $\tau/13$. Additionally, f_c must be an integer multiple of the carrier frequency f_0, to ensure phase transitions only occur at the zero-crossing of the transmitted waveform.

The phase at any time t is given by Equation 5.14. It is important to note that the AES function is only required when Equation 5.12 changes, otherwise simple indexing of the current block buffer with Equation 5.11 will provide the correct phase. Not requiring the AES calculation for every sample reduces the number of computations therefore allowing parallel code optimization using FPGA or ASIC integrated circuits.

The binary and phase states used in the BPSK sequence modulation are given by Equation 5.15 and the amplitude states given in Equation 5.16. The relationship between amplitude and phase states in a BPSK sequence is provided in Equation 5.17. The binary states $[0, 1]$ map to the phase states $[0, \pi]$, and the amplitude states $[-1, +1]$.

$$\omega(t) = binary(t)\pi \tag{5.15}$$

$$A(t) = binary(t) \cdot 2 - 1 \tag{5.16}$$

$$A(t) = cos(\omega(t)) \tag{5.17}$$

Essentially, the BPSK sequence can be implemented as a phase offset $[0\ or\ \pi]$, or as an amplitude modifier $[-1\ or\ +1]$ the resulting signal is the same and the terminology is interchangeable.

A comparison of the output statistics of the AES-192 crypto-bits to that of random-bits generated by Python's random number generator using the newest version of the Numpy package was done. This comparison confirmed the AES-192 coding was sufficiently random. The output of the random number generator was converted to BPSK code according to Equation. 5.18.

$$Random(N) = (numpy.random.rand(N) > 0.5) * 2 - 1 \tag{5.18}$$

A long length sequence was generated using both the Numpy random function and the AES method. Figure 5.2 shows the statistical density of constant phase periods in each sequence. The results from both methods are nearly identical.

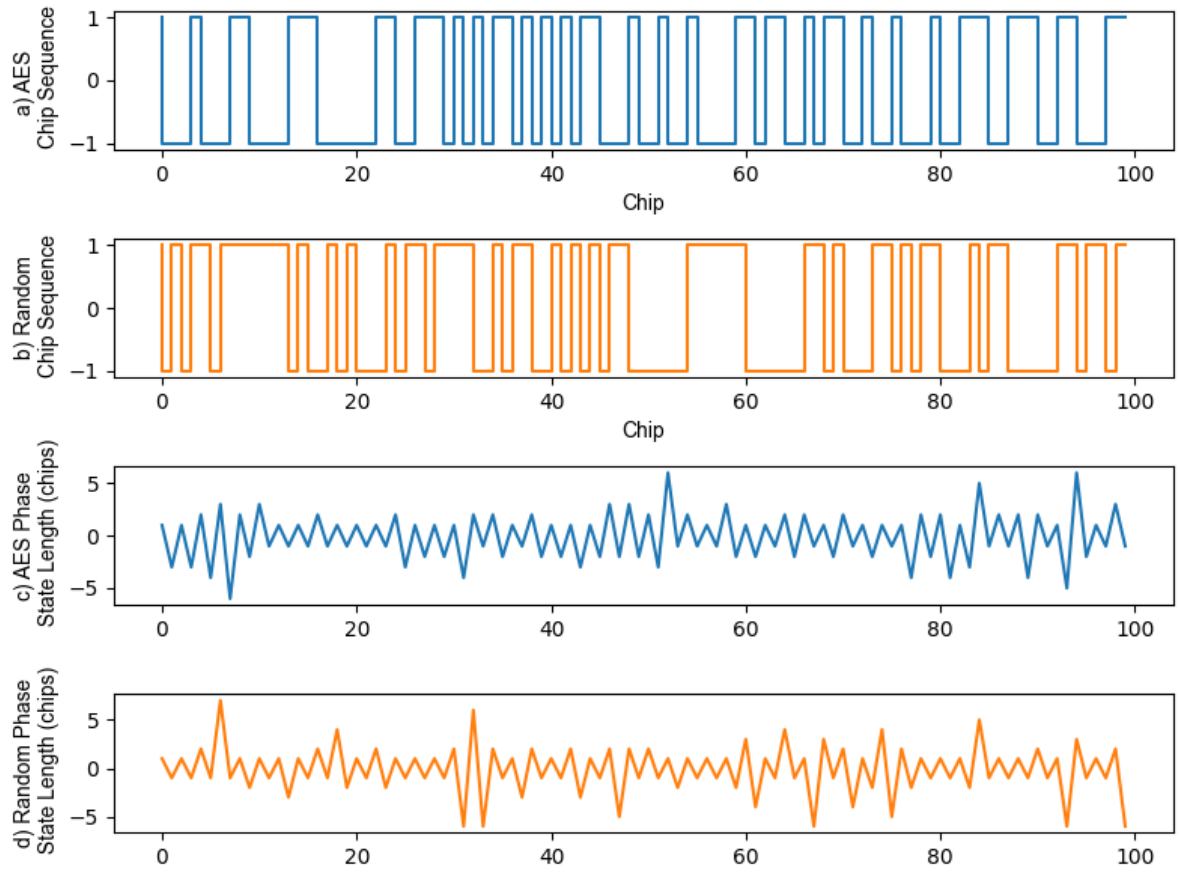

Figure 5.1: a) Sample output from the AES random generator, b) Sample output from Numpy random (Eqn. 5.18), c) Variability in phase state duration of the AES sequence. d) Variability in phase state duration of the Numpy random sequence.

5.1.3 AES PRI Randomization

The second half of the random hybrid is a random pulse repetition interval adjustment which adds a good Doppler ambiguity reduction and further obscures the signal at the cost of some spreading of ambiguous energy in the range domain. Since the ambiguous energy is a result of the signal structure, the spreading effect will also be mitigated in the CLEAN processing step later.

The number of bits per pulse shift is defined by P_B, this variable controls the discrete resolution of the random PRI time. By converting the bits from binary to integer, the number of possible pulse offsets (PRI resolution) is defined. Setting P_B to 4 would result in $2^4 = 16$ possible pulse positions within a PRI. Each PRI is essentially divided into 2^{P_B} places and one is selected using encrypted bits for the pulse activation point. The bits used in the PRI resolution

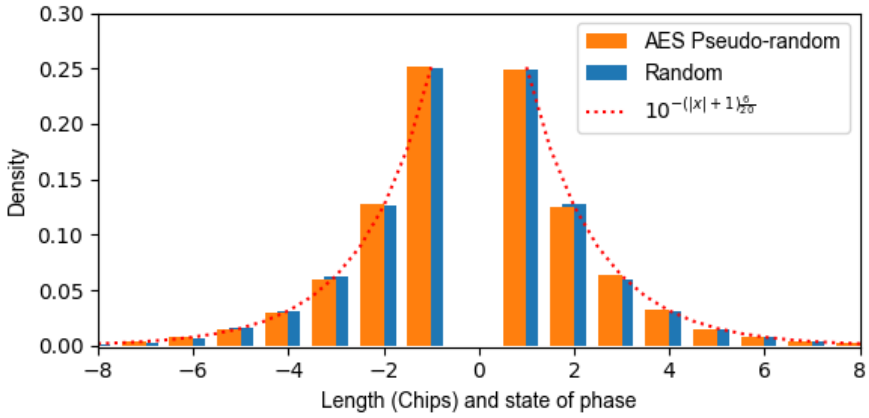

Figure 5.2: Density of constant phase state lengths in sequences generated using the AES and Numpy random methods.

changes the frequency that the encryption algorithm is required to operate at. Using 4 bits per pulse, each 128-bit AES crypto-text block would create activation times for $128/4 = 32$ pulses composed of random bits, and therefore the AES encryption would need to update every 32 pulses. Increasing the PRI resolution linearly increases the encryption frequency. A trade-off between system complexity and PRI resolution must be made. Converting the bit values to pulse shifts is shown in Equation 5.19.

$$\tau_0(t) = \frac{T - \tau}{2^{P_B}} \sum_{n=0}^{P_B - 1} crypto\left[n + P(t)P_B\right] \cdot 2^n \tag{5.19}$$

Generating the pulse uses a modified version of Equation 5.2 that adjusts each pulse activation point by $\tau_0(t)$, Equation 5.20.

$$a_r(t) = \begin{cases} 1.0, & (p(t) \geq \tau_0(t)) \,\&\, (p(t) \leq \tau + \tau_0(t)) \\ 0, & otherwise \end{cases} \tag{5.20}$$

The resulting shuffling effect on the pulse chain from Equation 5.20 is shown in Figure 5.3. The statistical distribution of pulses is limited by the PRI window size, which results in the maximum effective pulse separation being $2(T - \tau)$ and a minimum separation of zero. This method allows for controllable average power and pulse indexing using the virtual PRI set by

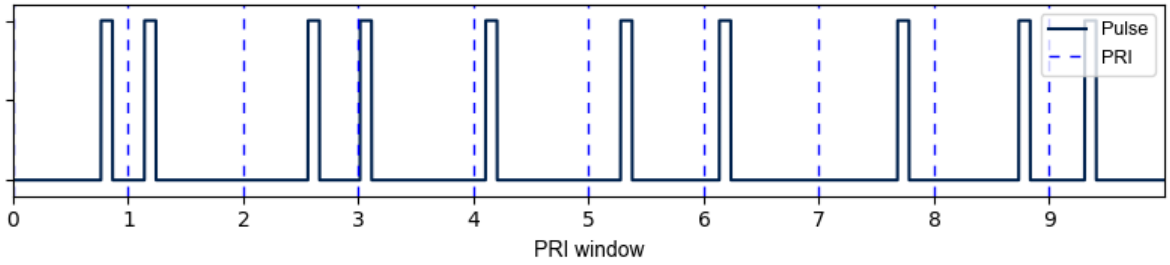

Figure 5.3: AES Random Adjusted PRI pulse sequence.

the PRI window. Pulse indexing makes generating the BPSK codes or other modulation patterns easier because even though the signal is randomized, it still maintains an order conducive to it's functional representation. This method is also designed for simplicity and would allow relatively simple hardware implementation.

