Investigation of a Novel Software Based Laboratory Jammer Architecture

by

Chirag Hingwala, B. Eng

A thesis submitted to the Faculty of Graduate and Postdoctoral
Affairs in partial fulfillment of the requirement
for the degree of

Master's of Applied Science
In
Electrical and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering
Carleton University
Ottawa, Ontario

Your file Votre référence
ISBN: 978-0-494-83032-1
Our file Notre référence
ISBN: 978-0-494-83032-1

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

DRFM jammers are important tools used in the development of ECM. Unfortunately, most commercially available DRFM jammers often do not give the full flexibility necessary for the complete study of jamming waveforms. This thesis studies a novel software based jammer architecture that allows users to create the input radar signal, and then subject them to various jamming techniques. The specific jamming parameters such as jamming duration and technique, pull-off distances and velocities, and pull-off direction, are easily adjusted in the designed Jamming Module software. Three artificial radar signals were created to represent typical early warning, surveillance and fire control radar systems. The signals were sampled and digitally down converted by the jammer to obtain the baseband in-phase and quadrature-phase data. Using threshold detection, the simulated radar pulse leading edges were found. Depending on the selected jamming profile, the radar pulse data was modulated in frequency and/or time delayed, or replaced with narrow band noise of a particular bandwidth and duration. The digital output of the jammer was analyzed and compared to the desired jamming waveform. Although a fixed frequency offset attributed to the hardware was discovered for small pulse widths, the particular method of applying artificial Doppler at baseband was shown to be effective, and thereby eliminates the traditional requirement for a variable LO during signal up conversion. While the throughput time of the present configuration was found to be too long for practical applications, the processing speed of the Jamming Module was not the limiting factor. The software based jammer was shown to be a viable concept, and this work may serve as a foundation to build upon.

Acknowledgements

I would like to thank Professor Jim Wight at Carleton University for his guidance and encouragement throughout my research. Without his efforts, many of the research opportunities I had would not have been available.

Secondly, I would like to acknowledge the Radar and Electronic Warfare Section at Defence Research and Development Canada (Ottawa). In particular, Dr. Jeff Lange was instrumental in helping develop the key ideas for this thesis and providing technical information to keep the work accurate and relevant.

I would like to recognize Dr. Dipak Roy, Chairman of D-TA Systems Incorporated, for allowing me to use the D-TA laboratory and facilities. In addition to providing all the equipment required for this thesis, many engineers at D-TA offered advice and practical expertise that allowed me to progress my work. I am grateful for their efforts not only in direct assistance with my thesis, but also for making me feel part of the D-TA team during my time with them.

Last, but certainly not least, I appreciate the continuous support and encouragement from my Family and Friends. In particular, my girlfriend Amala, endured countless hours of conversation about radars and jammers, and now may be considered a subject matter expert in her own right!

Table of Contents

Author's Declaration i

Abstract ii

Acknowledgements iii

Table of Contents iv

List of Tables vii

List of Figures viii

List of Abbreviations xi

Chapter 1 Introduction 1

1.1 Electronic Warfare 1

1.2 Problem Statement 2

1.3 Objectives 4

1.4 Contributions 5

1.5 General Scenario 5

1.6 Research Method and Thesis Organization 8

Chapter 2 Theory and Prior Research 10

2.1 Evolution of Radar and ECM 10

2.2 Modern Radars 14

2.3 Modern DRFM Jammers 16

2.4 ESM 19

2.5 Jamming Techniques 22

2.5.1 Disruptive Techniques 22

2.6 Deceptive Techniques 25

2.6.1 Angle Deception 28

2.6.2 Advanced Techniques 28
2.7 Classification of Radar 30
2.7.1 Conventional Pulsed Radar 30
2.7.2 Doppler Processing Radar 33
2.7.3 Pulse Compression 40
2.8 Radar Range Equation 43
2.9 Jamming Equations 45
2.10 Prior Research 48
Chapter 3 Jammer Simulation 53
3.1 Design and Purpose 53
3.2 Key Assumptions and Limitations 54
3.3 Creation of Radar Signals 55
3.4 False Target Profiles 62
3.5 Application of False Target Profiles and Noise 72
3.6 Simulation Results 74
3.7 Areas of Concern 79
3.8 Summary 80
Chapter 4 Implementation 81
4.1 General 81
4.2 Hardware Architecture 83
4.2.1 Production of Input Radar Signals 83
4.2.2 Analog to Digital Conversion 85
4.3 Software Architecture 88
4.3.1 General 88

4.3.2 Customized Jamming Software 89
4.4 Up Conversion 92
4.5 Real Time Implementation Challenges 95
4.6 Summary 97
Chapter 5 Results 98
5.1 General 98
5.2 Early Warning Radar 99
5.3 Fire Control Radar 102
5.3.1 Radar Signal with High SNR 102
5.3.2 Radar Signal with 10 dB SNR 109
5.4 Surveillance Radar 114
5.5 Throughput Calculations 119
5.6 Summary 124
Chapter 6 Conclusion 126
6.1 Summary of Work 126
6.2 Contribution 127
6.3 Noted Limitations and Future Work 128
6.4 Final Remarks 130
Appendix A – Oscilloscope and Spectrum Analyzer Plots 131
Appendix B – Results for Fire Control Radar Without Noise 136
Appendix C – Results for Fire Control Radar with 10 dB SNR 140
Appendix D – Results for Surveillance Radar with 10 dB SNR 144
References 146

List of Tables

Table 1.1: Typical radar operating parameters 7
Table 2.1: IEEE standard frequency bands in microwave and millimeter ranges 16
Table 3.1: Summary of parameters for created radar signals 61
Table 3.2: User controlled inputs variables for simulated jamming techniques 63
Table 3.3: Doppler results for six pulses after applying profile 3 to fire control radar 76
Table 3.4: Doppler results for six pulses after applying profile 4 to surveillance radar ... 77
Table 4.1: DDC parameters for various decimation rates assuming ADC sampling rate of 32 Msps 87
Table 5.1: Results of noise jamming 101
Table 5.2: Baseband frequency offset for raw radar data used to make the continuous pulse train for the fire control radar 111
Table 5.3: Frequency offset for each of the pulses looped to produce the pulse train 113
Table 5.4: Jamming results for applying profile 4 against surveillance radar 115
Table 5.5: Measured and expected times between ADC sampling and output of ADC Server Module 121
Table 5.6: Jamming Module throughput times per block of data for implemented radar versus jammer scenarios 122

List of Figures

Figure 1.1: Example scenario involving single self-screening aircraft moving towards a point of interest 7
Figure 2.1: Architecture of DRFM jammer 17
Figure 2.2: Signal sorting process in a RWR 21
Figure 2.3: Noise bandwidth comparison for spot versus barrage noise jamming 24
Figure 2.4: RGPO profile showing pull-off of jamming pulse from true echo 26
Figure 2.5: Generation of jamming pulse created by the superposition of false targets produced on four independent channels 29
Figure 2.6: Conventional pulsed radar waveform 31
Figure 2.7: Creation of range and Doppler ambiguities due to PRF selection 35
Figure 2.8: Spectrum of non-coherent versus coherent pulse train of N pulses 36
Figure 2.9: Representation of reference and received signals in the complex plane 38
Figure 2.10: Frequency response illustration of single versus double delay line cancellers 38
Figure 2.11: Frequency response illustrations of Doppler filter bank 40
Figure 2.12: Example of linear FM up-chirp and down-chirp 41
Figure 2.13: DRFM architecture using a channelized receiver 49
Figure 2.14: An improved channelized receiver used in DRFM hardware 50
Figure 2.15: Digital Up Conversion process 50
Figure 2.16: Block diagram showing the relationship of the JCU, TG and DRFM 51
Figure 3.1: Proposed software jammer architecture 54
Figure 3.2 a & b: Early warning radar signal power and frequency plot for a pulse train of five pulses 57
Figure 3.3 a & b: Pulse compressed surveillance radar signal power and frequency plot for a pulse train of 3 pulses 59
Figure 3.4 a & b: Fire control radar signal power and frequency plot for a pulse train of 10 pulses 60
Figure 3.5: Close-up of main lobe from fire control radar signal frequency plot 61

Figure 3.6 a & b: Profile 1 - False target timing and velocity information required for a parabolic RGPO 66
Figure 3.7 a & b: Profile 2 - False target timing and velocity information required for a linear VGPO 68
Figure 3.8 a & b: Profile 3 - False target timing and velocity information required for a down-range CRV 70
Figure 3.9 a & b: Profile 4 - False target timing and velocity information required for an up-range CRV 71
Figure 3.10: Jammer output pulses power and frequency plots 75
Figure 3.11: Overlaid frequencies of jammer pulses for received radar pulses 76
Figure 3.12 a &b: Overlaid IF spectrums for FM Chirp. Figure b shows a zoomed in view of the boxed area 78
Figure 4.1: D-TA sensor processing system components 82
Figure 4.2: DTA-2300 and DTA-1000 used in the implementation of the software jammer 83
Figure 4.3: DTA-2300 packet structure showing 7 frames of data 85
Figure 4.4: Spectrum illustrations of the ADC and DDC process 87
Figure 4.5: Data structure breakdown between software modules 89
Figure 4.6: Jamming Module software stages 92
Figure 4.7: Spectrum illustrations of the DUC and DAC process 94
Figure 5.1: Frequency of noise generated in I_j and Q_j channels 100
Figure 5.2: Power and timing of received radar and transmitted jammer pulses 101
Figure 5.3 a & b: Frequency output of jammer applying profile 3 against fire control radar without additional noise, data decimation by 2 103
Figure 5.4: Frequency output of jammer applying profile 3 against fire control radar without additional noise, using data decimation by 2, 524k point FFT and offset correction 105
Figure 5.5 a & b: Frequency output of jammer applying profile 3 against 5μs fire control radar without additional noise, using data decimation by 2, 65k point FFT and 524k point FFT 107

Figure 5.6 a & b: Time delay output of jammer applying profile 3 against fire control radar for decimation by 2 and 32 108
Figure 5.7 a & b: Frequency output of jammer applying profile 3 against fire control radar with 10 dB SNR, data decimation by 2 110
Figure 5.8: Generated IF signal with a 10 dB SNR 112
Figure 5.9: Frequency output of jammer applying profile 3 against fire control radar with 10 dB SNR, data decimation by 2, individual pulse correction applied 113
Figure 5.10: Baseband spectrum of surveillance radar 115
Figure 5.11 a & b: Frequency and time delay output of jammer applying profile 4 against surveillance radar with 10 dB SNR, data decimation by 2 117
Figure 5.12 a & b: Signal power measurement for decimation by 4 illustrating power fluctuations during the leading and trailing edges 118
Figure 5.13: Throughput time measurement locations 120

List of Abbreviations

ADC	Analog to Digital Converter
CARDS	Canadian Advanced Radar Deception System
COTS	Commercial-Off-The-Shelf
CPI	Coherent Processing Interval
CRV	Coordinated Range-Velocity
CW	Continuous Wave
DAC	Digital to Analog Converter
DDC	Digital Down Converter
DRDC	Defence Research and Development Canada
DRFM	Digital Radio Frequency Memory
DSP	Digital Signal Processing
EW	Electronic Warfare
ECM	Electronic Counter Measures
EPM	Electronic Protection Measures
EA	Electronic Attack
ECCM	Electronic Counter Counter Measures
EP	Electronic Protection
ERP	Effective Radiated Power
FFT	Fast Fourier Transform
FML	Frequency Memory Loop
FPGA	Field Programmable Gate Array
IF	Intermediate Frequency
JCU	Jammer Control Unit
JSR	Jamming to Signal Ratio
LO	Local Oscillator
LPF	Low Pass Filter
NCO	Numerically Controlled Oscillator
PCR	Pulse Compression Ratio
PDR	Pulse Doppler Radar
PRF	Pulse Repetition Frequency
PRI	Pulse Repetition Interval
PW	Pulse Width
RBM	Range Bin Masking
RF	Radio Frequency
RWR	Radar Warning Receiver
RGPO	Range Gate Pull Off
SNR	Signal to Noise Ratio
TG	Techniques Generator
VBM	Velocity Bin Masking
VPGO	Velocity Gate Pull Off

Chapter 1

Introduction

1.1 Electronic Warfare

Electronic Warfare (EW) is an essential component of military operations. Virtually all modern communication, navigation, and sensor equipment operate within specific regions of the electromagnetic spectrum. For this reason, the control of the spectrum at the expense of the enemy is often critical to mission success. By definition, EW is any action to control the electromagnetic spectrum [4]. EW itself is a vast subject area that encompasses everything from intelligence gathering to platform protection. It can be broken down into three main areas: Electronic Attack (EA), Electronic Protection (EP), and Electronic Support (ES) measures. EA refers to any Electronic Counter Measures (ECM) to protect the targeted platform, while EP is defined as Electronic Counter Counter Measures (ECCM) and refers to methods to render the ECM ineffective. As an example, chaff can be considered a form of EA, while use of frequency agility in radar is a form of EP. The field of ES is concerned with sensing emitter signals for the purpose of threat recognition, as done in a Radar Warning Receiver (RWR).

Air platforms use a combination of tactics and technology to prevent or limit their detection, tracking, and targeting. A radar jammer is a component found on most modern combat aircraft and is an example of a technological innovation. When active, these jammers attempt to confuse hostile radar systems by hiding the true echo or producing numerous false targets. However, as technology evolves and more capable radar systems

are fielded, there is a continual requirement to ensure that jammers can overcome radar capabilities. In this light, research in the field of EW is a never-ending quest to stay informed and ahead of the adversary.

Modern radar systems use complex waveforms and coherent processing techniques to limit the effectiveness of jammers. Radar receivers may also be equipped to detect poorly created jamming waveforms, and thus can not only disregard such returns but actually home in on jamming. Consequently, in order to remain effective, modern jammers must, among other things, use matched waveforms to the radar receiver, ensure proper coordination of Doppler modulations and time delays, and apply gradual and appropriate amplitude modulation for the duration of jamming. Compared to their analog predecessors, Digital Radio Frequency Memory (DRFM) jammers are able to copy, modify, and re-transmit multiple copies of the radar signals for EA purposes. Due to their success against present radars, virtually all modern jammers are based on DRFM technology.

1.2 Problem Statement

Well before a jammer system is fielded for use in a real-life tactical scenario, many hours are spent in simulation to investigate and test the effectiveness of different jammer waveforms and techniques. To validate the results of the simulation, the most promising jamming techniques are tested in ground and flight based trials using laboratory jammer systems. These laboratory types of jammers perform the same functions as their tactical jammer counterparts in a controlled setting and provide vital

findings to research and defence scientists. For example, Defence Research and Development Canada (DRDC) uses a system known as the Canadian Advanced Radar Deception System (CARDS) to perform this function. However, since its development, signal processing capabilities have progressed and CARDS is no longer representative of what is possible with current technology.

As an alternative, laboratory-type DRFMs can also be commercially purchased. Unfortunately, they have three main drawbacks. First, they are often "black boxes", with no ability for the user to study or change how the jamming waveforms are being produced. Secondly, there are limitations on inputs/outputs by the jammer. In other words, the user is confined to the pre-programmed jamming profiles without any ability to modify, adapt, or add to existing capabilities. Even if users were able to locate the source code, Field Programmable Gate Array (FPGA) programming requires specialized knowledge and equipment compared to commonly used C++ coding. Thirdly, laboratory DRFM jammers are extremely costly due to the unique and sensitive nature of the application. Proprietary information prevents the user from modifying jamming algorithms to allow for suitable experimentation.

Thus, there is a requirement to develop a flexible and cost effective laboratory jammer that facilitates research and development of future DRFM jammers. The challenge is the implementation of a versatile jammer that empowers the user with full control of production of the jamming waveform without overwhelming them with difficult or cumbersome programming. The proposed solution is an implementation of a

so called 'software' jammer, where signal processing functions are done by software external to the jammer FGPA. Compared to other known DRFM systems, the jamming software is based on simple C++ code which allows the user to easily adjust or change parameters related to jamming.

1.3 Objectives

The main objective of this thesis was to investigate the hardware and software architecture required for the implementation of a single channel software jammer. This was achieved by using a generalized Commercial-Off-The-Shelf system in conjunction with a newly created application specific software module to perform jammer functions. The hardware platform selected was the D-TA suite of sensor processing equipment. Special attention was given to the development and verification of software algorithms such that they created the desired jamming waveforms. Furthermore, the software algorithms were designed to be easily modifiable for changing radar and scenarios, as well as scalable to allow for new techniques and additional channels. Although a full implementation of the jammer was not completed, data rates and system limitations of the jammer in its present state are documented, and areas for future work are noted.

As preliminary work, it was important to study how radar systems operate. This included examining different radar waveforms, trends in modern radar systems, as well as common radar processing and detection methods. Similarly, traditional and modern radar jammers were also researched, including a number of different jamming techniques. The required background knowledge is included in this thesis.

1.4 Contributions

The main difference between the jammer developed in this thesis and existing solutions is that the jamming algorithms are written in C++ software, as opposed to being coded in FPGA firmware. In this manner, the user, as opposed to the developer, has full control over the production of the jamming waveform. Furthermore, modular software architecture will allow for the addition of new DSP modules and expansion of the system, as desired by the user. The newly created jamming software is intended to be a stepping point for further development.

This thesis also validates a baseband algorithm proposed by Lange [20] [21] to produce artificial Doppler modulations. By creating Doppler modulations at baseband, the traditional requirement for a variable Local Oscillator (LO) during signal up conversion is eliminated.

1.5 General Scenario

The general scenario of interest is a single self-screening aircraft moving into a hostile radar environment towards a point of interest, as illustrated in Figure 1.1. Typically, the aircraft can expect to confront a layered defence consisting of different types of radar. First, early warning (long range) radar will detect the threat approaching the area of operation. These types of radar are typically pulsed, low frequency (S-band), low Pulse Repetition Frequency (PRF), high power, and scan 360 degrees in azimuth. Since these radars are normally ground based and stationary, there is no restriction on

size and a large amount of power can be supplied to them. Consequently, early warning radars have the ability to detect targets hundreds of kilometers away.

As the aircraft continues to approach, the information from the early warning radar is passed to surveillance radars covering the specific sectors. Their main purpose is to search a particular volume of space and locate the positions of targets. Surveillance radars may establish target tracks to determine aircraft intent and begin the targeting process. Typically, surveillance radars are capable of track-while-scan operations, allowing them to monitor up to hundreds of aircrafts, with a limited range normally under 100 kilometers. The waveform can be pulsed, or can employ intra-pulse modulations to give finer range resolution while maintaining a long surveillance range. Typically, surveillance radars operate in the C-band.

Finally, the aircraft can expect to confront fire control radars. Fire control radar represents a high level of threat since they are often used by weapons systems. To speed the acquisition process, information can be passed from the surveillance radar to narrow down the volume of search for the target. The fire control radar uses a narrow pencil beam, and once it has established the target's position, it remains locked on it. For example, Surface to Air Missile batteries use fire control radars for targeting. The missiles can be semi-active, meaning they rely on other radar for guidance, or active, meaning they are self-guiding systems that carry their own Radio Frequency (RF) transmitters. In either case, fire control radars have very high PRF and tend to function at higher operational frequencies such as X-band.

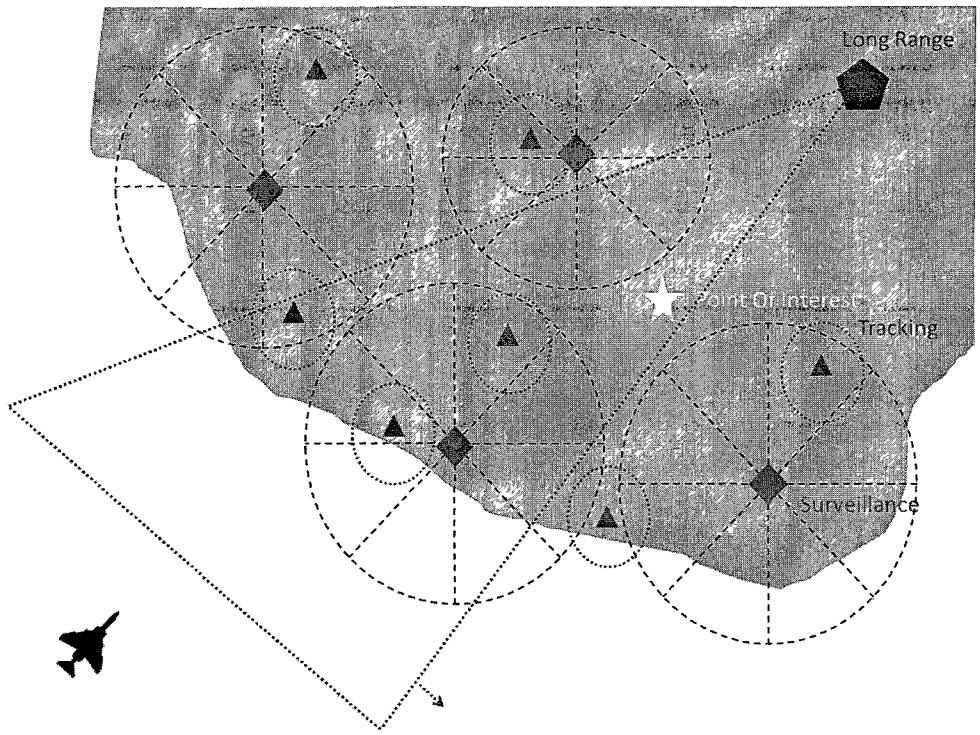


Figure 1.1: Example scenario involving single self-screening aircraft moving towards a point of interest

Based on this scenario, three common types of radars were considered: long range early warning radar, mid-range surveillance/acquisition radar, and short range fire control radars. Table 1.1 gives typical specifications for these types of radars.

Type	Frequency (GHz)	PRI (μs)	PW (μs)	Peak Power (kW)	Beamwidth Azimuth (deg)	Beamwidth Elevation (deg)	Scan Rate (s)
Early Warning	3-5	100-3000	10-100	100-300	1-3	5-15	5-15
Surveillance	5-8	25-500	5-50	1-10	1-2	8-20	1-5
Tracking	9-18,32-40	5-30	0.5-2	1-3	0.5-3	0.5-3	N/A

Table 1.1: Typical radar operating parameters

1.6 Research Method and Thesis Organization

Research for this thesis was separated into three phases. The first phase was a general literature survey in order to identify the modern developments in EA and EP measures, as well as information on the conventional hardware structure of DRFM jammers. While this provided some background knowledge and general information on modern jammers and jamming techniques, it was found that security classification and proprietary information limited the depth of open source literature. Some classified sources, which provided specific operational parameters for radar and details on novel jamming methods, were also reviewed. Information in this thesis will be limited to open source material.

The second phase involved simulations to create the types of radar signals described in Table 1.1, with the ability to make adjustments to any desired parameter. In addition, false target profiles were created to provide the required Doppler modulations as well as the false target delays required for range gate pull-off techniques. The target profiles were then applied to the input radar signal to produce the desired simulated jamming waveforms. Matlab software (version 7.6.0.324, R2008a) was used throughout.

The last phase involved practical implementation of the software jammer system using the D-TA Systems suite of sensor processing equipment. The Matlab code from phase two was used as the basis for the C++ coding. Software was written for a Linux-based server and a new Jamming Module was created to function with the existing D-TA software. The digital output of the jammer was imported into Matlab to validate that the

desired jamming waveform was in fact created. Hardware and software challenges due to real time implementation were documented.

Chapter 1 of this thesis provided the motivation for the research as well as the project objectives and contribution. Chapter 2 provides a summary of background information, including the general characteristics of radars, various EA methods, and different types of active jamming. The critical ES process that takes place prior to jamming is described. The chapter ends with a summary of the important equations for both radar and jammers. Chapter 3 gives results from Matlab simulations and shows examples of various desired target profiles. The actual implementation using the D-TA Systems suite of sensor processing equipment is covered in Chapter 4. It also provides benchmark measurements of maximum data rates supported by the jammer. Chapter 5 shows examples of the output from the jammer. Finally, Chapter 6 summarizes the work and provides areas for further research.

Chapter 2

Theory and Prior Research

2.1 Evolution of Radar and ECM

Air supremacy during conflict can give a considerable advantage over the enemy. During World War II, both sides of the conflict attempted to use their assets to their benefit while denying the same to the opponent. For this reason, not only was there a constant evolution in equipment and tactics, but also in the systems used for detection, tracking, and targeting. In the context of air operations, this meant the development of the first radars and subsequently, the electronic counter measure. Since that time, evolution in radar technology continues to be closely followed by development of updated radar counter measures.

From the post war years, four main stages of radar advancement can be considered [5][10]. The first evolution was the development of frequency agility in non-coherent radars and the use of pulse-to-pulse cancellers as electronic protection measures. Second was the development of the coherent radar, making it possible to filter out both natural and artificial clutter. The third major advancement was the use of broadband signals and pulse-coherent narrowband signals. Broadband signals are the foundation of a class of signals known as Low Probability of Intercept, while narrowband radar signals provided resistance against broadband noise. The fourth and most recent change in radars was the use of phased array antennas, marking the evolution from mechanical steering to analog and then digital steering methods.

ECM tactics continually evolved to keep pace with radar technology. From strictly passive methods such as simple chaff, basic jammers that were capable of producing noise were developed. Later, the frequency of the noise could be adjusted to be narrow or broadband in nature. Another advancement in jammers was the use of transponders and repeaters, which could transmit specific return pulses back towards a radar. These previously analog techniques were the predecessors to modern digital jammers. Cooperative jamming and use of towed or expendable decoys to produce false targets can cause further confusion for the victim radar.

There are several ways to classify EA. One manner is to separate it based on active and passive devices. Active devices use their own emitters to radiate energy back towards the radar, while passive devices do not require a dedicated emitter since they rely on the radar's original transmitted signal. An alternate method is to separate EA based on their underlying operating principle. In this case, EA can be either disruptive or deceptive in nature. Another term that is commonly used is self-protection and support EA. Self-protection means the EA is being done from the same platform that is being tracked by the radar, while support jammers are spatially displaced from the platform they are protecting. Support jammers can further be grouped as escort, stand-off, and stand-in. Stand-off jammers operate from a safe range outside the hostile zone and must transmit higher power to achieve the intended effects on a radar. Escort jammers operate from closer ranges, and thus tend to be more effective, but must maneuver with the protected platform(s). The most effective support jamming is done by stand-in jammers. They operate deep within hostile territory and are typically on smaller air platforms.

Unmanned Aerial Vehicles are well suited for this role. However, their increased effectiveness comes at a cost of a significantly higher vulnerability to enemy attack. When support EA is used, jamming can be done in a cooperative and coordinated sense to conceal the magnitude and size of a raid [4].

With modern systems, the distinction between active and passive ECM is sometimes unclear [22]. For this reason, perhaps the most logical way to classify ECM is through on-board or off-board applications. Off-board ECM includes examples such as chaff, flares, and towed or launched decoys. Chaff is used to produce an artificial cloud of clutter in which the target can be obscured. Essentially, the platform dispenses appropriately sized stripes of plastic coated with metallic material. The effects of chaff are time limited and more effective against conventional pulsed radars. Similarly, flares are used to seduce IR trackers. Towed decoys are reflectors that follow the aircraft at a predetermined distance to appear as a separate target. They can also be launched forward, in which case are expended. The latest towed decoys have built in transmitters from which a jamming signal can be emitted.

Alternately, on-board ECM can produce both disruptive and deceptive jamming techniques through the use of Frequency Memory Loops (FML), and DRFM jammers. FMLs can be considered the analog predecessor of DRFM jammers. Within an FML, a captured analog signal is circulated around a delay line. The signal can be amplified and frequency modulated to produce artificial Doppler before being re-transmitted. However, the circulation time (*ie.* memory) is limited by degradation in the signal due to thermal

noise. Although superior to transponders, FMLs are limited in technique scope and must capture a new signal each time an artificial pulse is produced. As will be discussed in section 2.3, DRFM jammers do not have these limitations.

Training and tactics also play a significant role in the success of ECM. Any method used in isolation will not perform as well as if used in conjunction with other methods. For example, the displacement of chaff will result in a short-lived clutter cloud. However, if chaff is applied by a pilot while effectively maneuvering the aircraft, it will have greater effect. Therefore, by knowing how and when to apply ECM most effectively, the pilot and platform maximize their chances of success.

A simple way to understand the battle between radars and jammers is to understand their underlying limitations. Radar has the advantage when it comes to signal processing. It has full knowledge of the transmitted waveform, and thus can optimize the receiver to detect weak signals and disregard mismatched waveforms. Also, to improve on detection performance, radars can integrate a number of pulses to increase the Signal to Noise Ratio (SNR). However, radar must transmit sufficient energy such that at least a sufficient amount of detectable energy is returned back from the target. The power returned to the radar receiver from a target decreases by a factor of $1/R^2$ for each direction of travel, and thus a factor of $1/R^4$ for the return trip. On the other hand, the jammer receives a much stronger signal from the transmitting radar due to the one-way travel, and thus has the advantage for receiving a much higher SNR to perform ESM. Similarly, the jammer can transmit at relatively lower powers and still remain above the

detection threshold at the victim radar. However, the radar receiver will not process any mismatched waveform transmitted by the jammer, potentially rendering the jamming useless. Consequently, even though the jammer can send more power to the radar then the target echo signal, the success of the jammer will be based on how well it can penetrate the radar receiver. This is the crux of the radar versus jammer battle.

2.2 Modern Radars

Virtually all modern radar systems are coherent. Although there are several definitions of coherence, it generally refers to a system where the phase relationship from pulse to pulse is known or preserved. Most often, it is achieved by using a master oscillator keyed by a power amplifier type transmitter. Less often, due to the added complexity, coherence can also be achieved by locking the phase of the transmitted pulse to an oscillator [1]. The significance of a coherent system is that it allows for the pre-detection integration of pulses, which significantly increases the SNR, and ultimately improves the overall detection capabilities. The frequency spectrum of a coherent pulse train versus a non-coherent pulse train is compared in Figure 2.8.

A second trend for modern systems is the use of intra-pulse modulation schemes. Most commonly, a long (uncompressed) pulse is modulated prior to transmission by either frequency modulation or phase coding. The relatively long pulse means the radar can transmit more energy and thereby increase its range. To compensate for the poor range resolution of a long pulse, the return signal is processed through a pulse

compression filter, which provides a processing gain and increase the resolution. See section 2.7.3 for more information.

Modern radars also tend to use both frequency and Pulse Repetition Interval (PRI) agility. Frequency agility refers to the fact that a radar will change frequencies within its operational bandwidth. By doing so, it limits the effects of jamming since the jammer will need to constantly look for these frequency changes and adjust the jamming frequency. PRI agility refers to the use of different PRIs between pulses. Not only does this resolve range ambiguities in targets, but it also causes additional complications for jammers. Specifically, if the PRI is constant, then false targets are achievable both up and down-range. However, if the radar employs PRI agility, then producing false targets up-range is not possible without the use of PRI prediction algorithms. Therefore, knowing the PRI pattern is also an important consideration for jamming. Some modern radar systems may use as many as four PRIs [1]. Note that within a single Coherent Processing Interval (CPI), the frequency and PRI must remain constant.

The operating frequency is dependent on the use of the radar. For example, long range radars typically use HF to UHF bands. However, these bands require large antennas/apertures, which limits where they can be used. Many ground and ship based radars operate in the microwave range (L and S bands). For airborne radars, higher frequencies (typically X band) are most often used due to benefit from the small antenna/apertures needed. Higher frequencies (K band and higher) can be used, but start

suffering from atmospheric attenuation. Therefore, this frequency range is limited to short range applications. Microwave frequency bands are shown in Table 2.1 [1].

Band	Frequency Range (GHz)
L	1-2
S	2-4
C	4-8
X	8-12
Ku	12-18
K	18-27
Ka	27-40

Table 2.1: IEEE standard frequency bands in microwave and millimeter ranges

The use of coherent radars and pulse compression techniques has resulted in the development of coherent jamming sources. Not only is the jamming waveform matched with that of the transmitting radar, but since all of the transmitted jamming pulses are in phase, they are able to take advantage of the processing gain on the order of 30 to 60 dB [4], which significantly attenuates non-coherent jamming sources.

2.3 Modern DRFM Jammers

DRFM jammers digitize and store intercepted radar signal. The captured signal can be re-transmitted as many times as desired. Aside from being a duplicate of the radar waveform, and thus matched to the radar receiver, the digital signal stored in a jammer can be modified to enhance the realistic nature of the jamming waveforms. This is done by controlling the frequency, amplitude and time delay for successive jamming pulses. Compared to their analog FML predecessor, they have the advantage of a much longer storage time and, depending on the DRFM architecture, more flexibility to modify the stored waveform by using techniques such as sub-pulse sampling for the generation of

composite waveforms. This comes at the cost of added complexity and memory requirements. It should be noted that DRFM jammers are equally effective against conventional non-coherent radars.

The basic block diagram of a DRFM structure is shown in Figure 2.1 [18]. This architecture shows the RF being down converted by an analog mixer. After filtering to remove the upper side bands of mixing, the signal is then sampled at the Intermediate Frequency (IF) and stored in memory. A controller is required for read and write control of the memory. Although not explicitly shown, some form of modulation (*ie*. amplitude, frequency, time) is applied to the data, either before or after the digital to analog conversion. After the modulations are applied, the digital data is up converted to RF for re-transmission.

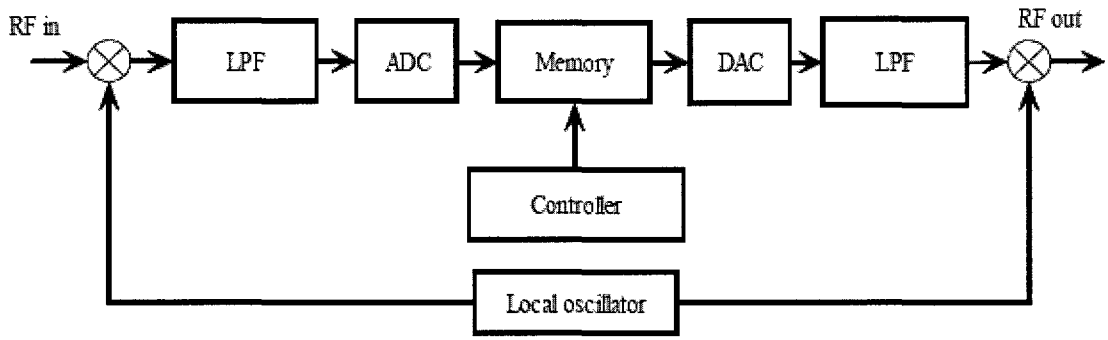


Figure 2.1: Architecture of DRFM jammer

A component that impacts the performance of a DRFM system is the Analog to Digital Converter (ADC). Specifically, the ADC sampling rate and number of quantization bits are of importance. The ADC sampling rate will determine the bandwidth of the DRFM system (where the bandwidth is half the sampling rate). Faster

performance Analog to Digital Converters (ADCs) tend to have few quantization bits, which implies lower amplitude resolution capabilities and higher quantization noise. For example, some recent ADC which sample in the GHz use only 4 bits for quantization. Another disadvantage of a small number of quantization bits is unwanted suppression of small signals (again due to the coarse amplitude quantization). Therefore, the sampling rate and number of bits given by the selected ADC will lead to design tradeoffs.

Serrodying is the process used in deceptive jammers to generate false Doppler in jamming pulses. For most DRFM systems, it is accomplished by using a variable LO in the up conversion from baseband to IF. The offset between the down and up converting LOs generates the artificial Doppler shift [4].

The development and progression of FPGA technology has been a key driver in the advancement of DRFM jammers. Two main considerations are the memory access speeds and size of memory available. Modern FPGAs have high performance configurable Input/Output ports, which allow for fast and direct interface with ADC and DACs. Once the data has been digitized, it can be stored directly on the FPGA RAM. High speed multiplexing and demultiplexing may be required to keep up with the sampled data rates. For example, if data from the ADC is coming in faster than can be written to memory, it will need to be slowed down by buffering or polyphase filters (see section 2.10). The memory depth will impact the delay and Doppler resolution while the memory access time controls the throughput delays in the system. The current trend is to have both the controlling and modulation functions written in the FPGA memory.