5.2 Intermediate Frequency Model

The signal processing is done at the intermediate frequency (IF) to reduce the code's computational cost. The IF signal is generated by simulating the demodulation of the received RF signal using a local oscillator (LO). Mathematically, the model is derived using the Cosine Product Identity followed by a low pass filter (LPF) as shown here[28].

$$cos(a)cos(b) = \frac{cos(a-b) + cos(a+b)}{2} \tag{5.21}$$

Consider frequency a as the carrier RF frequency F_0, and b as the local oscillator frequency F_{LO}. The frequencies are converted to angular frequency by multiplication with two Pi. This results in Equations 5.22 and 5.23.

$$\omega_0 = 2\pi F_0 \tag{5.22}$$

$$\omega_{LO} = 2\pi F_{LO} \tag{5.23}$$

$$cos(\omega_0 t+\theta)cos(\omega_{LO} t+\phi) = \frac{cos((\omega_0 - \omega_{LO})t + \theta - \phi) + cos((\omega_0 + \omega_{LO})t + \theta + \phi)}{2} \tag{5.24}$$

The high frequency term in Equation 5.24, $cos((\omega_0+\omega_{LO})t+\theta+\phi)$ is removed using a lowpass filter and the remaining signal is centered at ω_{IF} resulting in Equation 5.25.

$$\omega_{IF} = \omega_0 - \omega_{LO} \tag{5.25}$$

The phase and frequency of the LO is considered to be constant, but the phase and frequency will vary in the received signal due to the round-trip signal delay time and Doppler frequency shift. The target's phase in the IF signal is given by Equation 5.26

$$\theta_{IF} = \theta - \phi - \frac{2R}{c}\left(\left(1+\frac{2V_R}{c}\right)\omega_0 - \omega_{LO}\right) \tag{5.26}$$

If the phase of the transmitter and LO are assumed zero at $t = 0$, Equation 5.26 can be simplified and given as 5.27

$$\theta_{IF} = -\frac{2R}{c}\left(\left(1+\frac{2V_R}{c}\right)\omega_0 - \omega_{LO}\right) \tag{5.27}$$

The time delay of the reflected signal from a target is given as t_d = $2R/c$ where R is the range to target and c is the speed of light. The observed Doppler frequency shift is modeled as a scaling effect on the RF caused by the target's radial velocity V_R written as $1 + 2V_R/c$ and is observed in the RF return signal. The amplitude of the IF signal can then be modeled according to Equation 5.28.

$$A_{IF}(t) = cos\left(\left(1+\frac{2V_R}{c}\right)\omega_{IF}t + \theta_{IF}\right) \tag{5.28}$$

5.2.1 Sampling Bandwidth Filter Model

The energy and power spectral density of the radar transmissions have a limited bandwidth and the signal is centered at the carrier frequency. The received signal must therefore be sampled at at least twice the highest frequency of interest($f_{sampling} = 2 \times \omega_0$) to prevent aliasing that could distort the signal. The return signal is also affected by the type of antenna, dispersion caused by the propagation media, system hardware, etc. All of these effects can be reversed ("undone") by designing a signal filter that does the inverse of the distortion that the return

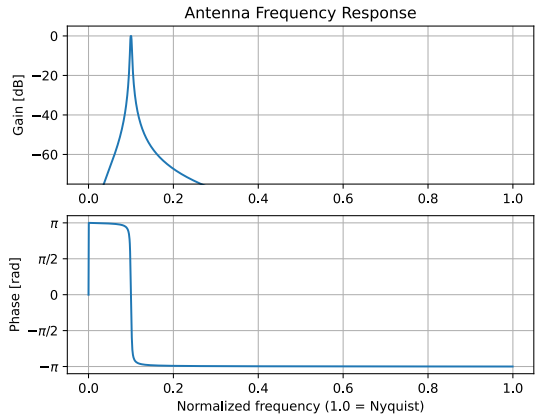

Figure 5.4: Simple antenna BPF model.

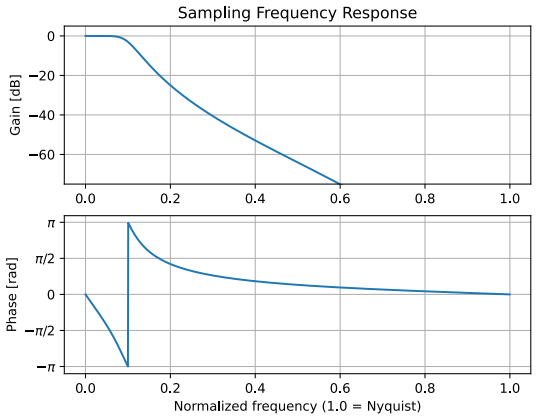

Figure 5.5: ADC LPF model.

signal experiences. This is a type of "focusing' and it is done using digital signal processing (DSP) in the research.

An example of this, consider the problem of effects of transition blurring that occurs due to atmospheric dispersion and other effects. These effects are accounted for and the signal "re-sharpend" using digital signal processing. This is discussed in subsequent sections.

5.3 Carrier Model Validation

In order to verify the accuracy of the intermediate frequency (IF) simulation model, a short portion of a test signal was generated using both the carrier frequency and IF methods. The system model filter was applied to both signals and the results are compared in Figure 5.6. The digital base-band signal's instant phase transitions are the primary point of interest for the comparison between the two models. Both models closely match in amplitude and time excluding a small high frequency bleed-through that is explainable using the Cosine Product Identity. The high frequency signal prior to the LFP Figure 5.6(cyan) contains both the (a-b) and (a+b) components covered in the IF model section by Equation 5.24. The high frequency signal after the LPF is applied Figure 5.6(blue) is primarily the (a-b) component with a greatly reduced (a+b) component. The results from Equation 5.28 in Figure 5.6(red) do not include the bleed-through from the (a+b) component, but do closely match the overall resulting signal. The similarity between the methods means that the simulation sample frequency only needs

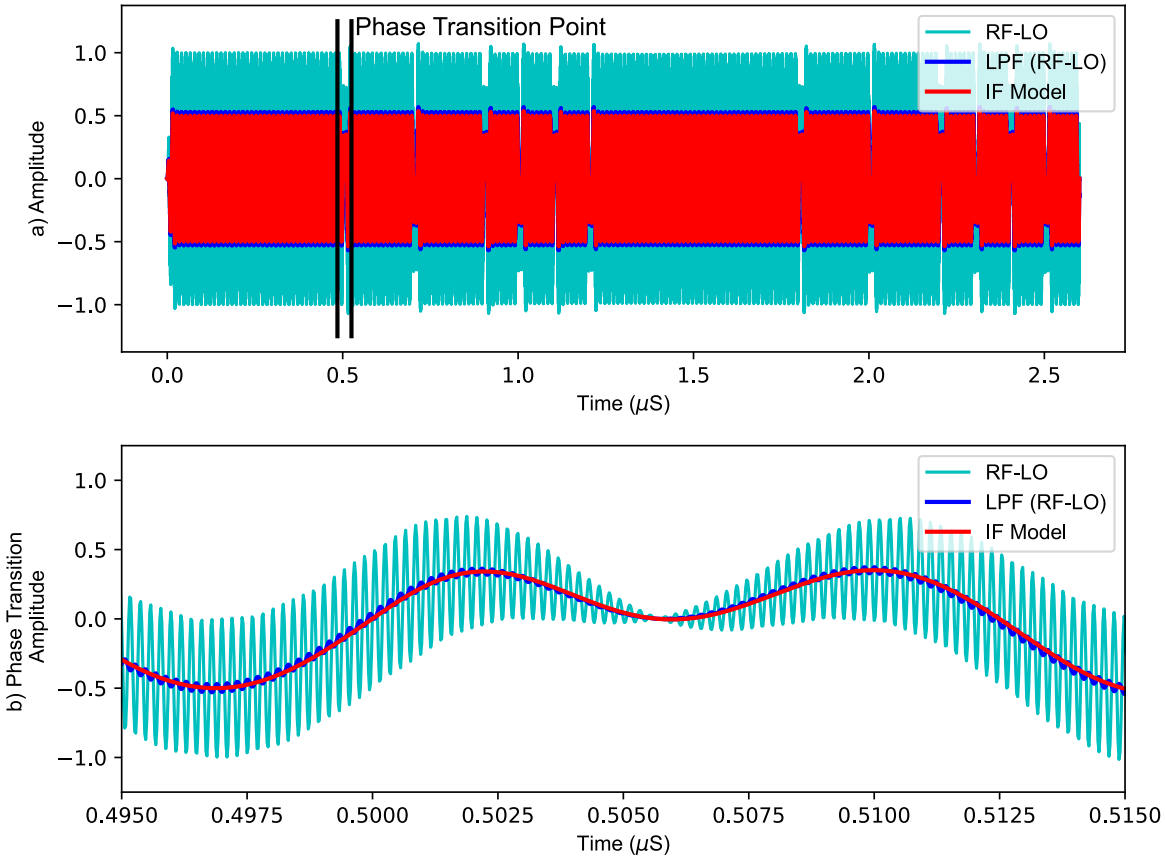

Figure 5.6: a) Band-limited BPSK Barker-13 modulated signal, b) Phase transition point of interest.

to meet the Nyquist criteria for the intermediate frequency plus expected Doppler shift. This greatly reduces the number of samples required for the simulations.