DRFMs can be classified as either having narrowband or wideband architecture. In a wideband structure, a single DRFM covers a frequency band of interest. Its main advantage is that it can better handle large bandwidth (such as pulse compression radar signals), as well as frequency agile radars provided their operational frequency is within the DRFM frequency band coverage. This comes at the cost of added complexity and its performance is currently limited by hardware, specifically the digital to analog conversion. Single channel wideband DRFMs can operate over a 1 GHz instantaneous bandwidth [4]. Narrowband structures operate by dividing the instantaneous bandwidth into narrowband channels, with each channel covering on the order of 400 MHz. The main advantage of this architecture is that it can be implemented using readily available hardware. However, if the instantaneous bandwidth of a radar is greater than the bandwidth of the individual narrowband channels, the performance will significantly degrade.

Finally, depending on application, the form and fit overall system are also important. For tactical application, space and weight must be minimized, compared to laboratory DRFM systems where these requirements can be relaxed.

2.4 ESM

ESM is a critical part of the ECM process. Without an accurate ESM system, ECM would not be possible. Two general classes of ESM are the RWR and reconnaissance receivers [6]. The former is used to warn the aircraft that it is being strobed while the latter is used to map enemy radar and communication installations. The

output from an RWR is time critical and will often lead to an immediate action by the pilot or the platform counter-measures system, whereas the data from a reconnaissance receiver will be analyzed for intelligence in non-real time. The capabilities and specifications of ESM system used by jammers are usually classified, but they operate in much the same way as a RWR. The general processing steps are summarized below.

The ESM process in a RWR is illustrated in Figure 2.2 [9]. Captured signals from the antennas will be passed to the jammer ESM processor. The receiver will perform the three main functions of parameter estimation, pulse de-interleaving, and emitter identification. The parameter estimation involves measuring both the inter-pulse and intra-pulse parameters. The typical measurements include carrier (RF) frequency, pulse width (PW), pulse repetition interval, pulse amplitude, and time of arrival. The measured parameters are used to form a set of vectors known as Pulse Descriptor Words. Next, the receiver will attempt to separate the possible emitters by comparing and matching the PDWs [2][4][9].

Certain parameters are easier to measure than others, and so they are used in the first sorting pass. For example, the direction of arrival can be measured accurately within 15 degrees, enabling its use to separate different emitters. Separating based on frequency is also common. The remaining emitters will be separated based on their other parameters such as PW, PRI, and intra-pulse modulation. This exercise, known as pulse deinterleaving, is largely statistics based. Many sorting algorithms are well documented, and can be referenced in [23].

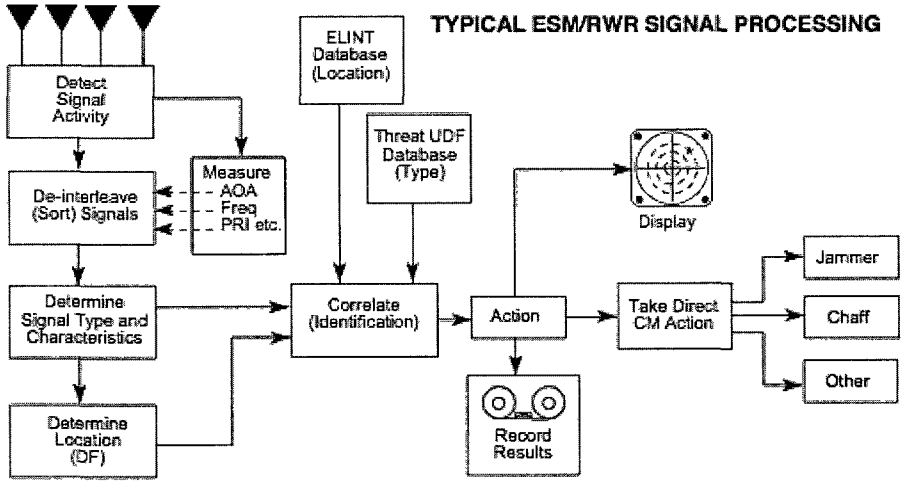


Figure 2.2: Signal sorting process in a RWR

Once the emitter parameters are known, they are matched to a library of known emitters. Generally, there will be some knowledge of the types of radar expected to be encountered based on the area of operation. Thus, the ESM system can often pinpoint the name of the transmitting radar system, be it land, air, or sea based. Even if the system is unable to classify the emitter, the measured parameters can give insight into the type and intent of the emitter.

The final step is passing the information obtained to perform some type of action. Typical actions include displaying the direction of arrival and identified emitting radar to the pilot for information. If deemed critical, immediate and automatic evasive action such as chaff or other deceptive/disruptive jamming could be taken. Alternately, no action will be taken if the emitter is found to be low threat or identified as a friendly transmitter.

2.5 Jamming Techniques

Different types of radars are susceptible to different jamming techniques. Based on the identified radar and the posed threat level, the most appropriate type of jamming will be selected [10]. Even if the specific emitter cannot be exactly identified, some generic jamming technique may be applied. In general, the objective of jamming is to either disrupt or deceive its targeted radar. Disruption jamming interferes with the radar, and includes techniques such as the production of noise, release of chaff, or the deliberate overloading of radar with false targets. On the other hand, deception techniques attempt to mislead the radar. Their main objective is to break lock with the radar, forcing it back into a search mode. In either case, the effectiveness of a given jamming technique depends on the type of radar being attacked. Since each radar has particular vulnerabilities, it is critical to select an appropriate jamming technique that attacks the radar's weaknesses. Otherwise, jamming may be detrimental in serving to alert the adversary.

2.5.1 Disruptive Techniques

Disruptive techniques aim to overwhelm the radar receiver and processor. One of the most common forms is known as noise jamming. Noise jamming decreases the signal SNR by transmitting noise concurrent to the true skin return, which has the same effect as increasing the transmission path length or decreasing the target RCS [13]. When noise jamming is present, it is normally much stronger than the ambient noise power alone, so a Jamming to Signal Ratio (JSR) is used in place of SNR. Of course, regardless of how much power is transmitted, the only effective jamming will be that which penetrates the

radar antenna, receiver, and signal processing. For example, the radar antenna will primarily receive radiation from its main lobe, and much less so from its other lobes. The matched filter in a radar receiver is meant to remove frequencies other than those that are expected from the echo. The signal processing can be used to ignore inputs until the desired times. These measures mean that in order for noise jamming to be effective, the power should be maximized, and the frequency and timing should be carefully considered. Otherwise, a significant portion of the noise power will be wasted.

When the produced noise is wideband, the jamming is called barrage noise. Since the noise covers a bandwidth greater than the victim radar, barrage noise is preferred for wide bandwidth or frequency agile radars, or for covering multiple radars. However, as an unwanted consequence, much of the noise power is outside of the band of interest meaning that power is wasted on generating signals that are never processed.

On the other hand, narrowband noise, also referred to as spot jamming, can be used if the radar frequency is known. By not jamming the entire bandwidth, the jamming power is more efficient and not wasted on unwanted frequencies. The tradeoff is that the jammer must constantly verify that it is within the instantaneous bandwidth of the radar. The term 'look through' describes the periods of time when the jamming ceases in order to verify the noise is still within the instantaneous bandwidth. The look through period for a noise jammer is a tradeoff between jammer accuracy and vulnerability. Methods to determine and optimize look through times is discussed in [13]. As an alternate option to continually re-tuning the frequency of noise required for spot jamming is to sweep the

spot noise across the operational bandwidth. This is known as swept spot noise. In this case, the sweep rate can be optimized based on the known radar characteristics. Figure 2.3 illustrates the difference between barrage and spot noise.

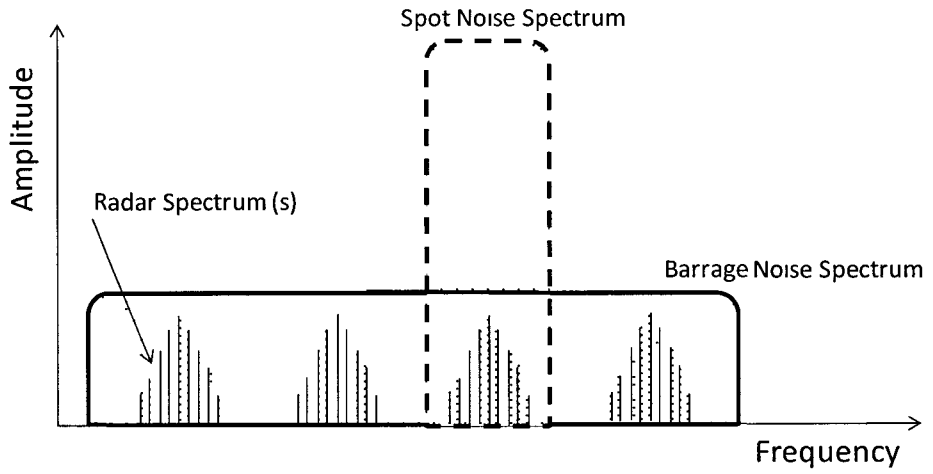


Figure 2.3: Noise bandwidth comparison for spot versus barrage noise jamming

Noise jamming can be effectively injected into the main beam or any of the sidelobes. If sidelobes are targeted, the jammer must use more power or be used from a closer distance to compensate for the reduced gain in sidelobes. Both barrage and spot jamming can be produced in a cooperative fashion by standoff or escort jammers, or individually by self-screening platforms. Using artificial noise generated at the desired frequencies and pulsed at the appropriate times, the true echo signal reflected back to the radar can be concealed.

Other forms of disruptive masking are Range Bin Masking (RBM) and Velocity Bin Masking (VBM). In RBM, rather than using noise to mask the echo signal, copies of

the radar pulse are transmitted by the jammer before and after the received radar pulse. This will produce an effect on the radar such that targets appear in a number of adjacent range bins, thereby masking the location of the true echo signal. Similarly, VBM is meant to saturate adjacent Doppler bins in order to hide the true echo signal.

2.6 Deceptive Techniques

Deceptive techniques attempt to break radar lock. To accomplish this, the radar is first allowed to lock onto the target. The jammer then increases the JSR in the returned echo signal. This step, known as capturing the range or Doppler gate, is essential since it raises the detection threshold to a level high enough to render the true skin return weak compared to the jamming signal. The time required to capture the range gate depends on the radar, but in general, the power of the jammer should be 6 to 10 dB greater than the signal power alone. A gradual increase in amplitude can be employed to avoid any detection mechanism in the receiver. Once the gate has been captured, the jammer senses subsequent the radar pulse, but transmits the jamming pulses with controlled time delays and/or frequency modulations [12] [14].

When a Range Gate Pull Off (RGPO) is employed, the jamming pulses are delayed in time but not shifted frequency. As illustrated in Figure 2.4, RPGO gradually and successively pulls the radar away from the true target by adjusting the timing of the jamming pulse. The jamming ceases once there is sufficient physical separation between the skin echo and the false target, forcing the radar to reacquire the target. The separation distance is a trade-off between technique time and separation distance. RGPOs are most

effective against low PRF and non-coherent radars. An important point to note is that the PRI of a radar must be predictable in order to produce up-range targets. Otherwise, only down-range targets are possible. The PRI information would normally be passed from the ESM receiver. Reference [11] discusses the impact of stable, staggered and jittered PRI on DRFM systems.

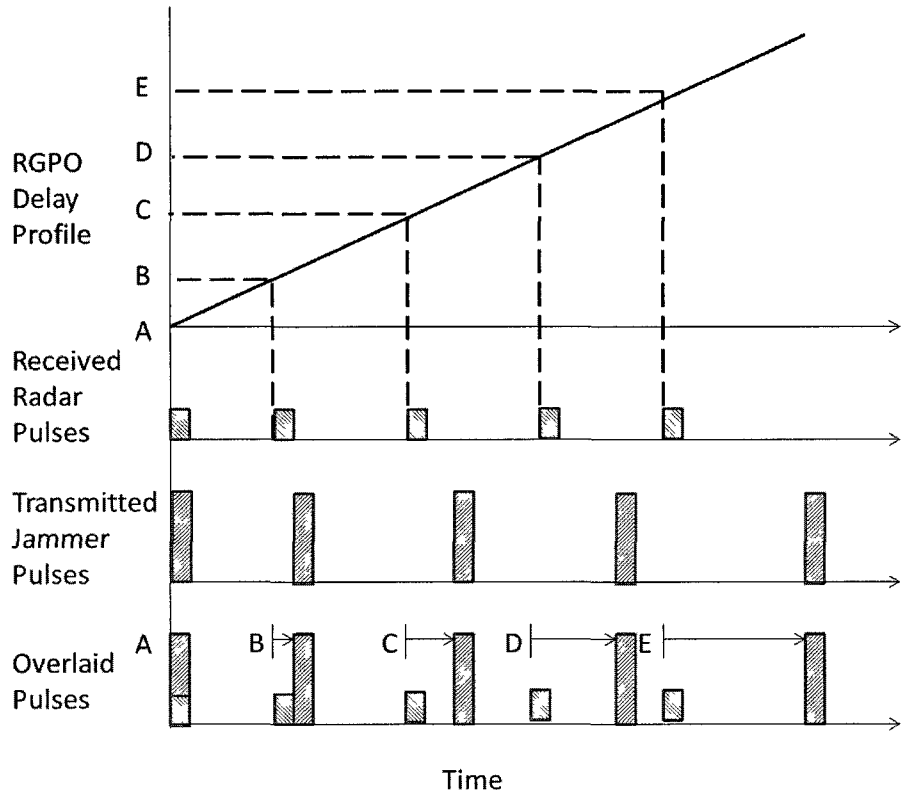


Figure 2.4: RGPO profile showing pull-off of jamming pulse from true echo

Conversely, when Velocity Gate Pull Off (VGPO) is used, jamming pulses are modified in frequency, but not in time. After the tracking gate is captured, frequency modulation is applied to the captured radar pulses to produce an artificial Doppler shift in the transmitted jamming pulse. It will therefore appear to the victim radar that the target

is accelerating or decelerating. The sign of the Doppler shift will change depending on if the platform is moving away or towards the radar. Specifically, targets closing on a radar will produce a positive Doppler shift resulting in a greater return signal frequency. The magnitude of the Doppler shift is directly related to velocity and carrier frequency. VGPOs are used against high PRF radar and PDR.

The rate at which pull-off is achieved by a RGPO and/or a VGPO is controlled by a false target profile, which can be made to look as if the target has a constant velocity or is accelerating. A "para-linear" pull-off starts with a parabolic profile which transitions to a linear profile at a specified point. This gives an appearance of a gentle acceleration until the desired velocity is reached. The production of realistic target profiles is critical to the effectiveness of deceptive jamming.

To further enhance effectiveness, RGPO can be coordinated with Doppler processing to produce a false target with a matching Doppler shifted echo. This is known as a Coordinated Range-Velocity (CRV) Pull-Off. As an example, if a down-range CRV was attempted, successive jamming pulses would be delayed in time relative to the received radar pulse, and modulated with a negative Doppler shift commensurate to the pull off in range. CRV can either slave the range timing of the pulses to match the Doppler information, or vice versa. Despite the added complexity of coordinating range and Doppler, a CRV is generally preferred to RGPO and VGPO since it produces more realistic waveforms. Examples RGPO, VGPO and CRV profiles are shown in section 3.4.

2.6.1 Angle Deception

It should be noted that the jamming techniques described above result in masking or movement in the radial direction relative the victim radar. While this type of jamming may hide the true echo or cause the radar to break lock, reacquisition could happen quickly since the true target will remain illuminated on the same line of sight. To increase the reacquisition time, it is necessary to include angle deception techniques in jammers. Angular deception can be achieved through the use of towed or expendable decoys, or cooperative jamming techniques. For self-screening platforms, other well-known techniques such as 'terrain bounce', 'inverse gain jamming', 'cross-eye' and 'cross-pol' deception explained and illustrated in [2] [15] and [16]. However, these techniques are beyond the scope of this work.

2.6.2 Advanced Techniques

By storing a digital copy of the radar waveform, DRFM jammers are capable of performing novel and advanced jamming techniques. As already mentioned, false targets can be produced individually in any range or Doppler bin. Targets can then be moved in a coordinated or uncoordinated manner. Copies of a recorded radar pulse can be modified in amplitude or frequency and sent out individually or as pulse trains. Another capability DRFM jammers provide is the ability to transmit segments of recorded pulses or send out time reversed pulse. This is especially useful for jamming radars that use pulse compression. Since these jamming waveforms are partially matched to the radar pulse, they will pass through the filters producing disruptive effects. Time reversed pulse will cause a stretched out noise pattern at the output of the compression filter.

All of the techniques can be combined in a multi-channel DRFM system to produce novel and dramatic jamming waveforms. For example, a four channel system is shown in Figure 2.5 [20]. A chirped pulse has been shown for ease of illustration. In each channel, the range, Doppler and amplitude can be controlled independently. The copied radar pulse is modified as desired, and saved as a primary target (each channel will have a different primary target). For example, channels 1 and 2 have duplicate pulses, channel 3 has reversed pulses and channel 4 has partial pulses with reduced amplitude. Then, secondary targets are produced on each channel by repeating the primary target at the desired interval. The output of the jammer will be the sum of all the independent channels, provided the power does not become saturated.

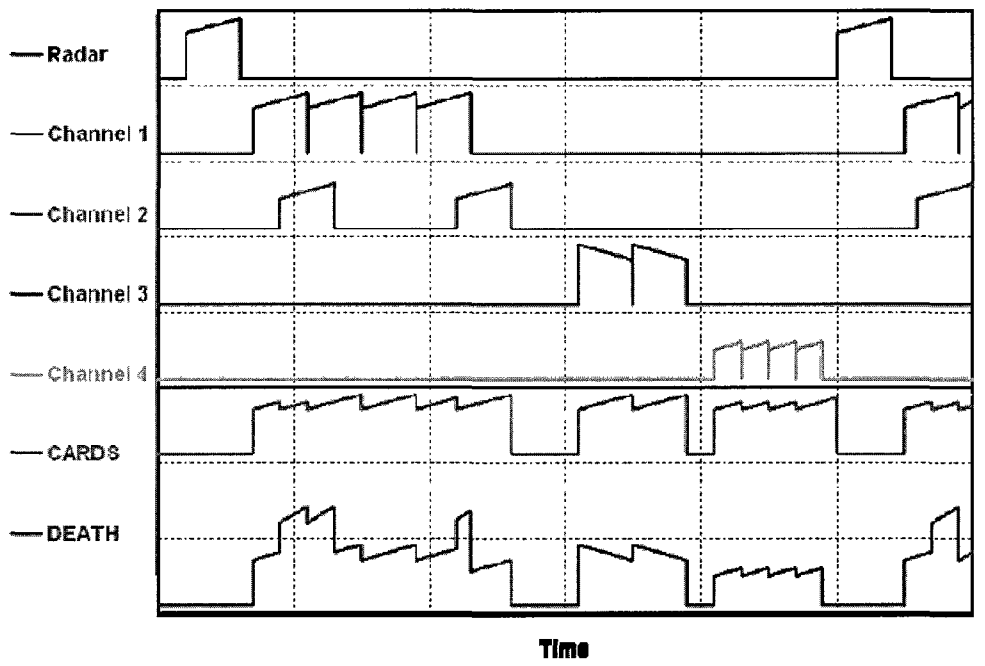


Figure 2.5: Generation of jamming pulse created by the superposition of false targets produced on four independent channels

By overlaying primary and secondary targets, numerous forms of jamming pulses are possible. When received by the victim radar, these waveforms can overcome the radar processing gain and effectively exhaust the radar processor.