5.4 Target Simulation with IF Model

The IF demodulation of the return signal produced results consistent with target range, size, and expected Doppler frequency shift. The target signatures in the return signal are created using pulse control and modulation based on the range R, radial velocity V_R, and cross-sectional area of each target. Multiple targets are simulated by summing each individual target signature.

5.5 Simulated Target Responses

The specific parameters used for the simulations are given in table 5.4. The intermediate frequency model and radar equations are used to model the transmitted signal. Target reflections

Symbol	Value	Property
f_S	$80.0e6$	Sampling frequency
f_0	$3.0e9$	Carrier frequency
f_{LO}	$2.98e9$	Local oscillator frequency
f_{IF}	$20e6$	Intermediate frequency
T	$25e$-6	PRI
τ	$1.0e$-6	Pulse on time
bw	$20.0e6$	Filter model band-width
C_N	2	Filter model order
M	65	Pulses in CPI
N	$1.04e5$	Sample buffer length
f_C	$1.0e6$	Code chipping frequency

Table 5.4: List of values used for target simulation and CLEAN processing.

are created by time delaying an attenuated replica of the transmitted signal with appropriate phase delay and amplitude attenuation. The target's reflected power is given by Equation 5.29. [30].

$$P_r = \frac{P_t G_t G_r \lambda^2 \sigma}{(4\pi)^3 R^4} \tag{5.29}$$

Where:

- P_r Power received in watts.
- P_t Power transmitted in watts.
- G_t Transmitter antenna gain.
- G_r Receiver antenna gain.
- λ Carrier wavelength in meters.
- σ Radar cross section (RCS) in square meters.
- R Target range to radar antenna in meters.

The signal voltage is calculated by taking the square root of the power amplitude of the ADC converter as given in Equation 5.29 and the time delay of the reflected signal and Doppler frequency shift given by Equations 5.30, and 2.3 respectively.

$$t_0 = \frac{2R}{c} \tag{5.30}$$

The Doppler shift observed in a signal is applied by creating scalar S_{dop} from the radial velocity V_r shown in Equation 5.31. When multiplied with the original frequency the result is the Doppler shifted version.

$$S_{dop} = 1 + \frac{2V_r}{c} \tag{5.31}$$

The pulse repetition frequency for instance is considered to be low enough that any resulting Doppler shift is unobservable and can be ignored in most cases. The effects of the Doppler frequency shift are included in all simulated frequencies and the general form of the base-band modulation is given in Equation 5.32.

$$b(t) = \begin{cases} a_r(t)bit(t) \cdot 2 - 1, & type = AES. \\ a(t)IBH(t), & type = Ipatov - Barker. \end{cases} \tag{5.32}$$

The time delay $t(n)$ of a sample n is given by Equation 5.33 where f_S is the sampling frequency.

$$t(n) = \frac{n}{f_S} \tag{5.33}$$

A single target's modulated, scaled, and delayed signal in the sampled IF domain $x[n]$, is given by Equation 5.34.

$$x[n] = b\left(t(n) - t_0\right) A_{IF}(t(n)) \sqrt{P_r} \tag{5.34}$$

Simulating the reflections from multiple targets is done by independently simulating each target's reflected signature and then summing the results to get a simulated scenario.

5.5.1 Comparative Analysis

Before simulating multiple targets or testing the CLEAN algorithm performance, each signal is simulated with a single virtual target at zero range and zero Doppler shift with an amplitude of 1.0. This is used as the sampled ambiguity function that is modified according to each target's range, velocity, and size. The received signal is analysed by plotting its matched filter output and spectral signature to determine the target's range and Doppler shift as shown in Figures 5.8,

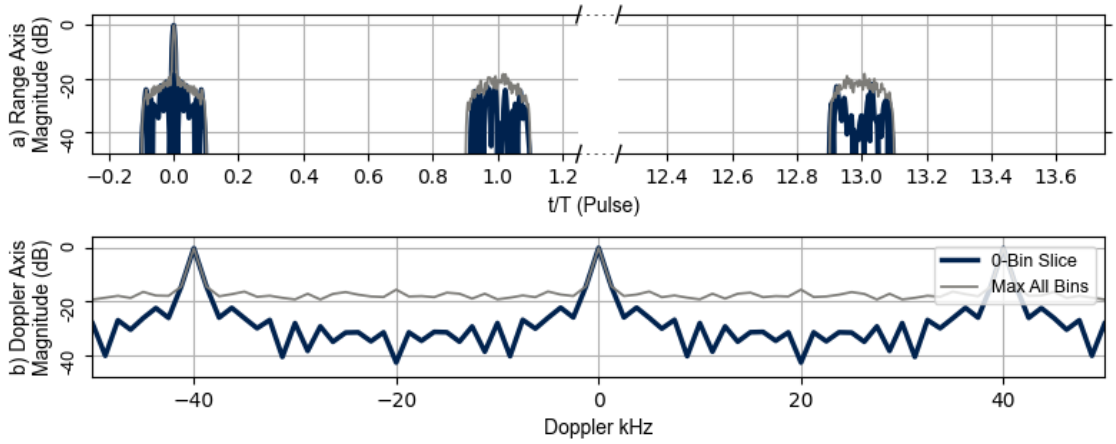

Figure 5.7: AES BPSK maximum ambiguous side lobes in Range and Doppler bin axes.

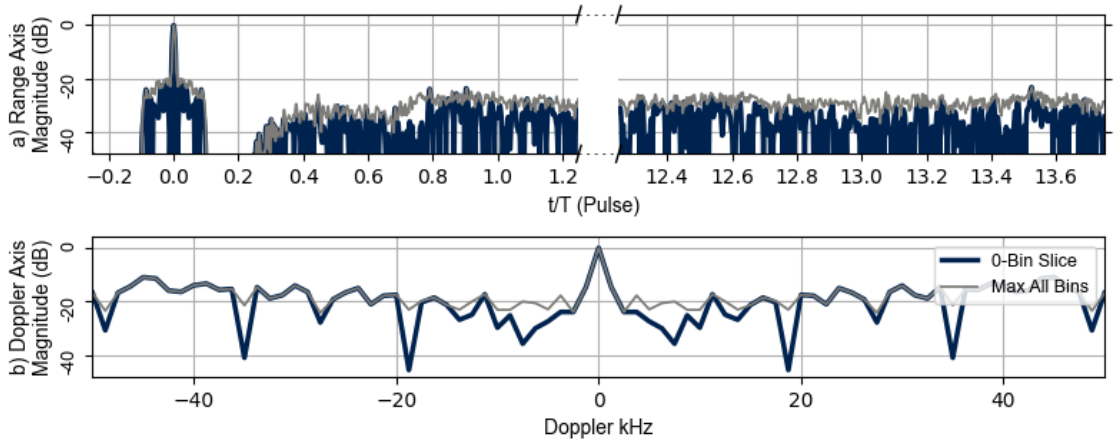

Figure 5.8: RPB maximum ambiguous side lobes in Range and Doppler bin axes.

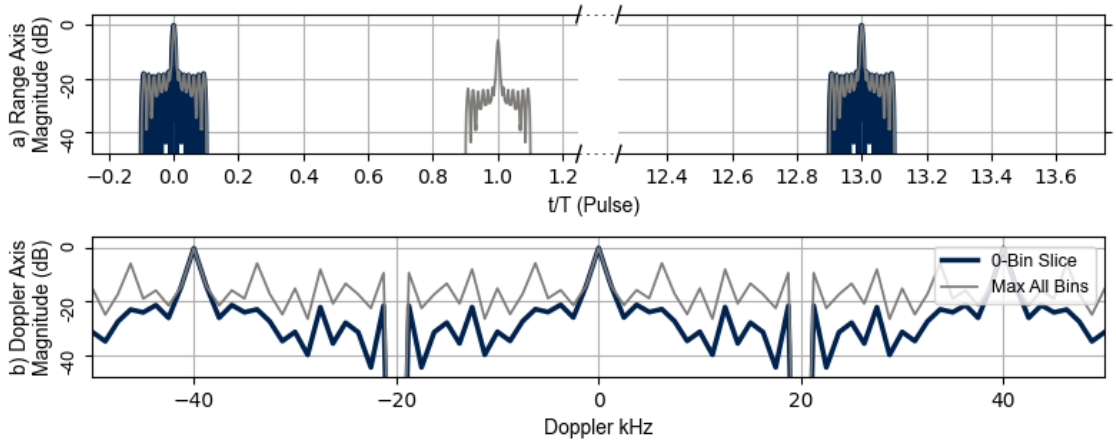

Figure 5.9: IBH maximum ambiguous side lobes in Range and Doppler bin axes.