2.7 Classification of Radar

Radar waveforms can be separated into classes based on their characteristics [6]. One class of radar waveform is Continuous Wave (CW). These radars continuously transmit, and consequently must use separate and well isolated transmit and receive antennas. Far more common than CW radars are pulsed systems, including conventional pulsed systems that measure target range, systems that use Doppler processing, and systems that employ pulse compression. The basic operation of these types of pulsed radars is explained in the subsequent sections.

2.7.1 Conventional Pulsed Radar

Figure 2.6 shows a simple example of three pulses from an amplitude modulated pulsed waveform [11]. The frequency of the sinusoid is the carrier frequency. The pulse width is the duration of the pulse in time and the PRI denotes the time between the leading edges of the pulses. The PRF is given by the reciprocal PRI.

The range measurement of a target by a conventional pulsed radar is done using a method known as pulse delay ranging. Pulse delay ranging requires measuring the time, Δt, between the transmitted and received pulse. Assuming the target is within the unambiguous range, the range, R, is found by equation (2.1). The factor of two in the denominator accounts for two-way propagation, and c is the speed of light. In order to

determine target velocity, a range differentiation calculation (*ie.* measuring the rate of change in range between at least two received pulses) must be done.

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

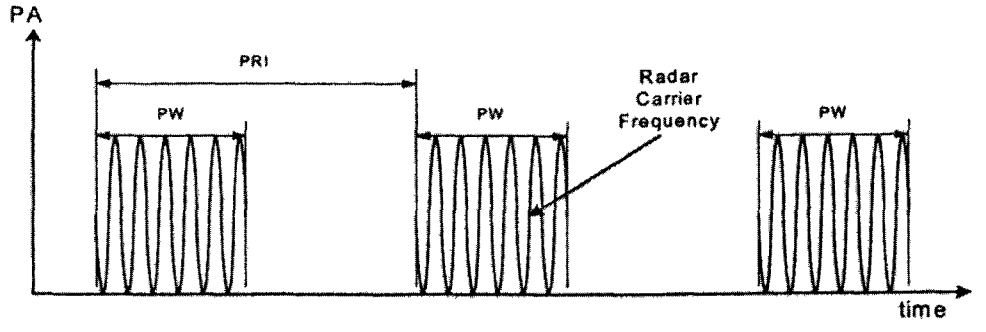


Figure 2.6: Conventional pulsed radar waveform

Based on its function and environment, a radar system will be designed to operate with a specific maximum range in mind. This distance is known as the unambiguous range, R_{un}. It is determined by the PRF, or alternately the corresponding PRI, T, as shown in equation (2.2). Beyond this range, targets that are detected will be multiple-time around echoes, meaning that they will be associated with the incorrect transmitted radar pulse and will give erroneous range measurements, as shown in Figure 2.7.

$$R_{un} = \frac{cT}{2} \tag{2.2}$$

The range resolution, R_{res}, of the radar is the minimum distance required to resolve two separate targets. It is determined by the pulse width, τ, through the following relationship.

$$R_{res} = \frac{c\tau}{2} \tag{2.3}$$

Knowing the unambiguous range and the range resolution, the path a radar signal travels can be broken down into range gates (also known as range bin). Each range gate corresponds to the distance of one range cell, given by equation (2.3). The concept of range gate is important because data can be independently processed for each range bin.

By equating equations (2.1) and (2.3), the time difference between echos from targets in adjacent range bins can be found to be τ seconds. In other words, this is also the time delay required by a jammer to place a false target in an adjacent range bin to the true target. If a target is desired at one range bin down-range, the jammer would transmit τ seconds after the detection of the radar pulse. To place a target one range bin up-range, a jamming pulse would have to be transmitted τ seconds before the arrival of an actual radar pulse. The duty cycle, d_t, of a radar is defined as the ratio of pulse width to PRI.

$$d_t = \frac{\tau}{T} \tag{2.4}$$

The energy, E, transmitted during a single PRI can be found as a product of the peak power, P_{peak}, of the transmitter and the pulse width. Alternately, the average power can be found by the energy divided by the PRI.

$$E_p = P_{peak}\tau = P_{av}T = P_{peak}d_tT \tag{2.5}$$

The radar receiver is responsible for processing the return signals from transmitted pulses. Almost all conventional pulsed radars use a superheterodyne receiver with a matched filter in the IF stage. It can be shown that the matched filter maximizes

the peak SNR, and thus maximizes the probability of detection [1]. Once the signal has been passed through the matched filter, the phase relationship between pulses is destroyed. The output is compared against pre-defined detection to determine if a target was present. Note that pulses can be integrated in both the matched filter (coherent or pre-detection integration) or at the output of the matched filter (non-coherent or post-detection integration).

Short pulses have finer range resolution and are therefore better able to reject clutter. These properties make them ideal for target classification. On the other hand, there are some limitations of using short pulses. The large signal bandwidth results in several disadvantages such as increased receiver complexity and signal processing demands, a decreased receiver dynamic range, and a greater vulnerability to interference from other EM sources. Perhaps most importantly, in order to maintain adequate energy in transmission, the peak power of the transmitter will have to be increased to compensate for the short pulse width. Unfortunately, large peak power at high frequencies is difficult to produce due to oscillator limitations and potential breakdown in transmission lines at microwave radar frequencies.

2.7.2 Doppler Processing Radar

Radars that use Doppler processing take advantage of the Doppler shift produced by moving targets. Essentially, they are able to distinguish targets based on velocity. In this way, the effects of natural or man-made clutter (such as rain clouds or chaff) can be minimized, and moving targets hidden in clutter become visible. Although the

transmitted waveform has similar characteristics as the conventional pulsed system (see Figure 2.6), target velocity measurements are made directly through a phase detector in the receiver chain. However, the requirement for a stable coherent oscillator is essential.

Doppler processing radars can be sub-classified based on their pulse repetition frequency (PRF) as high, medium, or low PRF. High PRF radar, such as a Pulsed Doppler Radar, is useful for measuring velocity, but will have many range ambiguities. Conversely, low PRF radar such as a Moving Target Indicator (MTI), is better suited for ranging, but will not be able to unambiguously measure target velocity. Medium PRF radars settle for an acceptable balance between range and velocity measurements. Figure 2.7 shows how low PRF radar has Doppler ambiguities and high PRF radar has range ambiguities [4].

The term coherence in pulsed radars means that the phase reference is maintained from pulse to pulse. By achieving coherence, there are two important advantages. First, pre-detection integration of pulses over a CPI is possible. This reduces the effects of noise and raises the signal so that there is a less chance of missed detections. Secondly, there are important differences in the spectral characteristics of a coherent versus non-coherent pulse train. As shown in Figure 2.8, the spectral width of a non-coherent pulse train will extend to $f_0 \pm 1/\tau$, whereas for a coherent pulse train, individual spectral components can be seen at multiples of the PRF within the envelope [3]. This makes it possible to distinguish a Doppler shift provided that the pulse train is long enough to

make the lines reasonably narrow and the PRF is high enough to spread the spectral components [2].

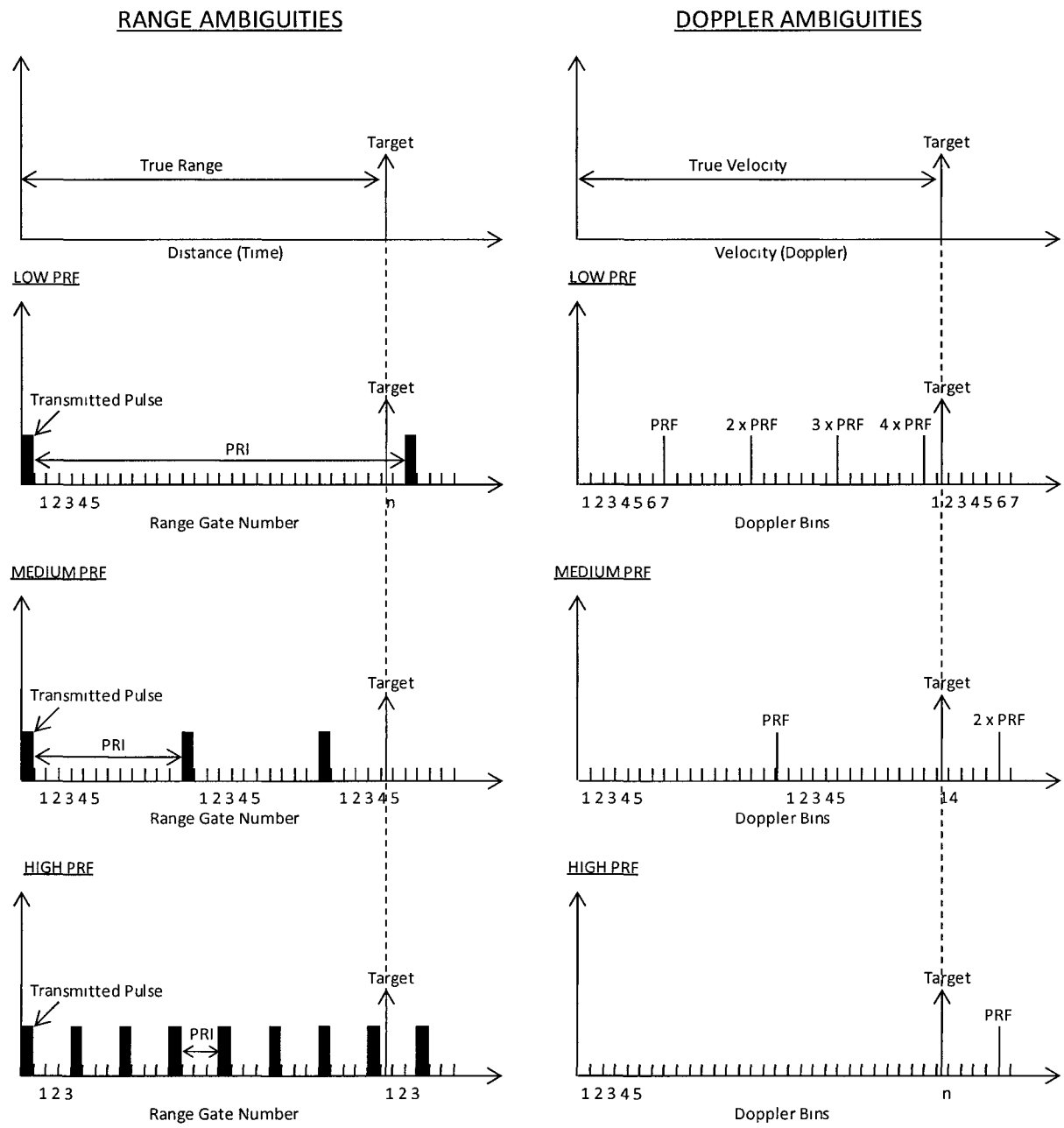


Figure 2.7: Creation of range and Doppler ambiguities due to PRF selection

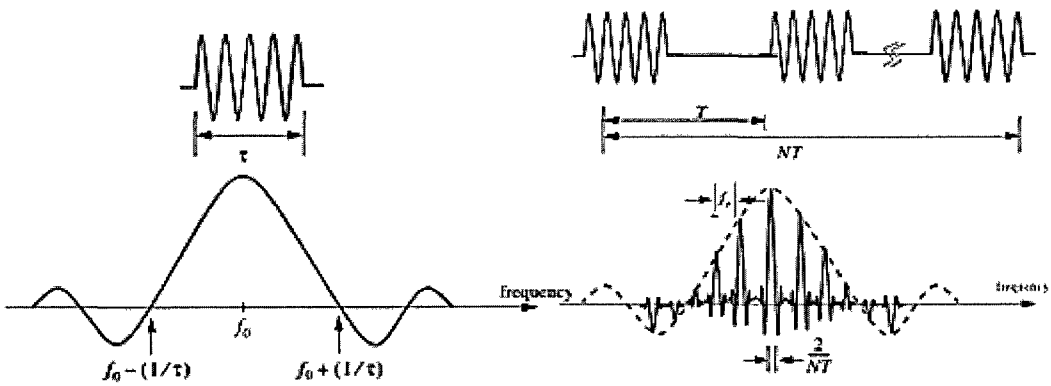


Figure 2.8: Spectrum of non-coherent versus coherent pulse train of N pulses

The Doppler shift produced by a target is directly proportional to its radial velocity. By measuring the Doppler shift and knowing the carrier frequency, the velocity of a target can be calculated. The relationship can be derived by first considering the total phase change, ϕ, in the two-way propagation path from the radar to the target. The signal wavelength is represented by λ.

$$\phi = \frac{2R}{\lambda} \cdot 2\pi = \frac{4\pi R}{\lambda} \tag{2.6}$$

Differentiating the phase change shows that it is directly proportional to the radial velocity, v_r.

$$\frac{d\phi}{dt} = \frac{d}{dt}\frac{4\pi R}{\lambda} = \frac{4\pi}{\lambda}\frac{dR}{dt} = \frac{4\pi}{\lambda}v_r \tag{2.7}$$

Thus, from the two equations above, the received phase will be related to the range, while the phase change will be related to the radial velocity of the target. Note that a stationary target will produce zero phase change. Since the rate of phase change with time is also the angular frequency, the relationship between Doppler and radial velocity is given by

equation (2.9). Here, ω_d is the angular frequency, f_d is the Doppler frequency and f_c is the carrier frequency.

$$\frac{d\phi}{dt} = \omega_d = 2\pi f_d = \frac{4\pi}{\lambda} v_r \tag{2.8}$$

$$f_d = \frac{2v_r}{\lambda} = \frac{2v_r f_c}{c} \tag{2.9}$$

Upon receiving the echo signal, the phase relationship between the transmitted and received pulses is extracted by the receiver. A phase detector, also known as a synchronous detector, is used in place of the matched filter. The Doppler shift produced by a target can be visually represented in the complex plane. Figure 2.9 shows a phasor representing the transmitted pulse. Recall that for coherent radar, its phase, ϕ_{Ref}, is constant or known from pulse to pulse. The received signal phasor is plotted on the same plane and is shown to have a phase of ϕ_{Rec}. For a moving target, the Doppler shift will be represented in the form of a continuous phase shift from pulse to pulse. Therefore, the received signal phasor will rotate with respect to the transmitted phasor. The rate and direction of rotation will be directly related to the radial velocity of the target and the targets direction of movement (either towards or away from the radar). Use of in-phase and quadrature-phase channels in the synchronous detector will give information on the direction of movement.

The output of the phase detector is processed through delay line cancellers or a Doppler filter bank. Older radar systems used analog cancellers, which have now been almost completely replaced by digital Finite Impulse Response or Infinite Impulse

Response filters. The frequency response of a basic delay line canceller will generally have a magnitude proportional to $|sin^n(\pi f_d T_p)|$, wher f_d is the Doppler shift frequency, n is the number of delay lines, and T_p is the PRI. The frequency response of a single and double line canceller are shown with the clutter spectrum in Figure 2.10 [1] [3]. By using a larger number of delay lines, a greater amount of the clutter spectrum is rejected. However, the narrower the frequency response, the higher the chances of actual targets being missed. Various weightings on the filter taps can be used to optimize the frequency response based on particular criteria.

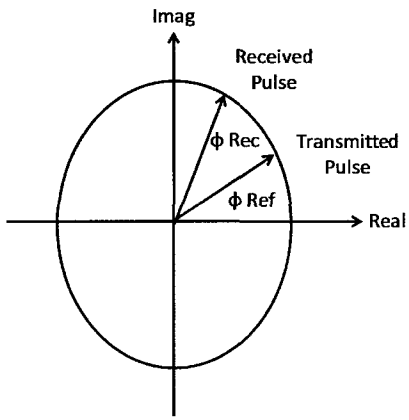


Figure 2.9: Representation of reference and received signals in the complex plane

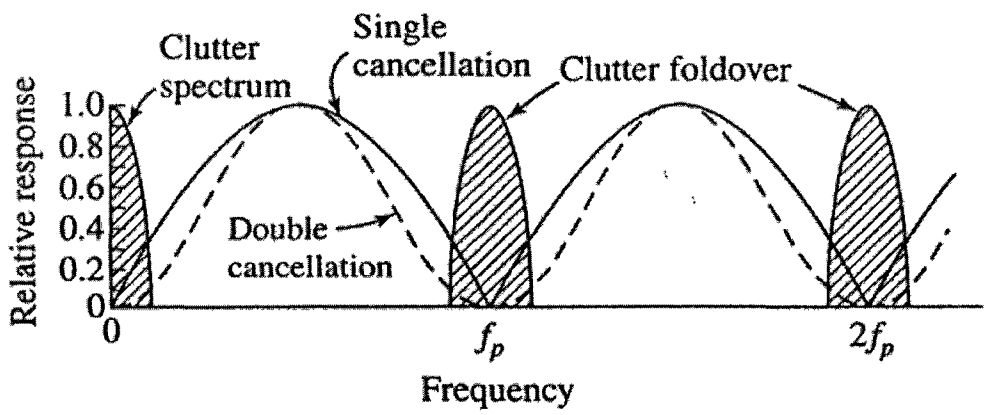


Figure 2.10: Frequency response illustration of single versus double delay line cancellers

One important observation from Figure 2.10 is that the frequency response from line cancellers will have nulls at integer multiples of the PRF, f_p. This corresponds to what is known as blind speeds. For example, if a target is traveling at a blind speed, the output will fall at a null, rendering the movement invisible. Radial velocities that produce blind speeds are given by equation (2.10).

$$v_n = \frac{n\lambda}{2T_p} = \frac{n\lambda f_p}{2} \qquad n = 0,1,2,3,... \tag{2.10}$$

Obviously, blind speeds can cause serious limitations in radar performance. To increase the blind speed, the radar system can be designed to operate at lower frequencies (increasing λ) or higher PRFs. Alternately, if the radar uses a staggered PRF, the blind speed of the overall system can be increased by allowing targets that are unseen at one PRF to be seen by the alternate PRF.

More commonly, a Doppler filter bank is used in place of the delay line cancellers. Essentially, the filter bank separates the frequency response into a set of contiguous filters, where each filter is tuned to a different Doppler frequency (the set of filters will cover the complete Doppler space). The main advantage of using a filter bank is that it allows for the discrimination and tracking of targets based on velocity. The total bandwidth of the filter bank should be the lesser of the range of Doppler frequencies expected to be encountered or the PRF of the radar. The 3 dB bandwidth of each particular filter will be inversely proportional to the integration time, as shown in equation (2.12) [1] [2].

$$t_{\text{int}} = N \cdot T_p \qquad N = 0,1,2,3,... \tag{2.11}$$

$$BW_{3dB} \approx \frac{1}{t_{\text{int}}} \approx \frac{1}{N \cdot T_p} \approx \frac{f_p}{N} \qquad N = 0,1,2,3,... \tag{2.12}$$

The output of the filter bank will resolve all targets in range and Doppler. An illustration of a filter bank is shown in Figure 2.11 [1]. Recall that when VGPO or CRV jamming is used, it seeks to move the echo signal several Doppler bins from the true velocity. Since Doppler processing radar can determine target velocity directly through the filter bank and also by range differentiation, jammers should coordinate false Doppler with false pulse timings to maximize their effectiveness.

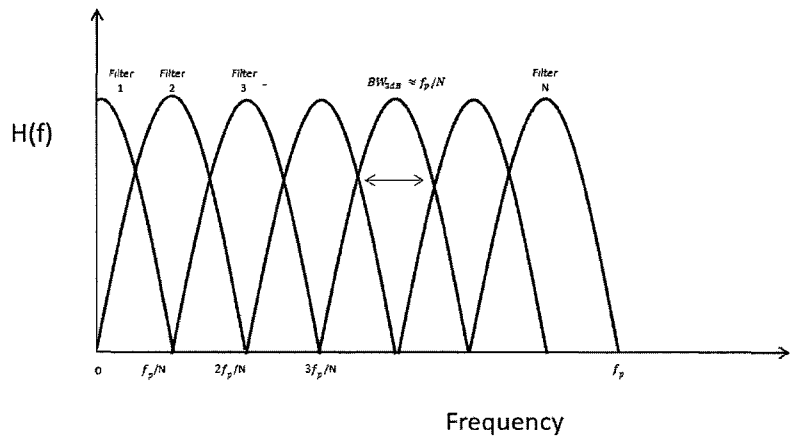


Figure 2.11: Frequency response illustrations of Doppler filter bank

2.7.3 Pulse Compression

It is often desired to have a long detection range while maintaining fine range resolution. To achieve this, a radar would need to transmit high power, short pulsed waveforms. For reasons such as limitations in power generation at high RF frequencies, these radar waveforms are not typical. Instead, a method known as pulse compression is

commonly used. The transmitted pulse will be relatively long (*ie*. have greater signal energy), and modulated in some fashion. Most commonly, linear frequency modulation, also known as chirps, or phase modulation is used. A sketch of an up and down chirped time waveform is shown in Figure 2.12 [3], where τ is the uncompressed pulse width, and ΔF is the chirp frequency range. The spectrum of such a waveform will be symmetric about the highest frequency component, with a bandwidth of $2\Delta F$.

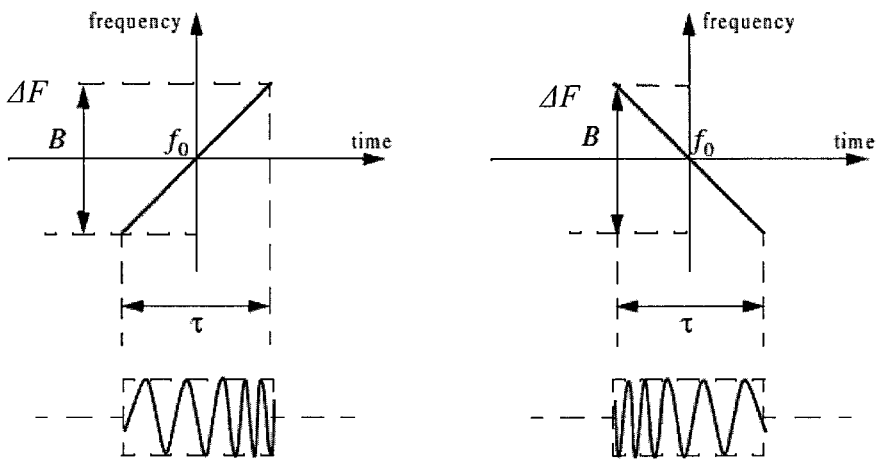


Figure 2.12: Example of linear FM up-chirp and down-chirp

Upon receiving the radar echo signal, the return is passed through a particular pulse compression filter, which essentially removes the initial modulation. Thus, the signal output of the pulse compression filter is shortened to obtain the desired fine range resolution.

The Pulse Compression Ratio, PCR, (also known as the compression gain) is defined as the pulse width of the long pulse before the pulse compression filter divided by the compressed pulse length, τ_{comp}, at the output of the pulse compression filter. For

linear frequency modulation the PCR is also equal to the total frequency range of the chirp, ΔF, to the minimum frequency difference required to resolve separate targets, Δf.

$$PCR = \tau / \tau_{comp} = \Delta F / \Delta f \tag{2.13}$$

It can be shown that the minimum frequency difference for pulses to be resolved is also equal to $1/\tau$ [2]. Thus, an alternate form of the PCR known as the time-bandwidth product is given by equation (2.15).

$$\Delta f = 1/\tau \tag{2.14}$$

$$PCR = \tau \Delta F \tag{2.15}$$

From equation (2.15), it is easily seen that to increase the PCR, either the uncompressed pulse width can be increased or the frequency range of the chirp can be increased. Alternately, by equating equations (2.13) and (2.15), the width of the compressed pulse, and consequently the range resolution, is determined solely by $1/\Delta F$.

For phase coded signals, the pulses are phase modulated. The received pulses are passed through tapped delay lines instead of a pulse compression filter. The delay line is separated into segments with appropriate phase conversions for each segment. The output is summed and will be at its maximum at the point where the received echo completely fills the delay lines (since all taps will be in phase). Well-known phase codes include Barker codes and Frank codes.

The advantages of pulse compression techniques come at the cost of increase complexity in both the transmitter and receiver. In addition, designers of radars that use

pulse compression must be aware that ambiguties in range can be inadvertantly caused by doppler effects. Despite this, it is generally considered that the benefits of pulse compression greatly outweigh the disadvantages and thus pulse compression is commonly found in modern radars.

2.8 Radar Range Equation

The radar range equation considers the effect of the transmitter, receiver, antenna, target and environment on the detectable range of a radar system. Complete derivations can be found in [1] and [2]. In its most basic form, the power received from a target is given in equation (2.16). The first term, $P_t G$, is known as the Effective Radiated Power (ERP), is the transmitted power multiplied by the gain of the transmitting antenna. The factor of $1/4\pi R_t^2$ is the area the transmitted power is spread over, where R_t is the range from the transmitter. The target radar cross section, given by σ, determines how much of the received power will be radiated out from the target, and again the factor of $1/4\pi R^2$applies. R_r represents the distance of the radar receiver from the target. Finally, the amount of power receiver depends on the effective area of the antenna, A_e. A general loss term, L_r, is included to account for internal and external losses, as will be explained in the following paragraphs.

$$P_r = P_t G \frac{1}{4\pi R_t^2} \sigma \frac{1}{4\pi R_r^2} A_e \frac{1}{L_r} \tag{2.16}$$

Assuming that the radar transmitter and receiver are co-located, and substituting effective area in terms of gain,

$$A_e = \frac{G\lambda^2}{4\pi} \tag{2.17}$$

$$P_r = \frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 R^4 L_r} \tag{2.18}$$

To find the maximum range of the radar, the power received is considered in terms of the minimum detectable signal power, S_{min}.

$$R_{\max} = \left[\frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 S_{\min} L_r} \right]^{1/4} \tag{2.19}$$

By considering the noise figure of the receiver F_n, the term S_{min} in (2.19) can be translated to the minimum required SNR at the output of the matched filter. Since the receiver input noise is thermal and if the input power is the minimum detectable signal, the following equations apply.

$$F_n = \frac{SNR_{in}}{SNR_{out}} = \frac{S_{in}}{N_{in}} \frac{N_{out}}{S_{out}} = \frac{S_{in}}{kT_o B} \frac{N_{out}}{S_{out}} \tag{2.20}$$

$$S_{in} = F_n kT_o B \left(\frac{S_{out}}{N_{out}} \right) \tag{2.21}$$

$$S_{\min} = F_n kT_o B (S_{out}/N_{out})_{\min} \tag{2.22}$$

The term k is Boltzmann's constant, T_o is the temperature and B is signal bandwidth. This is a useful substitution since the term $(S_{out}/N_{out})_{min}$ can be directly expressed in terms of the probability of detection and probability of false alarm. Substituting (2.22) into (2.19), the maximum range of radar can be found in terms of the minimum SNR out of the matched filter.

$$R_{\max} = \left[\frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 k T_o B F_n (S_{out}/N_{out})_{\min} L_r} \right]^{1/4} \tag{2.23}$$

Loss is an important variable which must also be considered. Losses come from both the system and environment. For example, system losses account for unwanted signal reflection in the transmission lines and internal signal attenuation, as well as non-idealities from antenna beam shape and polarization. Also included in this category are signal processing losses that result in practical systems such as filtering loss. In terms of the atmosphere, depending on the frequency of operation, altitude, atmospheric conditions and weather, the radar performance may be significantly different then if operated in free space. Reference [1] and [3] provides additional detail on both system and environment losses and lists other sources. Lastly, the statistical nature of the minimum detectable signal and the large swings in the target radar cross section (σ) make detection more meaningful in terms of probability. A general loss variable can be added to the denominator of (2.23) to account for these system and environmental effects.

2.9 Jamming Equations

The signal received by a jammer will be relatively stronger compared to the power in the echo signal received back at the radar. A jammer will pick up a radar signal through its ESM system, whose antennas have a gains of 0 to 1 dB. The power received at the jammer, P_{jr}, from a transmitting radar with power P_t, gain G, and distance R, can be estimated by (2.24). Essentially, this is the radar range equation for a one-way path.

$$P_{jr} = \frac{P_t G}{4\pi R^2} \tag{2.24}$$

Quantitatively, when disruptive noise jamming is present, the effect is the same as decreasing the received signal SNR [3]. In effect, the receiver capability is reduced from SNR alone to signal to noise plus interference. For noise jamming, the SNR is reduced across the full operating bandwidth of the jammer. The jammer ERP, ERP_J, depends on the jammer power, P_J, jammer gain G_J. A general loss term for the jammer, L_J, has also been considered.

$$ERP_J = P_J G_J \frac{1}{L_J} \tag{2.25}$$

By the time the jamming signal reaches its intended target, the power radiated by the jammer will be reduced by a factor of $1/R^2$. Losses from to the atmosphere, as well as antenna losses and RF losses in the receiver front end will also reduce the jamming signal in the same manner they impact the radar signal. Assuming a self-screening jammer attacking the main beam, the jammer power at the input of the victim radar receiver is given by (2.26). Now, the power received at the radar, P_r, is given by equation (2.26), where A_e is the L_r are the radar related terms explained above.

$$P_{rj} = \frac{P_J G_J}{L_J} \frac{1}{(4\pi)R^2} \frac{A_e}{L_r} = \frac{P_J G_J G \lambda^2}{L_J (4\pi)^2 R^2 L_r} \tag{2.26}$$

Since the jammer bandwidth, B_j, will be much greater than the radar bandwidth, B_{if}, some of the jamming power will be not be processed (see Figure 2.3). Then, the jamming power at the output of the radar receiver can be approximated by

$$P_{rj} = \frac{P_J G_J G \lambda^2}{L_J (4\pi)^2 R^2 L_r} \frac{B_{if}}{B_J} \tag{2.27}$$

To understand how the radar range is affected when jamming is present, it is first assumed that the jammer power at the receiver will be much greater than the thermal noise of the receiver.

$$N_{out} << P_{rj} \tag{2.28}$$

$$\frac{S_{out}}{(N_{out} + P_{rj})} \approx \frac{S_{out}}{P_{rj}} \tag{2.29}$$

The signal power to jamming power ratio at the output of the radar receiver, SNJ_{out}, can be found by replacing the numerator and denominator of equation (2.29) by equations (2.18) and (2.27).

$$\frac{S_{out}}{P_{rj}} = SNJ_{out} = \frac{\dfrac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 R^4 L_r}}{\dfrac{P_J G_J G \lambda^2}{L_J (4\pi)^2 R^2 L_r} \dfrac{B_{if}}{B_J}} = \frac{P_t G \sigma}{(4\pi) R^2} \frac{L_J}{P_J G_J} \frac{B_J}{B_{if}} \tag{2.30}$$

Since the jammer requires only one-way transmission compared to the radar that requires two-way transmission to receive the signal, the jammer power will generally be greater than the signal power. However, from equation (2.30) it can be seen that as the jammer approaches the radar, the denominator decreases by a factor of $1/R^2$. Thus, as the distance between the radar and jammer decreases, the signal power will increase quadratically. Eventually, there will be a distance where the signal to jamming ratio is too high for effective jamming. At this range, the received signal power from the true echo signal, will "burn-though" the artificial jamming power. The burn-through range is given by equation (2.31) and represents the range at which jamming is no longer effective.

$$R_{BT} = \sqrt{\frac{P_t G \sigma}{(4\pi)(SNJ_{out})_{\min} L_r} \frac{L_J}{P_J G_J} \frac{B_J}{B_{if}}} \tag{2.31}$$

It is suggested that when the signal power is greater than the jamming power by 8 to 12 dB, the radar will be able to detect the true signal even in the presences of jamming [2].

2.10 Prior Research

Most of the published research work to date has focused on the hardware requirements for DRFM systems. All DRFM systems are comprised of essentially the same hardware components, including mixers, filters, ADCs and DACs, memory, and a jamming modulator. All architectures are meant to convert the RF to a low enough frequency for sampling, a write to memory and application of desired modulations, a DAC and up convert the signal back to RF for re-transmission. A general block diagram of a DRFM system was shown in Figure 2.1. Some variations to the traditional structure are now discussed.

The greater part of DRFM research focuses on wideband structures. One problem with the traditional DRFM structure for wideband applications is finding high speed converting devices (specifically, high speed multi-bit DACs). Even if such high-speed devices were readily available, data could still bottleneck at the interface of the FPGA due to limited read/write speeds and processing times for modulations. The use of a channelized receiver in a DRFM, such as the shown in Figure 2.13 [17], can address these concerns.

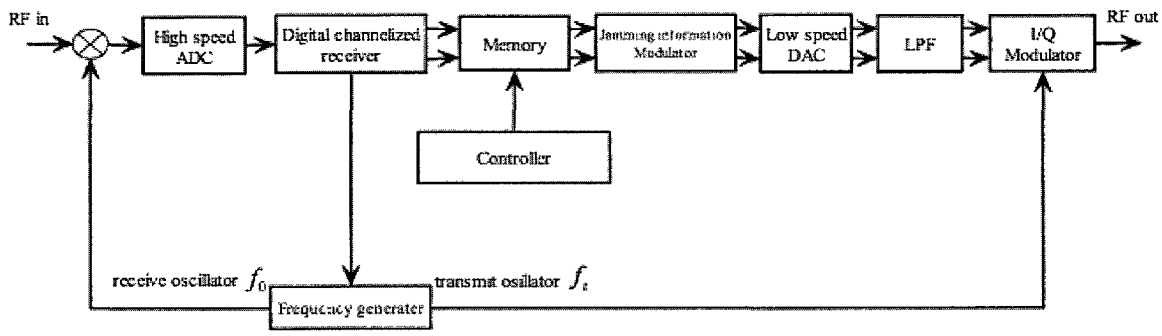


Figure 2.13: DRFM architecture using a channelized receiver

In this structure, the down converting receiver LO has a fixed frequency. A high speed ADC is used, allowing for large bandwidth coverage. However, unlike the traditional DRFM, the data is separated into D sub-channels using the channelized receiver, with each sub-channel covering $1/D$ of the total bandwidth. The channelized receiver can be realized by structures such as the polyphase filter. The polyphase concept is commonly used in multirate Digital Signal Processing (DSP) systems, and can be realized by structures shown in [8] [17] [18]. The relatively slowed data rate in each sub-channel allows for additional processing time. Also, a low speed DAC can be used for the up conversion since it needs to cover only the sub-channel bandwidth.

A key aspect of this structure is that the transmit LO must be variable in order to reconstruct the signal. Also, since an analog quadrature modulator is used to convert the complex IF data to RF, there is an inevitable phase and amplitude imbalance between the real and complex channels, ultimately leading to the presences of image frequencies in the RF output [19]. A different version of the channelized receiver improves upon the phase imbalance from an analog quadrature modulator. This is done by adding a Digital

Up Conversion (DUC) step, which takes the complex quadrature data and converts it to real digital signal. The DAC is then applied to produce the analog IF. Figure 2.14 shows a block diagram of this improved DRFM structure [19].