5.9 and 5.7. The range axis (a) is extended to show any spurious lobes that may occur in the extended range. Figure 5.7 shows the output of the matched filter for a constant PRI signal. The frequency axis (c) is extended and a near replica of the low frequency response occurs at ± 40 kHz. A comparison of Doppler signature from a constant and random PRI BPSK signal is shown in Figure 5.8. It is evident that randomizing the PRI reduced the magnitude of the spurious (ambiguous) Doppler peaks, but randomizing the PRI did increase the signal noise on the range axis and caused higher average side lobes on the Doppler axis. The side lobes are artifacts and referred to as ambiguous energy or noise. The major benefit of using random PRI BPSK signal is that the actual target peak is always the largest peak in the matched filter output.

The CLEAN processing reduced the noise plateau seen in the matched filter response for both the constant and varible PRI signaling. However, the level of the spurious (ambiguous) peak is not reduced at $\pm 40kHz$ as shown in Figure 5.7. It is clear that the mitigation of range ambiguity that occurs using Ipatov-13 Barker-13 hybrid coding, causes a replica target signature to appear a much higher frequency and thus the true target velocity is ambiguous (Doppler ambiguity). Figure 5.9 shows no visible side lobes in the range axis for the zero Doppler shift bins. When the full set of range and Doppler bins is compressed by taking the maximum of all Doppler bins for a given range bin, an ambiguous peak appears, and multiple ambiguous peaks appear along the Doppler axis. Figure 5.9 showcases the fact that the true Doppler frequency caused by target motion is not certain if Ipatov-Barker hybrid coding is used whereas the random PRI BPSK signal is able to resolve the true Doppler shift.

5.6 CLEAN Reprocessing

The Ipatov-13 Barker-13 hybrid coding and AES -192 encryption methods are used to simulate virtual targets having an amplitude 1.0 at zero range, and a second target at a range of $0.3\ T$ having an amplitude -39dB relative to the virtual target. The second target amplitude was sufficiently reduced so that it would not be visible in the matched filter response without additional signal processing. However, the second target's response is observable in the output after the CLEAN algorithm is used. The primary portions of interest in the matched filter response are the true and false target's locations. The false target will be delayed by thirteen pulse periods.

The Doppler range of the matched filter output is adjusted to be slightly greater than the first ambiguous Doppler peak which occurs at the frequency $1.0/PRI = 40kHz$.

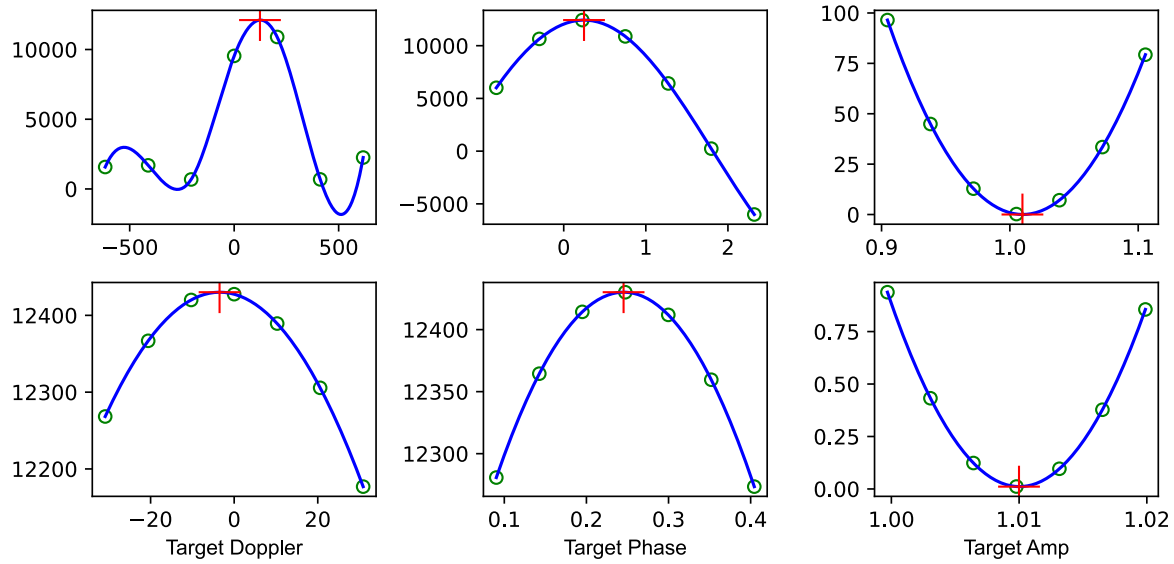

Figure 5.10: CLEAN replica parameter refinement on target 1. Doppler optimizer (Left Column). Phase optimizer (Middle Column). Amplitude optimizer (Right Column).

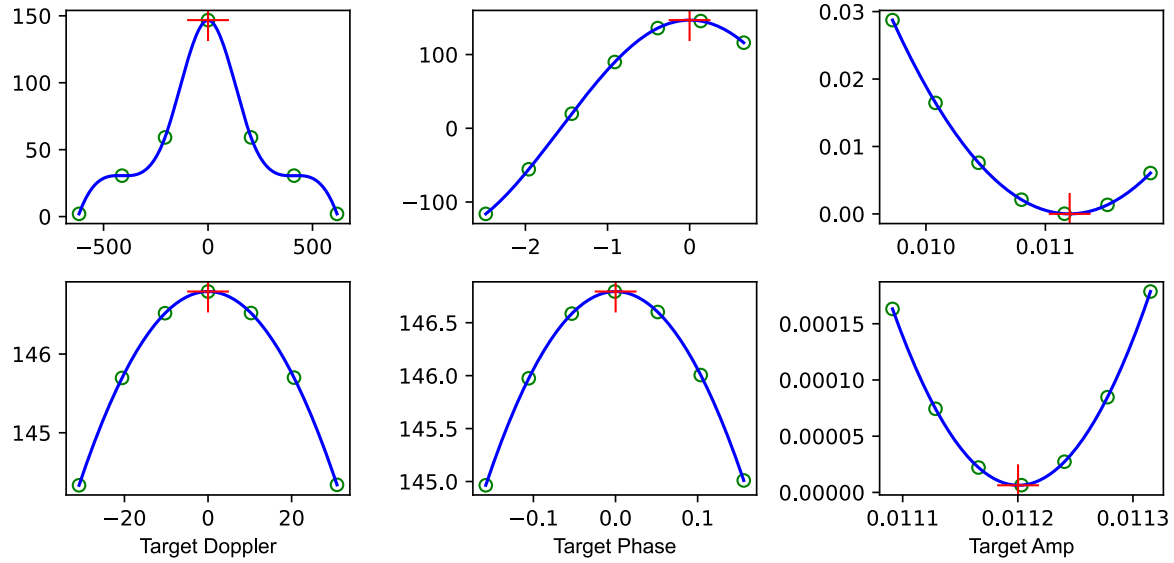

Figure 5.11: CLEAN replica parameter refinement on target 2. Doppler optimizer convergence (Left Column). Phase optimizer convergence (Middle Column). Amplitude optimizer convergence (Right Column).

The AES 192 encrypted signaling causes significant spurious noise and additional false Doppler target lobes that can mask smaller target responses. The original matched filter output

magnitude is plotted after the CLEAN algorithm completes two cycles, once for each target found. The reduction in range lobe levels is visible in both signals in the early and late times of the matched filter response. The very low side lobes of the Ipatov-Barker hybrid are not visible due to axis scale and are considered smaller than a realistic noise floor level. The effective reduction in side lobe levels with a nearly perfect replica is approximately -70 dB. Note that since the signals are sufficiently spaced and are in a noise free environment, CLEAN is able to create and then negate a very accurate replica signature for both targets. The optimizer components of the CLEAN algorithm are shown in Figures 5.10 and 5.11. The search area generated around the coarse values sampled from the quadrature matched filter is shown to converge at the optimal replica parameter for each equation and both targets.

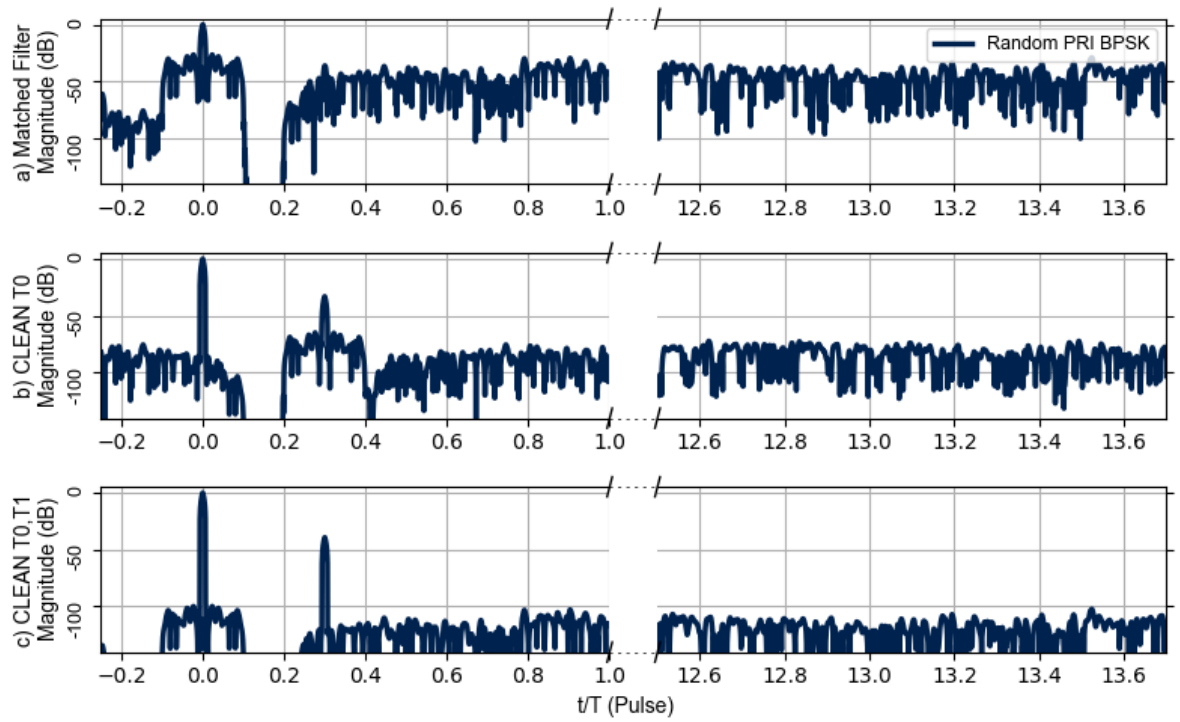

Figure 5.12: a) RPB signal raw matched filter output for one visible and one buried target. b) Single pass of optimized CLEAN on the primary target. c) Second pass of CLEAN on secondary target.

Additionally, the same simulation was run with added noise. Figure 5.16 shows the results of CLEAN on both signals with added noise. The noise floor at approximately -80 dB is consistent in both signals and the limiting effect it has on the reduction from CLEAN is visible.

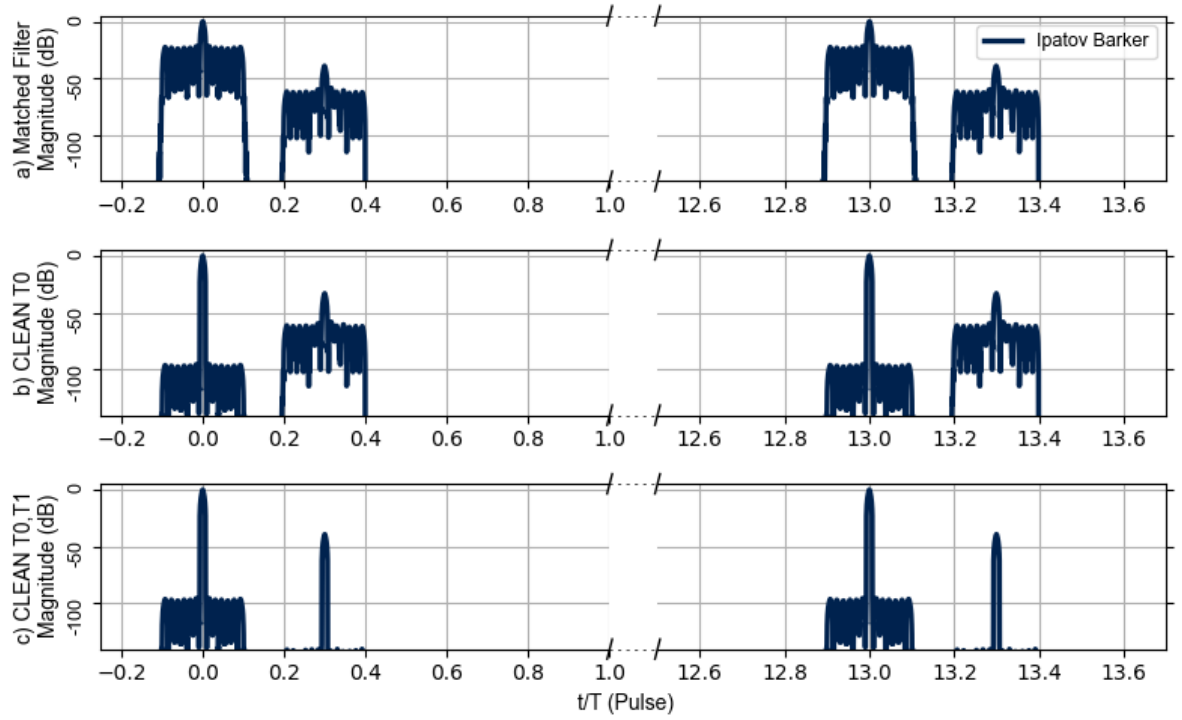

Figure 5.13: a) IBH signal raw matched filter output for one visible and one buried target. b) Single pass of optimized CLEAN on the primary target. c) Second pass of CLEAN on secondary target.

The region between pulse one and pulse twelve on the Ipatov-Barker sequence is fixed to the noise floor while the random PRI BPSK signal shows reduction that stops at the noise floor.

Since CLEAN is dependant on the replica's accuracy for effective ambiguous energy suppression, the band limited filter model's accuracy is directly linked to the effectiveness of the CLEAN algorithm. Figure 5.17 is the result of running CLEAN without a band-limited filter for the base-band replica. The peak to floor performance is decreased from -70 dB to -25 dB because of errors between the negation replica and target reflection signal.

A simulation was set up to test how base-band model accuracy affects CLEAN side lobe energy reduction. The base-band replica was modified by changing the bandwidth of filter used on the digitally generated base-band signal. The difference between the total bandwidth of the simulated received signal and the negation replica filter bandwidth is represented as a percent of bandwidth error. Figure 5.19 represents the results of the test on the Random PRI BPSK hybrid (RPB) and the Ipatov-13 Barker-13 hybrid (IBH) signals. A target signature was

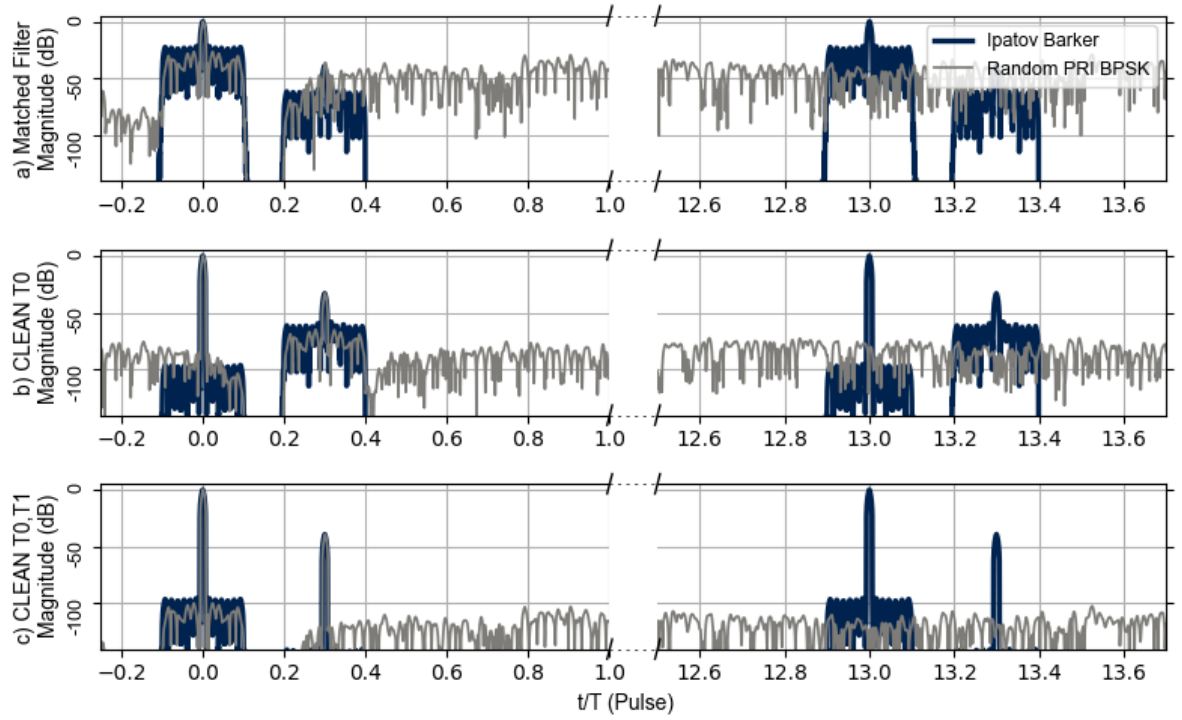

Figure 5.14: Overlay of Ipatov-Barker and the Random Pulse BPSK Hybrids. a) Raw matched filter output for one visible and one buried target. b) Single pass of optimized CLEAN on the primary target. c) Second pass of CLEAN on secondary target.