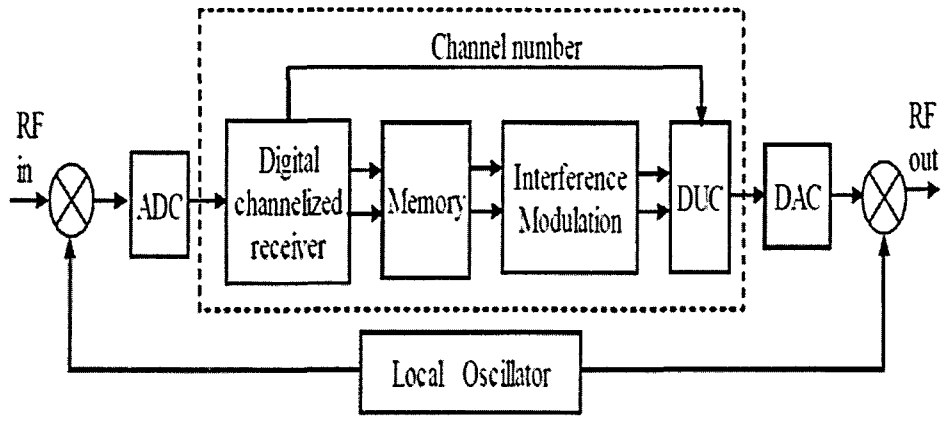


Figure 2.14: An improved channelized receiver used in DRFM hardware

In this structure, the frequency of the transmit LO is fixed, but the frequency of the Numerically Controlled Oscillator (NCO) in the DUC is variable. The detailed architecture for the DUC is found in [19], but a simplified version is shown below. The DUC process receives the complex baseband signal and up samples the data by interpolation. A low pass filter (LPF) then removes images before mixing to the desired IF.

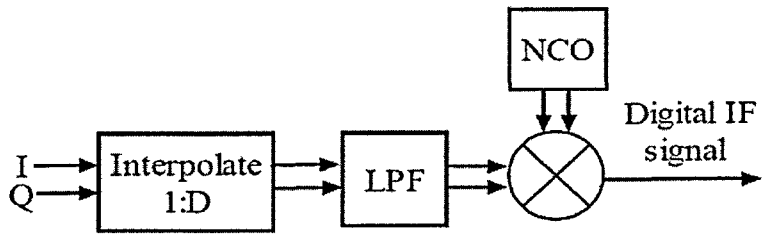


Figure 2.15: Digital Up Conversion process

Two internal DRDC reports were found to be the most applicable documents for this thesis. These reports recognize and elaborate on the importance of the Jammer Controller Unit (JCU) and a Techniques Generator (TG). The JCU performs a signal identification function for the purpose of determining the most effective jamming technique. This information is passed to the TG, which will apply the desired modulations to the recorded radar data to create the desired waveform. This process is illustrated in Figure 2.16 [20] [21].

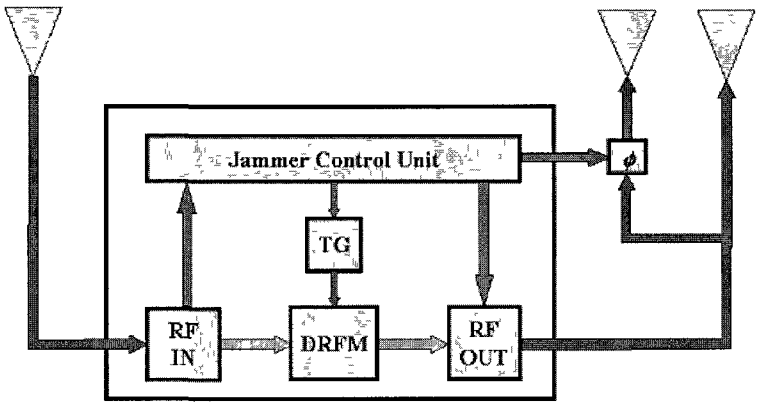


Figure 2.16: Block diagram showing the relationship of the JCU, TG and DRFM

One of the ideas presented is that the TG functions can be programmed in either the DRFM FPGA or externally. The main advantages of externally programming TG are that it frees memory in the DRFM FPGA, and when required, it allows one TG to be used for multiple DRFMs [20]. This comes at a cost of added complexity due to the data transfer requirements and greater potential for speed limitations. However, with the advancement of high speed data transfer methods and multi-core software processing, the benefits could outweigh the potential limitations.

In addition to the hardware aspect, the DRDC documents were the few sources that outlined various jamming modulations and how they could achieved. The positioning of false targets in range could be controlled by reading the contents of the DRFM memory at the right times, and multiple targets could be produced by recirculation of memory. An algorithm for the application of Doppler is also presented [21]. This algorithm applies a continuous phase shift to a pulse train, thereby creating artificial Doppler. Moreover, the algorithm is meant to be applied directly to the in-phase and quadrature-phase data. This baseband Doppler shift algorithm has yet to be validated in real-time implementation, which is part of the motivations behind this thesis.

Chapter 3

Jammer Simulation

3.1 Design and Purpose

Matlab was used for the initial development of the jammer. Since no real radar data was available, the approach taken was to first create examples of waveforms from early warning, surveillance and fire control radars. Essentially, these simulated radar signals would be the input to the jammer. Next, jamming profiles were created in order to provide the desired values for artificial Doppler and false pulse timings. Lastly, some of the created profiles were applied to the simulated radar signals using a baseband algorithm described in section 3.4. The simulation data was analyzed to verify the desired frequency and/or time changes were made to each radar pulse.

The simulation phase of this thesis had three main goals. Firstly, the simulation was meant to determine the theoretical jamming pulse timings and frequency modulations necessary to make the desired jamming waveforms. Secondly, potential areas of concern with the intended hardware and software implementation were identified. Thirdly, the results from simulation were used as an experimental control in that they were compared with the results of the implementation to see how closely the values agreed. Where the results did not agree, simulation data assisted in the debugging process. Consequently, the Matlab simulation was designed to mirror the anticipated physical implementation as closely as possible.

The architecture for the software jammer proposed in this thesis is shown in Figure 3.1. The input IF radar signal is sampled by the ADC and mixed to baseband. The down converted digital data, referred to as the I_r and Q_r, is the input to the jamming software. It is at this point the jamming modulations are applied. The digital output of the jammer software will be referred to as the I_J and Q_J data. IF_r and IF_J denote the respective radar analog input and jammer analog output IF.

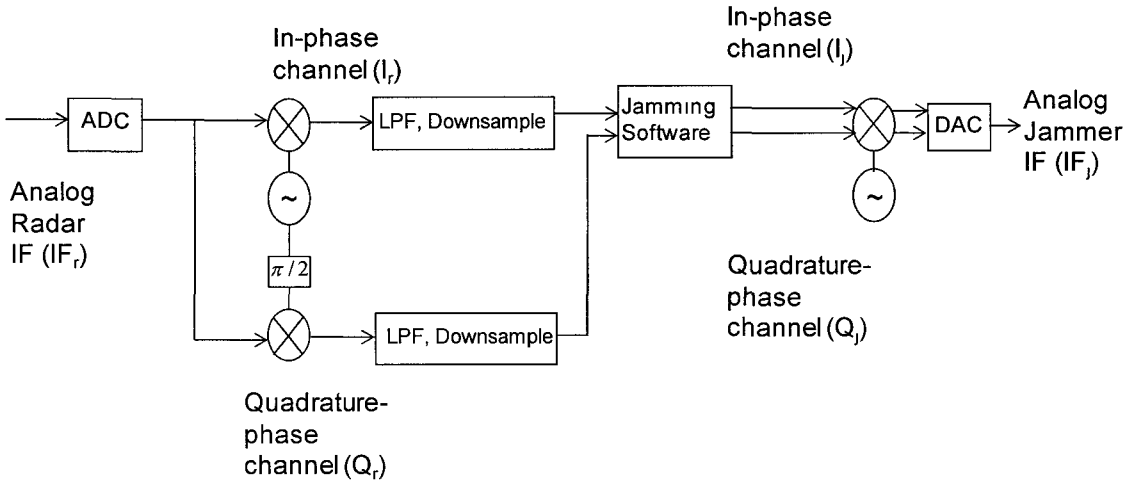


Figure 3.1: Proposed software jammer architecture

3.2 Key Assumptions and Limitations

In order to proceed with simulations, several important assumptions were made for the jammer. First, to work within the limits of the equipment available, the RF processing was not considered. This included capturing of the RF frequency by the antennas, as well as the mixing, amplification, and filtering done between the RF and IF stages of the jammer. Similar to a radar receiver, the RF signal would be accepted by the jammer's antenna and down converted to a frequency where signal processing is

possible. Therefore, it was assumed that the jammer front end would be able to take the signal of interest from the RF to an IF of 25 MHz.

Next, as described in section 2.4, it was assumed that a reliable ESM system was available to separate signals received from different emitters. In addition to pulse de-interleaving, the ESM system would provide accurate classification of the emitter, including the carrier frequency and both the inter-pulse and intra-pulse waveform characteristics. If a radar employs PRI agility, the agility pattern is known. If the PRI pattern is random, which is possible for leading edge radar systems, PRI prediction algorithms would be applied to provide this data to the jamming system.

3.3 Creation of Radar Signals

Even though some radar waveform generation programs already exist, a new script was developed. This allowed for a better understanding of how the parameters affect the pulse spectrum, and also gave the necessary flexibility to uniquely pack the data (as needed later in section 4.2.1). Based on the scenario described in section 1.5, three general types of radar waveforms were created in Matlab. For conventional pulsed signals, a sinusoid centered at 25 MHz was multiplied with a rectangular pulse train with the appropriate PW and PRI. To generate pulse compressed signal, a linear frequency modulation was applied to the pulse. To ensure coherency, the PW and PRI were selected so that an integer number of sinusoid cycles would be maintained both within a PW and PRI. Therefore, the initial phase of each transmitted pulse was the same for each pulse.

Two important specifications of the generated radar signals are the power and SNR. By scaling the amplitude, the peak power of the analog radar signal could be controlled. Using equation (2.24) and the typical radar operating parameters listed in Table 1.1, it was estimated that the peak power of the radar signal received at the jammer would be between -10 to 10 dBm. However, planning ahead to the implementation, it was known that the maximum peak power produced by the hardware was 3 dBm. To allow for a 10 dB jamming to signal power ratio required for capturing the range gate (see section 2.6), it was decided the peak signal power at the input to the jammer IF processor should be near -10 dBm. Producing a -10 dBm signal would require the signal amplitude in Matlab to be set to 2^{13} (refer to section 4.2.1). In terms of SNR, artificial white Gaussian noise could be added to the generated signal to account for imperfections found in a real system, such as jitter in the radar transmitter and thermal noise in the jammer receiver. Practically, by the time the signal arrives at the jammer IF processor, the SNR would be on the order of 10 dB. However, for the purpose of showing clear radar pulses, no noise was added to the radar signals and all plots are shown normalized in this chapter. During the implementation, signals with and without added artificial noise were studied to learn the consequence of signal corruption.

A waveform from a typical long range radar was created with a PRI of 2050 μs (PRF of 487.8 Hz), and PW of 10 μs. The signal bandwidth was 200 kHz. The corresponding unambiguous range was 307.5 km, with each range bin having a length of 1.5 km. Figure 3.2 shows the normalized power and spectrum for pulse train of 5 consecutive pulses.

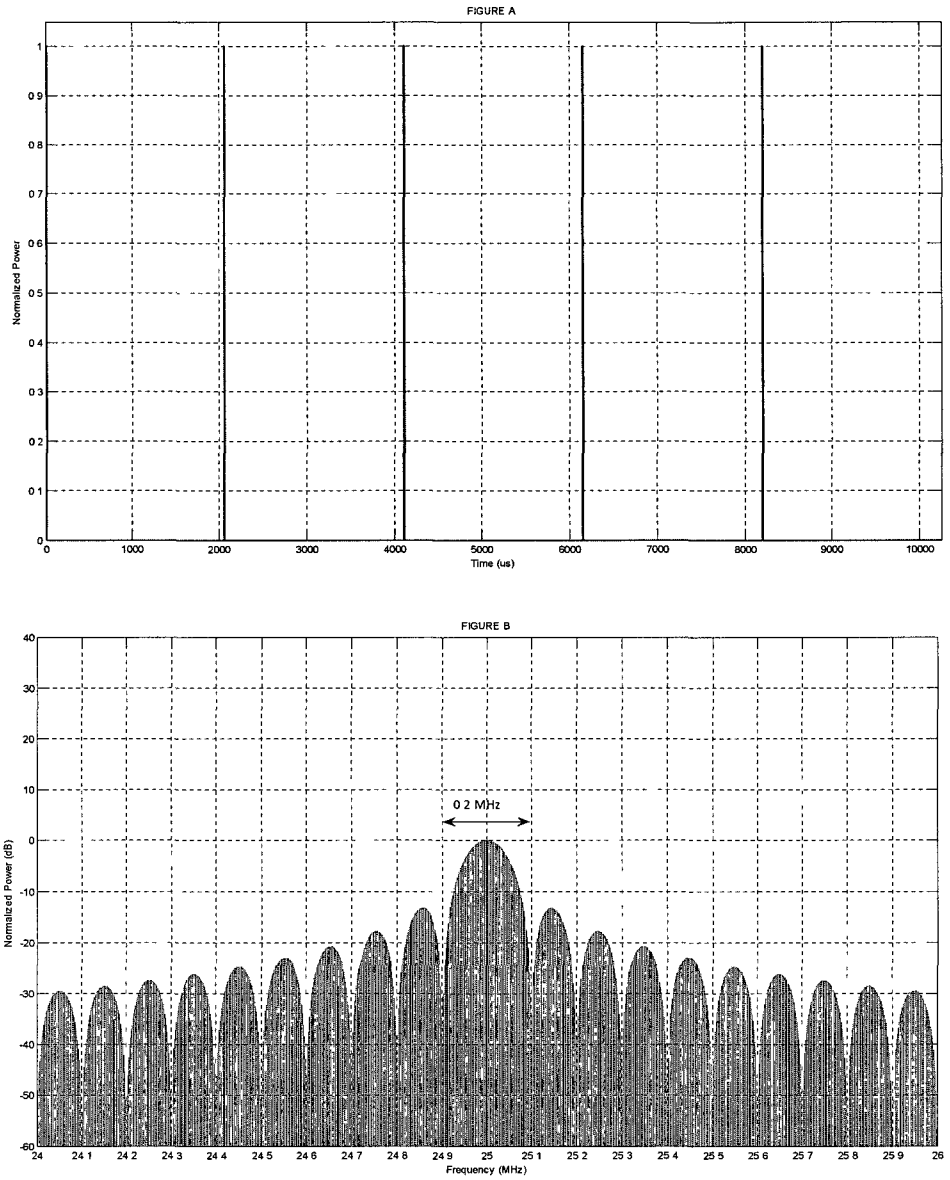


Figure 3.2 a & b: Early warning radar signal power and frequency plot for a pulse train of five pulses

As expected for a low PRF radar, the spectral components that make up the waveform are too close to each other to distinguish the individual spikes. As per the theoretical spectrum shown in Figure 2.8, the signal bandwidth can be measured from the

envelope width of the main lobe. In this case, it is found to be 0.2 MHz, which matches the value expected of a 10 μs pulse.

Surveillance radars perform in the same manner as early warning radars, except the scan time is reduced and the peak power is often limited due to the mobile nature of the radars. Consequently, surveillance radars often use pulse compression techniques to maximize the transmitted energy without losing range resolution. A pulse compression waveform was designed with an uncompressed pulse width of 50 μs. Assuming that a minimum range resolution of 50 m was desired, the corresponding compressed pulse width was 0.33 μs. Consequently, the required PCR was 150 and, using equation (2.15), the frequency range of the chirp, ΔF, was 3.0 MHz. The unambiguous range was arbitrarily selected to be 45 km, meaning that the PRI was set to 300 μs. With these parameters, the time and frequency domain plots shown in Figure 3.3 were produced.

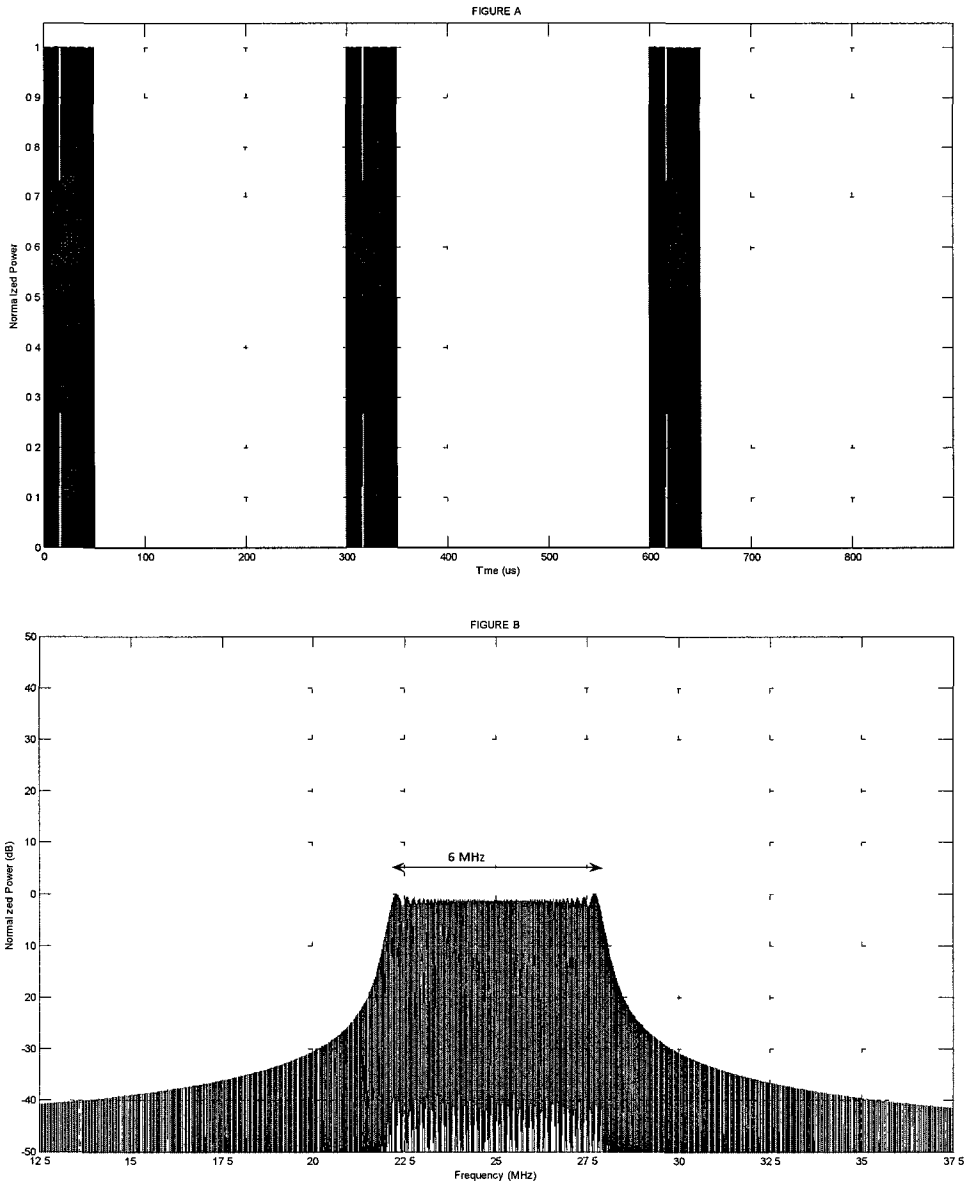


Figure 3.3 a & b: Pulse compressed surveillance radar signal power and frequency plot for a pulse train of 3 pulses

Compared to either early warning or surveillance radars, fire control radars have a much higher PRF and do not scan once they have acquired the target. A high PRF ensures that the radar can unambiguously track targets in Doppler as described in equation (2.10). A small PW will also give the adequate resolution to track targets in

range. In Figure 3.4, 10 pulses from a radar with a 1 μs PW and 30 μs PRI are shown. The range resolution was 75 meters and the unambiguous range was 4.5 km.