generated and CLEAN attempted to negate it with varying base-band replicas. A perfect base-band replica will produce nearly perfect negation results. This can be seen where both signals main lobe reduction (MLR) and side lobe reduction (SLR) approach zero (-inf in dB) when the filter bandwidth error is zero. As the base-band replica is distorted by changing the filter bandwidth, the negation replica used by CLEAN no longer matches the signal received causing a reduction in the effectiveness of the CLEAN algorithm. This can be seen as the MLR and SLR performance is diminishes with increasing bandwidth error. The same simulation tests were re-run using injected noise with a SNR set to -50 dB and low pass filter sampled at twice the Nyquest rate. The results of using a signal replica at base-band with error for the CLEAN process (with noise present) are shown in Figure 5.20. In both versions of the test simulation, the performance was nearly identical. As the target's model error increases, there is much less of a reduction in both the main and side lobe signatures using CLEAN. The Ipatov-13 Barker-13 hybrid suffered an increase in side lobes between the range ambiguity interval of pulses 1-12 when significant target model error was present. This is largely due to the fact that

the Ipatov sequence nearly eliminate side lobes between pulses 1-12 after the target and the distortions from CLEAN negatively affect the Ipatov sequences' correlation properties. In both figures CLEAN does reduce the main lobe response in the Ipatov-Barker hybrid, but the side lobe performance was too far above the axes to be visible (rising from approximately -150 dB to -130 dB, effectively a +20 dB loss in side lobe reduction). Since a large portion of the model error test results show a side lobe reduction around -25 dB, an approximation of the expected ambiguous energy reduction from CLEAN with the provided optimization functions would be near -25 dB.

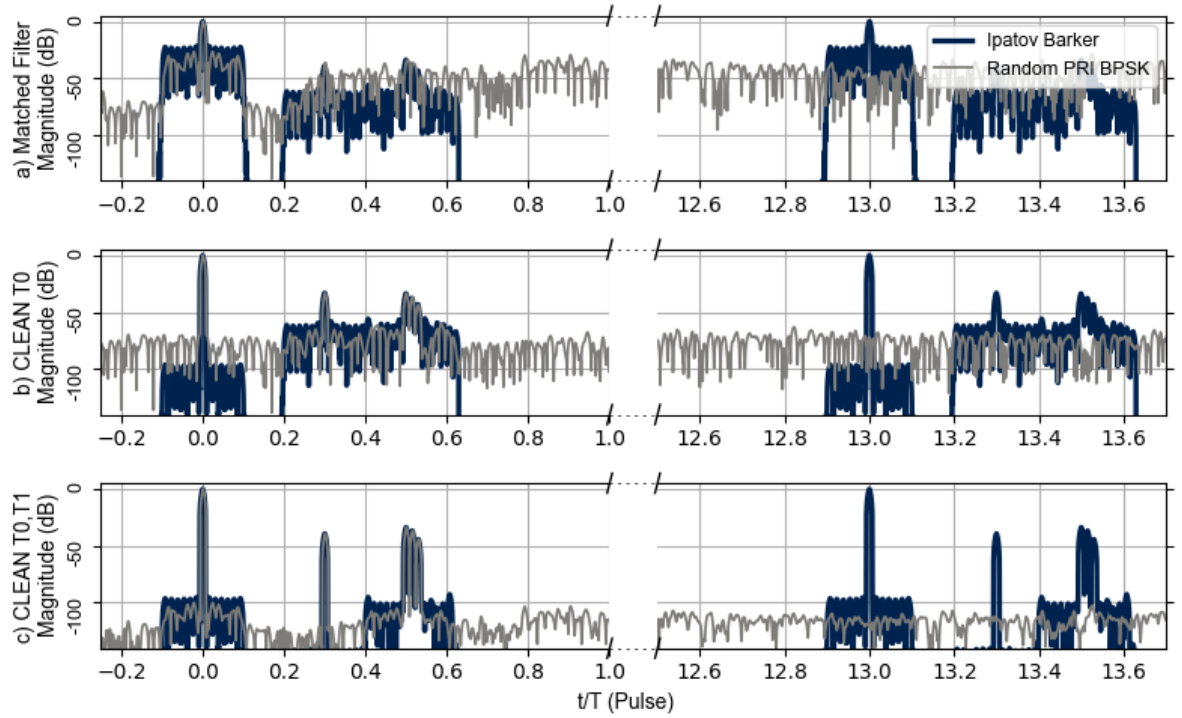

Figure 5.15: Overlay of Ipatov-Barker and the Random Pulse BPSK Hybrids. a) Raw matched filter output for all targets. b) Optimized CLEAN on the primary target. c) Final pass of CLEAN on all targets.

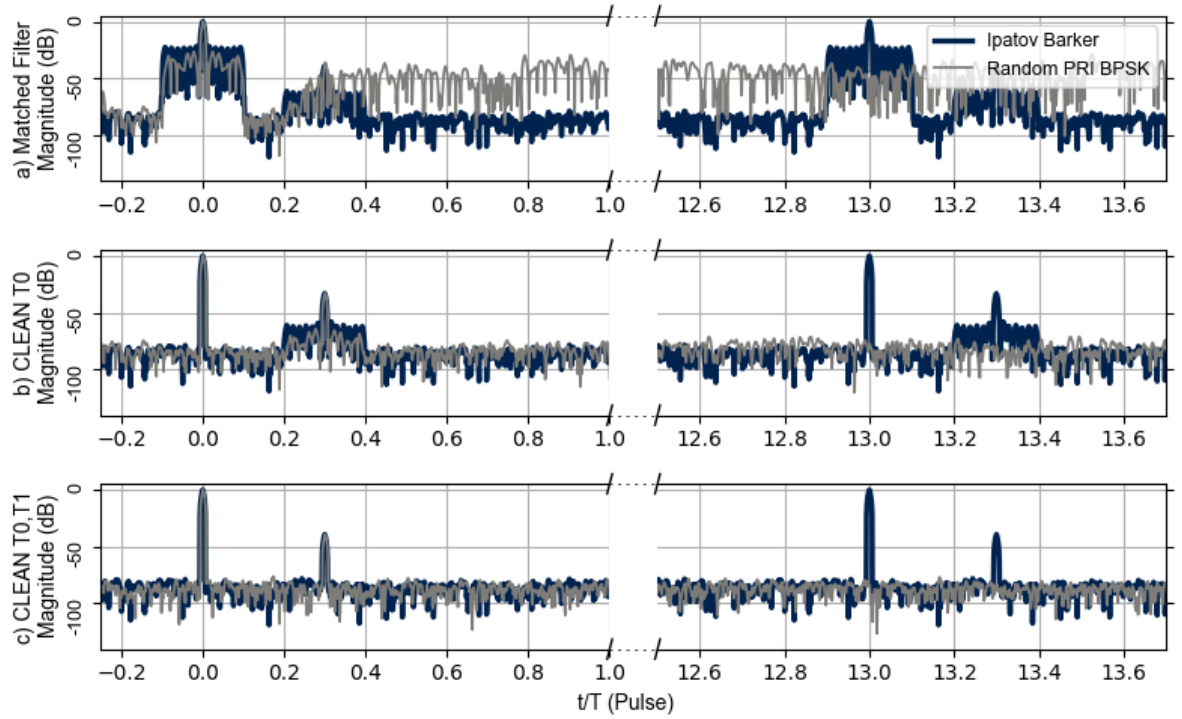

Figure 5.16: Overlay of Ipatov-Barker and the Random Pulse BPSK Hybrids with simulated noise. a) Raw matched filter output for one visible and one buried target. b) Single pass of optimized CLEAN on the primary target. c) Second pass of CLEAN on secondary target.

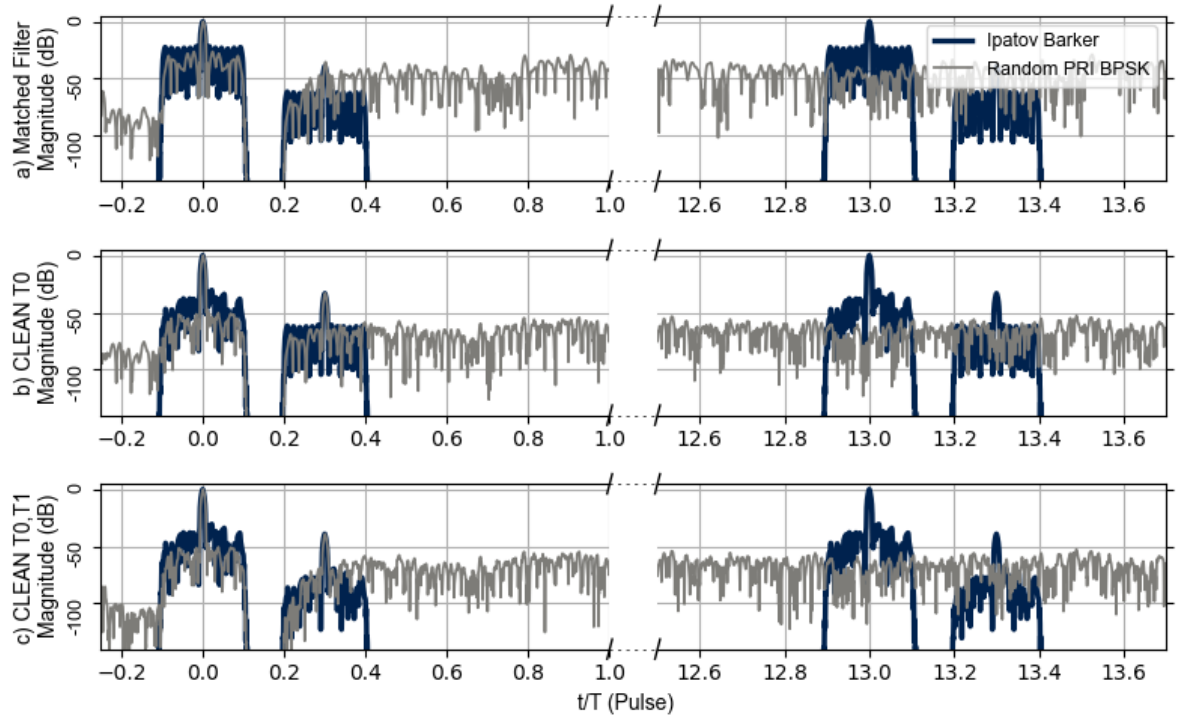

Figure 5.17: Overlay of IBH and RPB signals with no band limited filter model. a) Raw matched filter output for one visible and one buried target. b) CLEAN on the primary target. c) CLEAN on secondary target.

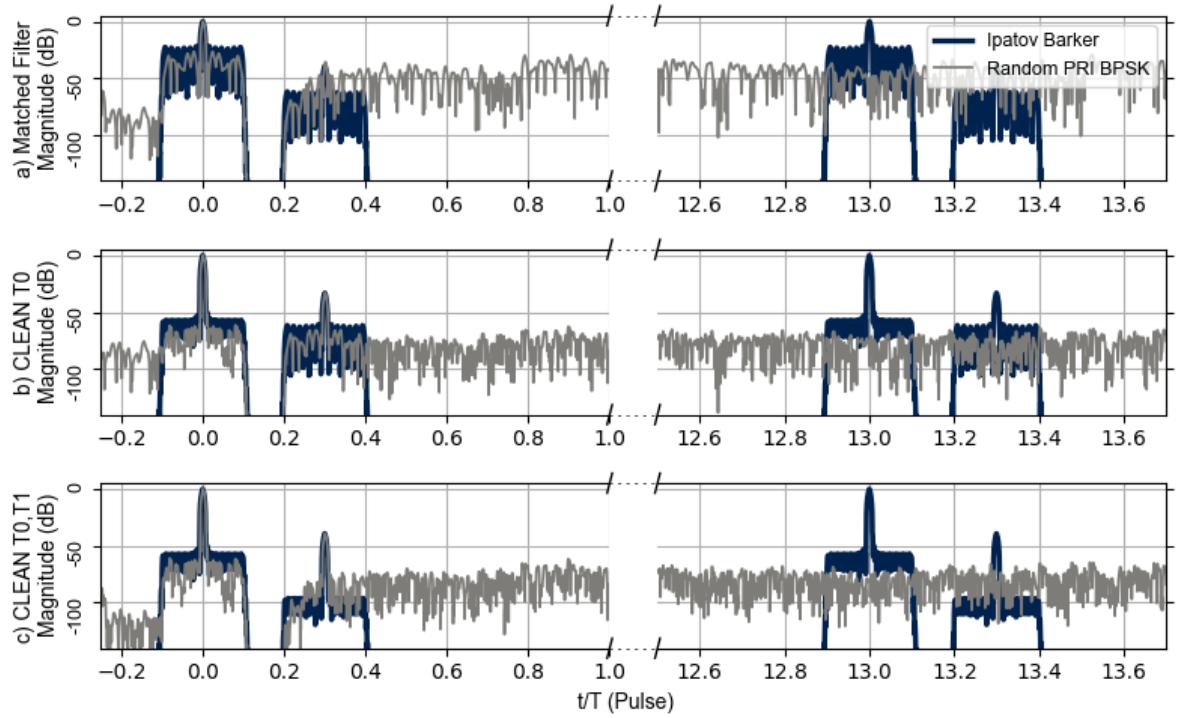

Figure 5.18: Overlay of IBH and the RPB signals with a 1 MHz band model error. a) Raw matched filter. b) CLEAN on the primary target. c) CLEAN on secondary target.

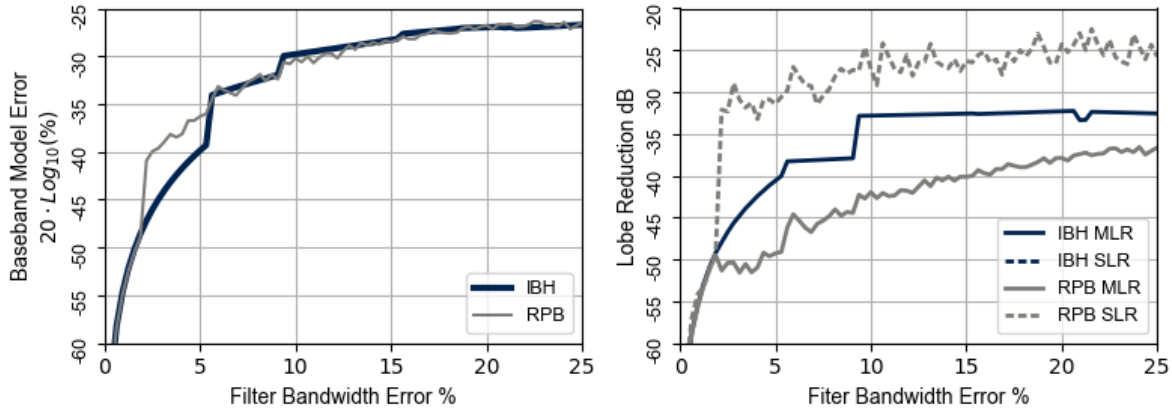

Figure 5.19: base-band replica model error due to bandwidth filter error (left). Peak to floor dB reduction from CLEAN with bandwidth filter model error (right).

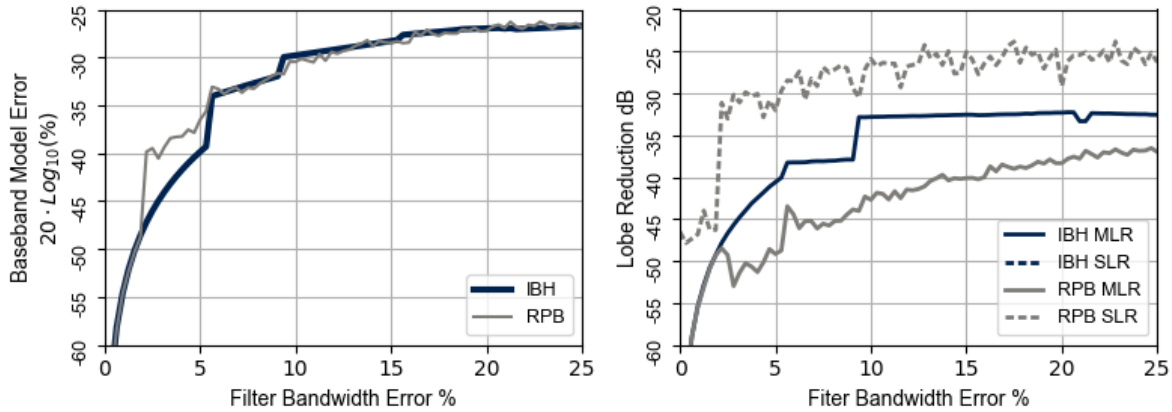

Figure 5.20: base-band replica model error due to bandwidth filter error in noise (left). Peak to floor dB reduction from CLEAN in noise with bandwidth filter model error (right).

Chapter 6

Conclusions and Future Work

6.1 Conclusions

In the simulations, the Ipatov-13 Barker-13 hybrid prevented any false target lobes from appearing until after the time delay associated with the Ipatov-Barker sequence length of thirteen pulses. For simulations done at the intermediate frequencies, CLEAN with the optimization equations was shown to effectively reduce the ambiguities in both the hybrid random signal and the cyclic Ipatov-Barker signal. In simulation with an accurate replica model the maximum reduction from a single iteration of CLEAN seen was approximately -60 dB. Losses from discrete digital sampling, oscillator noise and model errors will reduce the effectiveness of CLEAN. In real implementations, the effective reduction will be less than -60 dB and will most likely be similar to (-25 to -30 dB), shown in the results from the replica model error simulation.