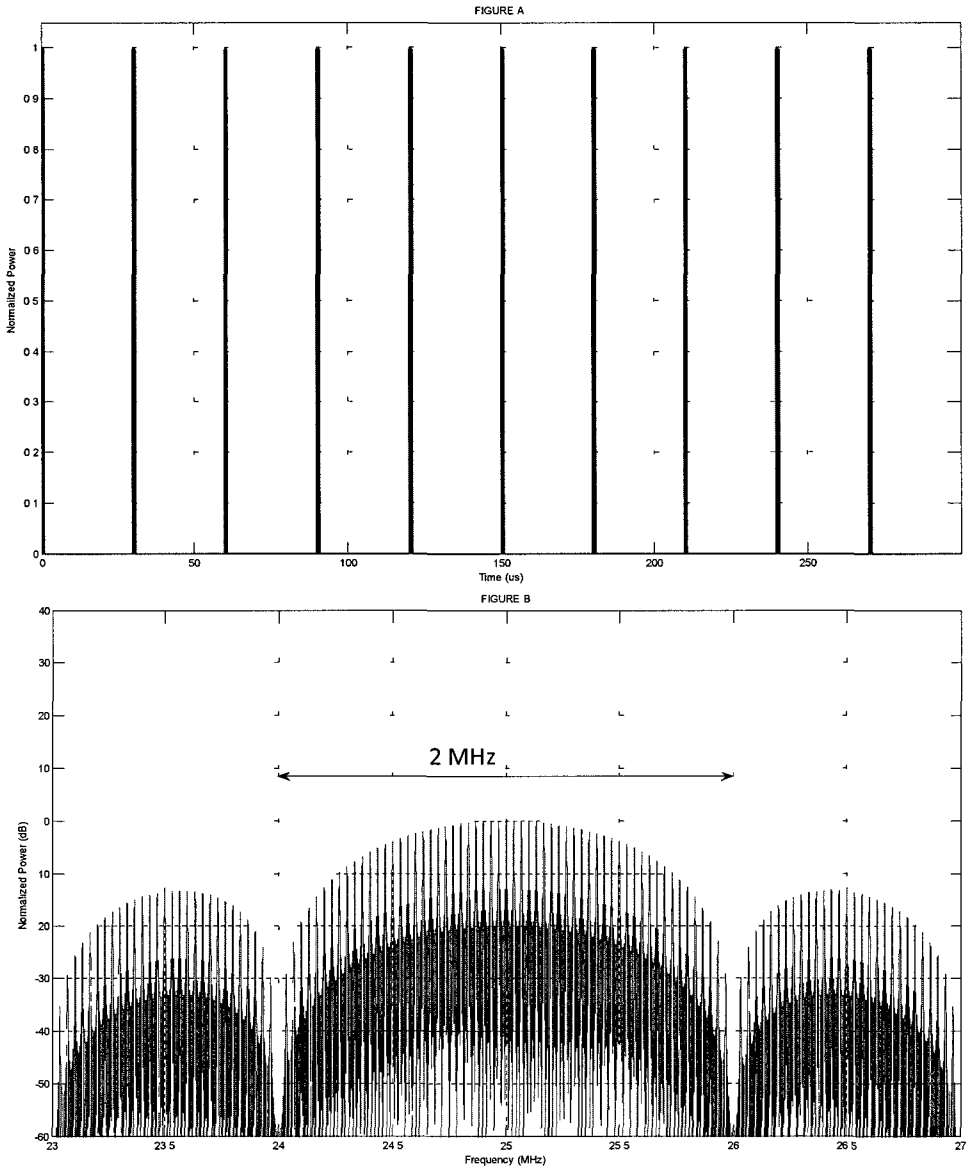


Figure 3.4 a & b: Fire control radar signal power and frequency plot for a pulse train of 10 pulses

In this case, the bandwidth of the main lobe was measured as 2 MHz. The individual spectral widths can also be seen. A close-up plot shows that spikes were

integer multiples of the PRF away from the main lobe, and the spectral widths were equal to 2/(N·PRI), as expected from Figure 2.8.

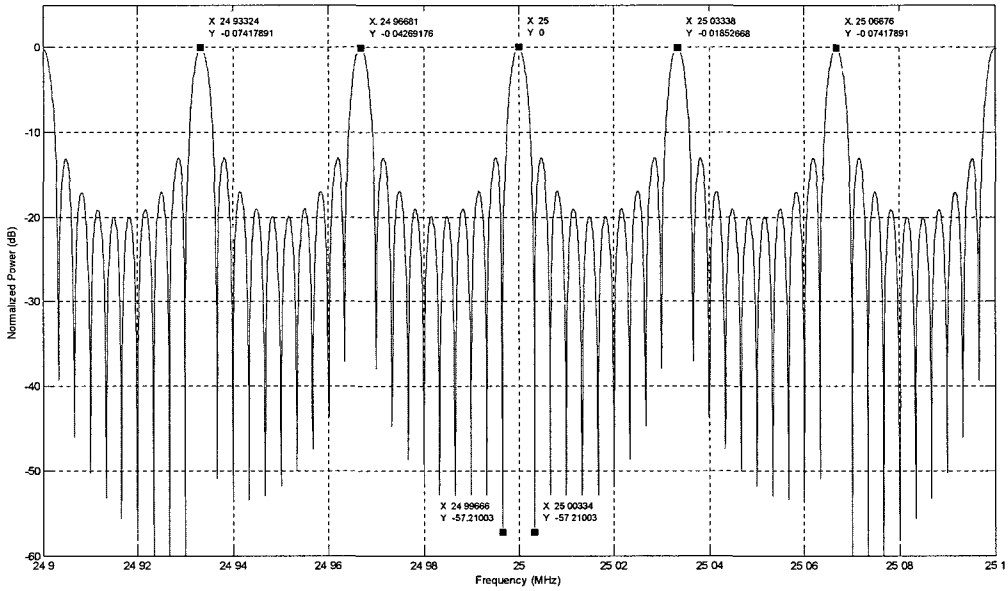


Figure 3.5: Close-up of main lobe from fire control radar signal frequency plot

Since these three radars will be regularly referred to in the remainder of the document, a summary of their characteristics are shown in Table 3.1. The IF frequency was centered at 25 MHz for all cases.

Parameter	Early Warning Radar	Surveillance Radar	Fire Control Radar
PW (μs)	10	0.3 (compressed) 50 (uncompressed)	1
PRI (μs)	2050	300	30
PRF (kHz)	0.5	3.3	33.3
Range Resolution (m)	1500	45	150
Unambiguous Range (km)	307.5	45	4.5
Bandwidth (MHz)	0.2	6	2
Waveform	Pulsed	Linear FM Up-Chirp	Pulsed

Table 3.1: Summary of parameters for created radar signals

3.4 False Target Profiles

Deception jamming techniques previously described in section 2.6 require false targets be placed at a particular range and/or with a specific artificial Doppler with respect to the target. In order to achieve this, the timing and frequency of the jamming pulse need to be well controlled over successive pulses. This is achieved by creating false target profiles. Based on user input, the false target profile will dictate the Doppler shift and timing required for the false targets (relative to the skin return) for the duration of the jamming. The Doppler profile relates directly to the apparent velocity of the target. By applying a positive Doppler shift, the apparent velocity of the jammer increases if the jammer is moving towards the radar (up-range) or decreases if the jammer is moving away from the radar (down-range). The timing profile controls if the false targets appear up or down-range. Down-range targets can be produced by delaying the jammer pulse up to a maximum time of one PRI. Significantly, delaying the jammer pulse greater than the radar PRI will actually result in an ambiguous up-range false target placement for the subsequent radar pulse. Amplitude profiling for the jamming pulses is also possible, but has not been done for this thesis. Noise jamming does not require a profile since size and frequency of the noise mask remains constant over the jamming cycle. However, the user may specify the noise bandwidth and mask size, provided the size of the noise mask does not exceed the PRI. Table 3.2 shows the input variables for the three deceptive techniques discussed, as well as for noise jamming.

Parameter	CRV (Range Master)	CRV (Velocity Master)	RGPO	VPGO	Noise
Carrier Frequency	X	X	X	X	
True Velocity	X	X	X	X	
Technique Time	X	X	X	X	X
Uprange/Downrange	X	X	X	X	
Mask Size					X
Mask BW					X
Final False Target Distance	X		X		
Final False Target Velocity		X		X	
Linear or Parabolic Pull	X		X		

Table 3.2: User controlled input variables for simulated jamming techniques

Although the PW and PRI are not explicit input variables, they should be considered when deciding the jamming profiles for two reasons. First, the PW and PRI are the minimum and maximum range pull limits. Pulling less than a PW has no effect since the target remains in the same range bin. Pulling in distances longer than a PRI will mean the jamming pulse is associated with the incorrect radar pulse. Second, the PW and PRI give an indication of range and Doppler resolution of a radar. Smaller pulse widths have finer range resolution, and therefore do not need to be pulled as far as longer pulse widths. Similarly, shorter PRI indicate a finer Doppler resolution due to the relationship between the PRF and the Doppler filter width (see Figure 2.11). If the number of pull-off bins is known in either range or Doppler, they can be converted to a physical distance or velocity by knowing the radar PW and PRI.

Note that in creating false target profiles, some assumptions were made. First, it was assumed the jammer platform's true velocity remains constant over the duration of the technique time. Also, since CRV techniques can either slave the range timing of the

pulses to match the Doppler information, or vice versa, the input parameters for a CRV technique differ slightly depending on the type of CRV selected. In this implementation, the profiles were designed such that the false target acceleration is constant. Therefore, for CRV (Velocity Master) and VPGO, the pull is always linear in velocity.

False target profiles were created using the equations from section 2.7 and the general kinematic equations listed below. The variable *d*, *v*, *a*, and *t* represent distance, velocity, uniform acceleration, and time. The subscripts '*av*', '*f*', and '*i*' indicate average, final, or initial values. Note that since the range and/or Doppler pull-off always start from the skin return, d_i is zero and is not included in the equations, and v_i is the true velocity of the jamming platform. Example profiles for RGPO, VGPO, and CRV techniques are shown in Figure 3.6 to Figure 3.9. These profiles were applied to various radars in simulation and later during the implementation.

$$d_f = 1/2(v_i + v_f)t \tag{3.1}$$

$$v_f = v_i + at \tag{3.2}$$

$$d_f = v_i t + 1/2\,at^2 \tag{3.3}$$

$$v_f^{\,2} = v_i^{\,2} + 2ad_f \tag{3.4}$$

For Figure 3.6 to Figure 3.9, the first plot is the range profile and the second plot is the Doppler profile. In both the range and Doppler profiles, the x-axis represents the time, and always spans the duration of the technique time. The false target timing can be obtained from the range profile. The timing of the false target relative to the received pulse will be in the order of microseconds, and can be read off the Y1 axis. The

corresponding distance the false target is away from the actual target is found from the Y2 axis of the same plot. Note that negative timing means a delay in transmitting the jamming pulse, and correspondingly, a false target that appears further down-range. Similarly, the Doppler profile gives the artificial Doppler shift to apply during jamming. This is the Y1 axis. The apparent velocity of the target equals the true Doppler shift (related to true velocity) plus the artificial Doppler shift, and is plotted on the Y2 axis.

The first profile is a 10 second, parabolic RGPO. The jamming aircraft was assumed to have a true air speed of 300 km/h (83.3 m/s) towards the radar, and the final false target distance was specified at a distance of 1500 meters down-range of the true position. It was also assumed the victim radar operates in the X-band radar with a carrier frequency of 10 GHz. Figure 3.6 shows the delay and Doppler requirements for this profile.

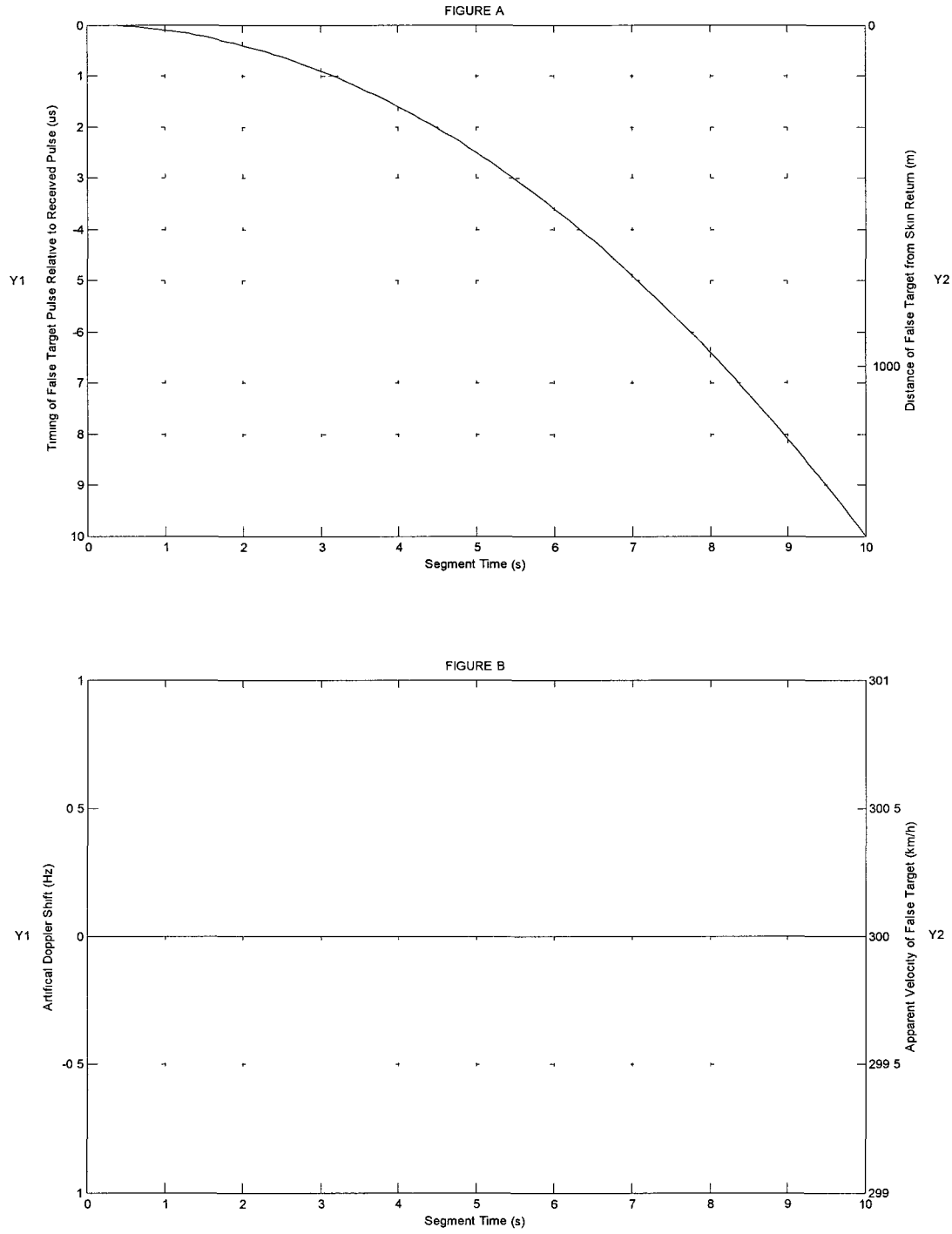
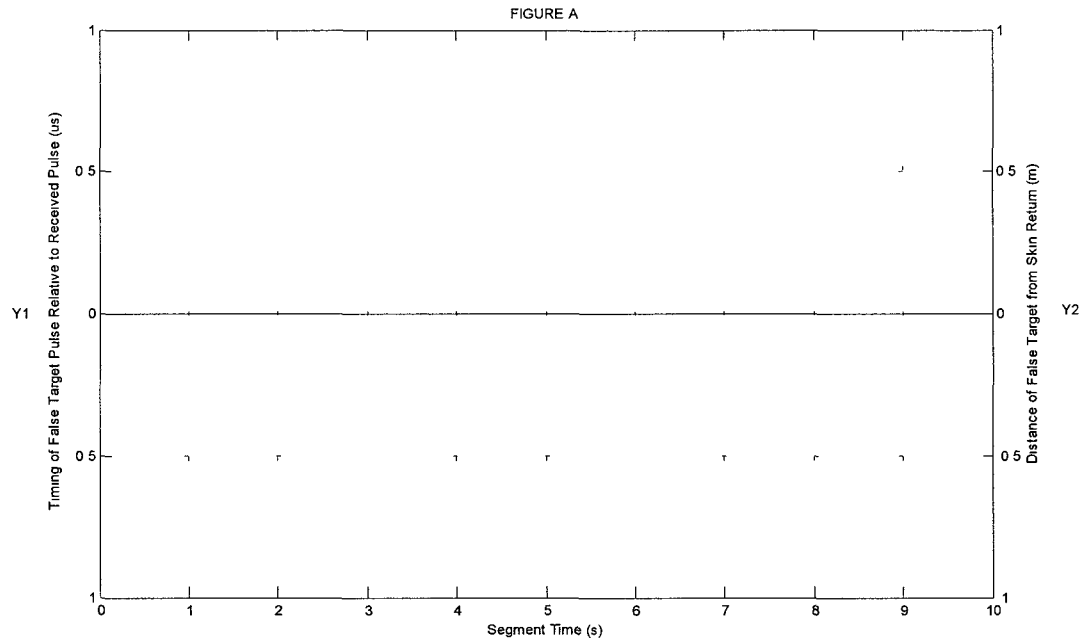


Figure 3.6 a & b: Profile 1 - False target timing and velocity information required for a parabolic RGPO (Carrier Freq = 10 GHz, True Velocity = 300 km/h, Technique Time = 10 s, Final False Target Distance = -1500 m)

From Figure 3.6a, it can be seen that each receive pulse is delayed, with a maximum delay of 10 μs at the end of the jamming profile. This delay places the false target at the desired distance of 1500 meters down-range from the true position. Figure 3.6b shows the artificial Doppler shift to apply is 0 Hz, which is the case for all pure RGPO profiles. Since no artificial Doppler shift is applied, the apparent velocity equals the true velocity, as shown on the Y2 axis. The positive value of the apparent velocity corresponds to movement towards the radar. In all likelihood, RGPO would be used against radar that does not use Doppler processing, so the apparent velocity would be irrelevant.