6.2 Future Work

The simulation is limited in its ability to accurately represent the performance of CLEAN with a random signal operating in a real world environment. The results from the simulation require verification with experimental results from a functional radar. Much of the work presented in this thesis provides the ground work for a large amount of testing and algorithm tuning on real data which frustratingly was not currently available. Future work with an s-band radar and an FPGA based BPSK code generator will be used to duplicate the tests done here with real world data. Testing involving the system filter model accuracy would provide insight into the limitations of the CLEAN algorithm. Since it is key to increasing the performance of the CLEAN

algorithm, analysis of the system filter model for the radar could be done in an anechoic chamber. One possibility is increasing the model parameters to include a search space for dynamic filter tuning. A radar performing tracking of targets could use a continuous processing version of CLEAN on identified targets. Instead of post processing signals, if enough parallel hardware (FPGA, ASIC, GPU) is available, the tracked targets can be processed continuously. The CLEAN type algorithms covered have a high sensitivity to signal modeling errors. In order to achieve good ambiguous energy reduction, the generated replica needs to be closely matched with the received target signal. Several contributing factors to modeling error include variation in target amplitude over the CPI, signal filtering effects of the target, non-linear Doppler and target geometry other than planar reflections. Currently the targets are assumed to be nearly constant amplitude for the duration of the CPI and they are assumed to have all their signal emanating from a singular range point. However, a more accurate model would estimate the dynamic effects of the amplitude, phase, and target area. Adaptive models for these parameters could be added to the system to further the accuracy of the target negation process.

Bibliography

[1] Nadav Levanon. “Mitigating Range Ambiguity in High PRF Radar using Inter-Pulse Binary Coding”. In: *IEEE Transactions on Aerospace and Electronic Systems* 45.2 (Apr. 2009), pp. 687–697. ISSN: 2371-9877. DOI: 10.1109/TAES.2009.5089550.

[2] Zouhair Ben Jemaa, Sylvie Marcos, and Safya Belghith. “Optimization of the Radar Ambiguity Function-Application to Chaotic Sequences”. In: *2019 International Conference on Wireless Networks and Mobile Communications (WINCOM), Wireless Networks and Mobile Communications (WINCOM), 2019 International Conference on* (2019), pp. 1 –6.

[3] Surya Prakash Sankuru and Prabhu Babu. “Designing unimodular sequence with good auto-correlation properties via Block Majorization-Minimization method.” In: *Signal Processing* 176 (2020).

[4] Dylan Eustice et al. “Amplifier-in-the-Loop Adaptive Radar Waveform Synthesis.” In: *IEEE Transactions on Aerospace & Electronic Systems* 53.2 (), pp. 826 –836.

[5] Janusz S. Kulpa, Lukasz Maslikowski, and Mateusz Malanowski. “Filter-Based Design of Noise Radar Waveform With Reduced Sidelobes.” In: *IEEE Transactions on Aerospace & Electronic Systems* 53.2 (2017), pp. 816 –825.

[6] Mojtaba Shahrab and Hossein Soleimani. “Secure hybrid pulse compression as a technique against jamming in radar systems.” In: *Physical Communication* 43 (2020). ISSN: 1874-4907.

[7] Nathaniel R. Carson et al. *Enhancement and Defense of GPS Navigation Using Signal Processing Techniques. [electronic resource]*. 2018. URL: http://spot.lib.auburn.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=cat07161a&AN=aul.4996524&site=eds-live&scope=site.

[8] Krzysztof Kulpa. "The CLEAN type algorithms for radar signal processing". In: *2008 Microwaves, Radar and Remote Sensing Symposium*. 2008, pp. 152–157.

[9] Troy Kilpatrick, I. Dennis Longstaff, and I. Vaughan L. Clarkson. "Sidelobe suppression and super resolution for MIMO imaging radar". In: *2013 International Conference on Radar*. 2013, pp. 362–367.

[10] P. Berestesky and E.H. Attia. "Sidelobe Leakage Reduction in Random Phase Diversity Radar Using Coherent CLEAN." In: *IEEE Transactions on Aerospace and Electronic Systems, Aerospace and Electronic Systems, IEEE Transactions on, IEEE Trans. Aerosp. Electron. Syst* 55.5 (2019), pp. 2426 –2435.

[11] Wang Jie et al. "A Novel Scheme for Ambiguous Energy Suppression in MIMO-SAR Systems." In: *IEEE Geoscience and Remote Sensing Letters, Geoscience and Remote Sensing Letters, IEEE, IEEE Geosci. Remote Sensing Lett* 12.2 (2015), pp. 344 –348.

[12] M. A. Richards, Jim Scheer, and William A. Holm. *Principles of modern radar: Basic principles*. SciTech Pub., 2010, pp. 4–5. ISBN: 9781891121524.

[13] M. A. Richards, Jim Scheer, and William A. Holm. *Principles of modern radar: Basic principles*. SciTech Pub., 2010, pp. 538–540. ISBN: 9781891121524.

[14] I. Tsmots et al. "Method of Synthesis and Practical Realization of Quasi-Barker Codes". In: *2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT)*. Vol. 2. 0. 2019, pp. 76–79.

[15] M. A. Richards, Jim Scheer, and William A. Holm. *Principles of modern radar: Basic principles*. SciTech Pub., 2010, pp. 165–201. ISBN: 9781891121524.

[16] M. A. Richards, Jim Scheer, and William A. Holm. *Principles of modern radar: Basic principles*. SciTech Pub., 2010, pp. 22–24. ISBN: 9781891121524.

[17] M. A. Richards, Jim Scheer, and William A. Holm. *Principles of modern radar: Basic principles*. SciTech Pub., 2010, pp. 274–275. ISBN: 9781891121524.

[18] Jan Matuszewski. "Jamming efficiency of land-based radars by the airborne jammers". In: *2018 22nd International Microwave and Radar Conference (MIKON)*. 2018, pp. 324–327. DOI: 10.23919/MIKON.2018.8405214.

[19] Mohammad Reza Zakerhaghighi, Mohsen Mivehchy, and Mohammad Farzan Sabahi. "Implementation and Assessment of Jamming Effectiveness Against an FMCW Tracking Radar Based on a Novel Criterion". In: *IEEE Transactions on Aerospace and Electronic Systems* 56.6 (2020), pp. 4723–4733. DOI: 10.1109/TAES.2020.3000001.

[20] A. Kawalec and R. Owczarek. "Radar emitter recognition using intrapulse data". In: *15th International Conference on Microwaves, Radar and Wireless Communications (IEEE Cat. No.04EX824)*. Vol. 2. 2004, 435–438 Vol.2. DOI: 10.1109/MIKON.2004.1357059.

[21] Sebastian Alphonse and Geoffrey A. Williamson. "On Estimating Nonlinear Frequency Modulated Radar Signals in Low SNR Environments". In: *IEEE Transactions on Aerospace and Electronic Systems* 57.3 (2021), pp. 1793–1802. DOI: 10.1109/TAES.2021.3050649.

[22] Altan Alparslan and Korkut Yegin. "A fast ELINT receiver design". In: *2016 European Radar Conference (EuRAD)*. 2016, pp. 217–220.

[23] Zhang-Meng Liu. "Recognition of Multifunction Radars Via Hierarchically Mining and Exploiting Pulse Group Patterns". In: *IEEE Transactions on Aerospace and Electronic Systems* 56.6 (2020), pp. 4659–4672. DOI: 10.1109/TAES.2020.2999163.

[24] Amir Almslmany and Tamer H. M. Soliman. “Advanced airborne system for air traget detection and spoofing jammers”. In: *2016 Fourth International Japan-Egypt Conference on Electronics, Communications and Computers (JEC-ECC)*. 2016, pp. 71–74. DOI: 10.1109/JEC-ECC.2016.7518970.

[25] Chang Zhou et al. “Anti-intermittent sampling repeater jamming method based on convex optimization techniques”. In: *2016 CIE International Conference on Radar (RADAR)*. 2016, pp. 1–5. DOI: 10.1109/RADAR.2016.8059595.

[26] M. A. Richards, Jim Scheer, and William A. Holm. *Principles of modern radar: Basic principles*. SciTech Pub., 2010, pp. 817–830. ISBN: 9781891121524.

[27] D.O.D. GPS NAVSTAR. “NAVSTAR GPS Space Segment/ User Segment L1C Interfaces”. In: 2021.

[28] M. A. Richards, Jim Scheer, and William A. Holm. *Principles of modern radar: Basic principles*. SciTech Pub., 2010, pp. 287–303. ISBN: 9781891121524.

[29] National Institute of Standards and Technology. *Advanced Encryption Standard (AES)*. en. Tech. rep. Federal Information Processing Standard (FIPS) 197. U.S. Department of Commerce, Nov. 2001. (Visited on 01/25/2020).

[30] M. A. Richards, Jim Scheer, and William A. Holm. *Principles of modern radar: Basic principles*. SciTech Pub., 2010, pp. 59–84. ISBN: 9781891121524.