Next, a linear VGPO profile is shown for the same conditions (*ie*. same carrier frequency, true velocity, technique time, and up-range movement) as the previous example, except instead of specifying a final false target distance, the final target velocity is selected to be 500 km/h. Physically, this can be interpreted as a target that will appear to be accelerating towards the radar. As shown in Figure 3.7a, there is no delay or advancement of the false jammer pulses, which is true of all pure VGPOs. Instead, each received pulse will be given the artificial Doppler shift shown on the Y1 axis of Figure 3.7b. Initially, no artificial Doppler shift is applied. By the end of the technique time, the artificial Doppler shift combined with the true velocity of the jammer platform will meet the specified final target velocity.



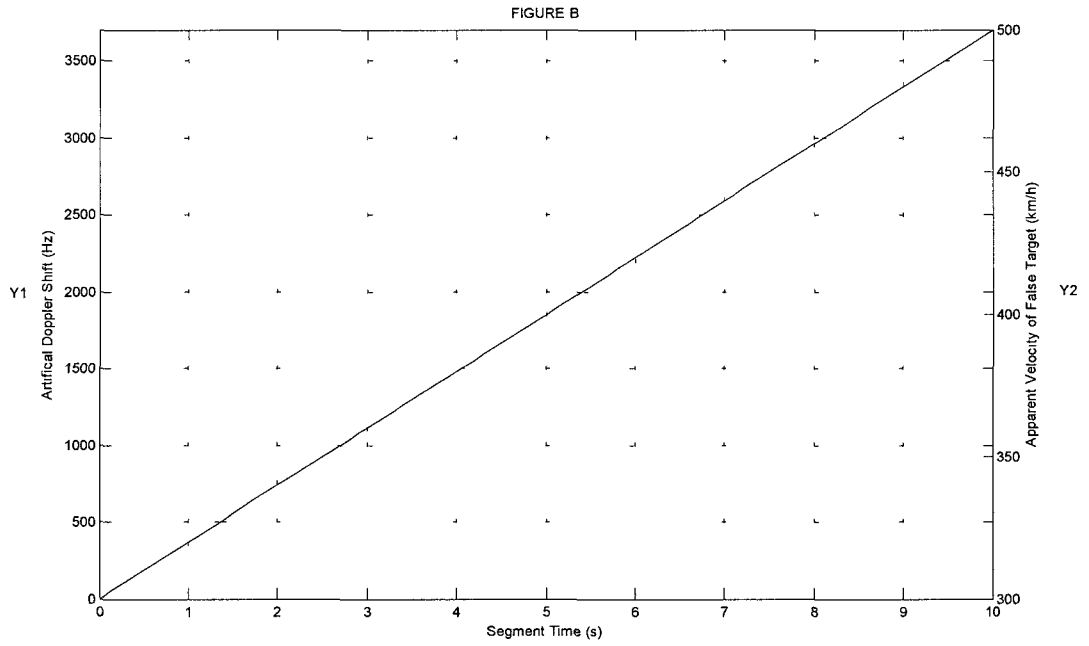
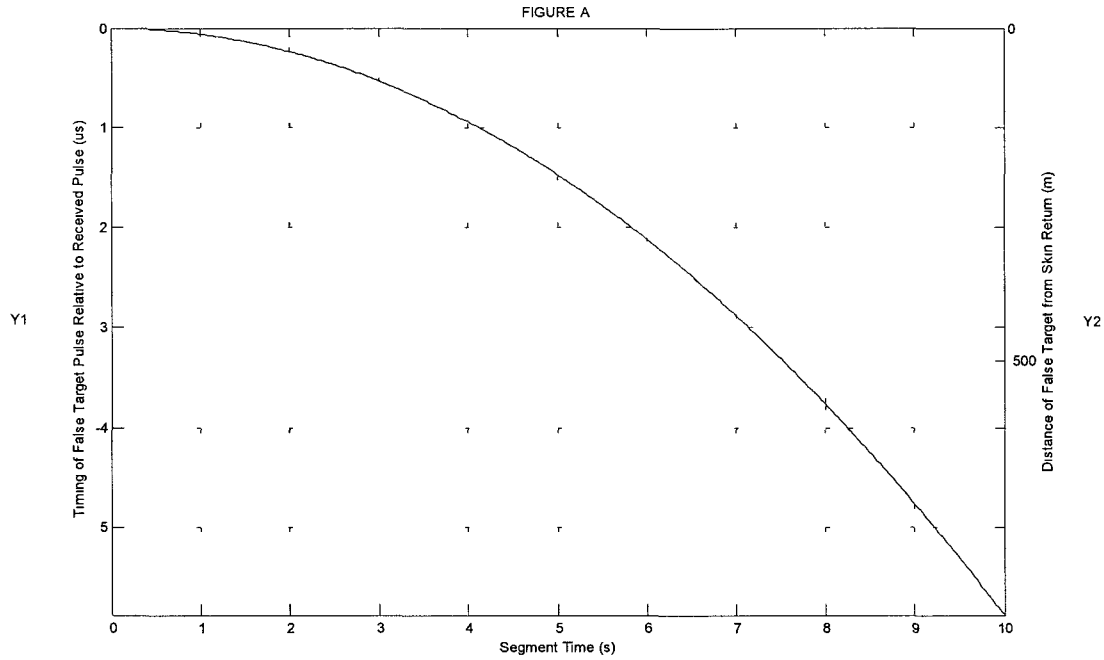


Figure 3.7 a & b: Profile 2 - False target timing and velocity information required for a linear VGPO (Carrier Freq = 10 GHz, True Velocity = 300 km/h, Technique Time = 10 s, Final False Target Velocity = 500 km/h)

In a CRV technique, both Doppler and delay are applied in a coordinated manner to produce the most realistic jamming waveform. Consider a case where a fighter aircraft is moving towards the radar at a speed of Mach1 (343 m/s or 1234.8 km/h). Upon detecting it is being strobed by a K-band fire control radar operating at 15 GHz, a CRV is used to pull the tracker off the target, making it appear that the target is slowing down to a speed of 600 km/h in 10 seconds. Note the corresponding acceleration is 17.6 m/s^2, which is well within the capabilities of a fighter aircraft. The profiles in Figure 3.8 were created and show both a delay and artificial Doppler needed to be produced. Note that the timing and Doppler information is now coordinated.

The last profile demonstrates a case where the radar PRI must be known by the jammer. In this example, a CRV technique is employed in the up-range direction, with the final false target distance specified at 1.0 km in the 10 second technique time. It was assumed that the radar carrier frequency was 8 GHz and the jammer platform was moving away from the radar at a velocity of -1234.8 km/h. This corresponds to a deceleration of 20 m/s^2, with the final apparent jammer platform speed of -874.8 km/h to match the distance profile. A positive artificial Doppler will therefore be applied to make it appear the platform is slowing down. Figure 3.9 shows that a pulse advance of 6.7 μs will be required at the end of the technique time to achieve the desired separation of 1.0 km between the skin return and false target towards the radar.



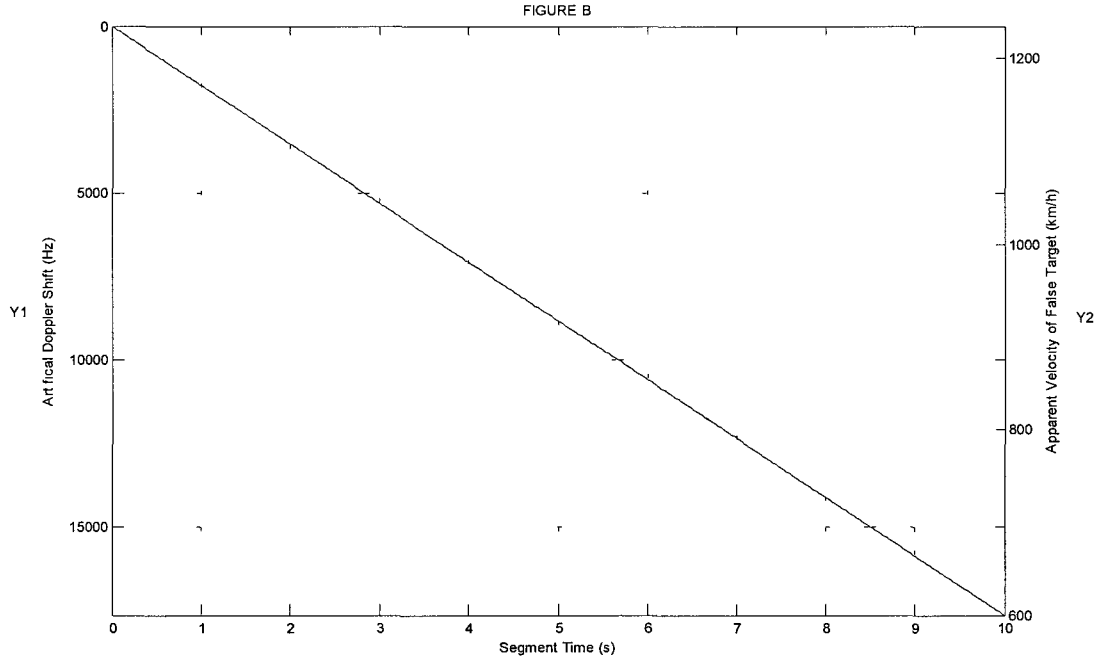
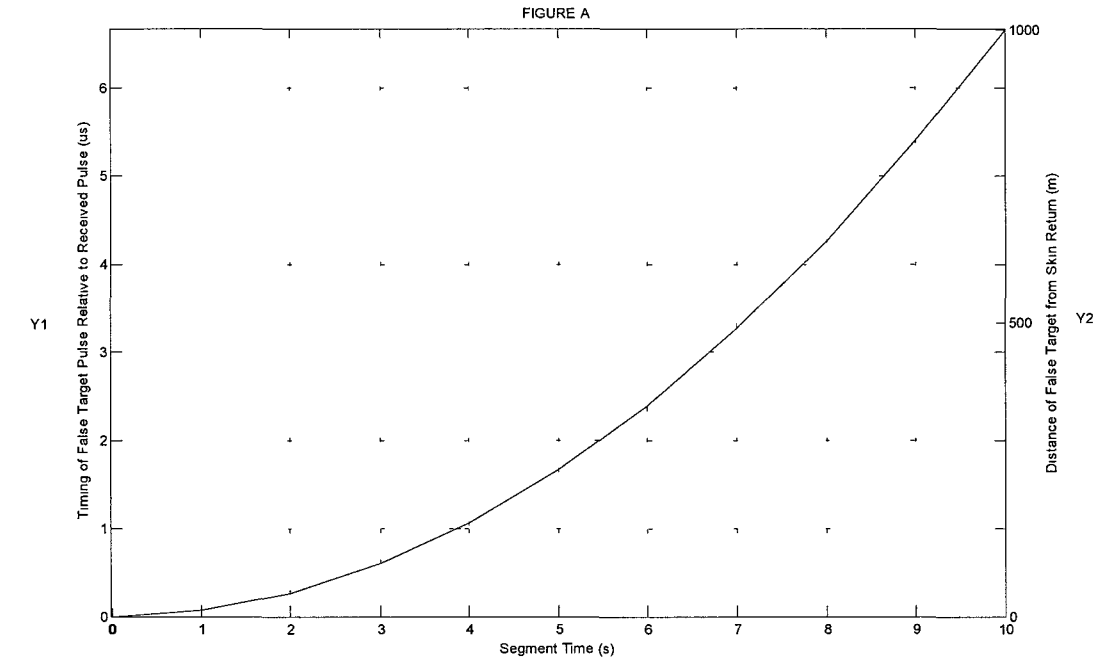


Figure 3.8 a & b: Profile 3 - False target timing and velocity information required for a CRV (Carrier Freq = 15 GHz, True Velocity = 1234.8 km/h, Technique Time = 10 s, Final False Target Velocity = 600 km/h)



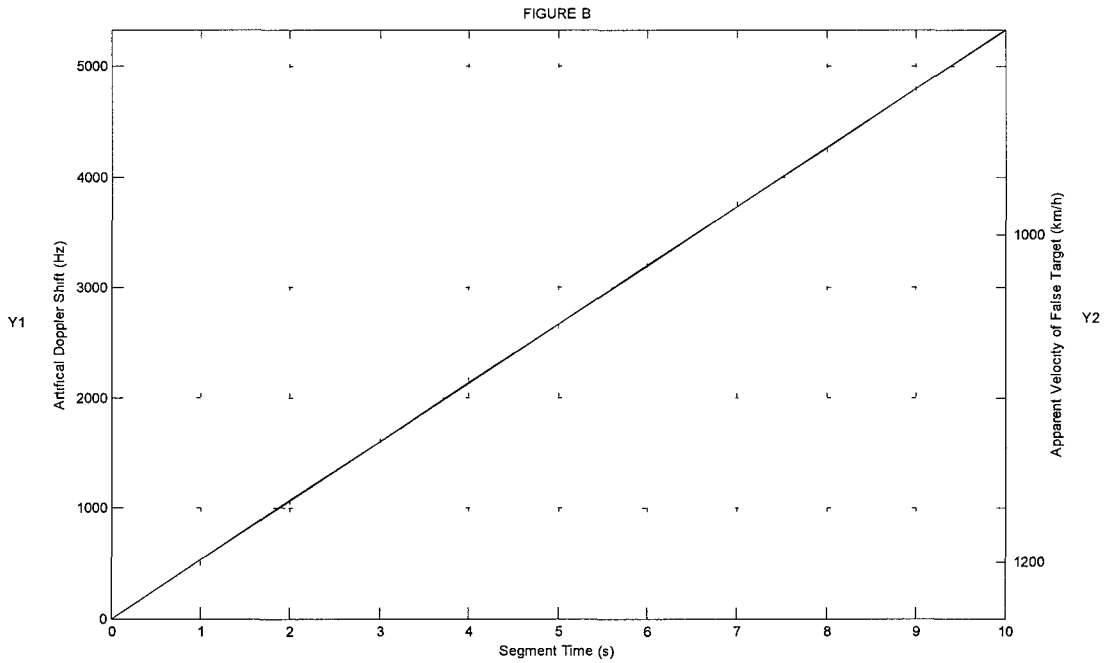


Figure 3.9 a & b: Profile 4 - False target timing and velocity information required for a CRV (Carrier Freq = 15 GHz, True Velocity = -1234.8 km/h, Technique Time = 10 s, Final False Target Distance = 1500 m)

When noise is being used, only the mask size and noise bandwidth are required, with no coordination required between these two variables. The mask size determines how many range bins ahead and behind the target are filled with noise, while the noise bandwidth will hide the true Doppler of the target. To determine this frequency, the maximum and minimum Doppler shifts, corresponding to movement towards and away from the radar respectively, were calculated using equation (2.9). Based on these values, the Doppler bandwidth was found. The frequency of the noise mask was then found by doubling the Doppler bandwidth, which would ensure that all possible Doppler frequencies were covered.

The above examples serve to demonstrate the scale of delays and Doppler that can be applied. Based on the true direction of movement, selected pull-off technique, and pull-off direction, many other permutations are also possible. Although any technique can be applied to any radar, the most realistic application would be noise jamming on the early warning radar, and CRV on both the surveillance and fire control radars. The next section describes how to apply these modulations.

3.5 Application of False Target Profiles and Noise

Once the radar signal has been sampled by the ADC and down converted to baseband using a complex exponential (*ie.* I_r and Q_r channels in Figure 3.1), the false target profiles can be applied. Both up-range and down-range false targets are produced by introducing a time delay in the transmitted jamming pulse. If an up-range target is

required, the previous pulse must be used as a reference. Then, by knowing the PRI, successive false targets can be placed up-range. Recall from section 2.7.1, the time delay/advancement required to move the false target to an adjacent range bin was τ seconds, where τ is the PW. The details of how time delay was measured and applied in the implementation are discussed in section 4.5.

For the VGPO and CRV techniques, where Doppler modulation is required, a unique idea to introduce the modulation at baseband was proposed in [20]. An artificial Doppler shift can be applied by using the identities in equations (3.5) and (3.6). The main advantage of producing the frequency modulation digitally at baseband is that it eliminates the need for variable LO which would normally be required to produce Doppler modulations during the signal up conversion to IF. Also, since I_r and Q_r data are being outputted from the digital down conversion, implementation of the Doppler modulation in this manner is computationally efficient. In equations (3.5) and (3.6), I_r and Q_r are the in-phase and quadrature-phase input channels to the jammer, A is amplitude, β is the desired Doppler shift and α is the baseband frequency. The jammer output is given by Q_j and I_j.

$$Q_j = A\sin(\alpha+\beta) = \sin(\alpha)\cdot A\cos(\beta) + \cos(\alpha)\cdot A\sin(\beta) = Q_r \cdot A\cos(\beta) + I_r \cdot A\sin(\beta) \quad (3.5)$$

$$I_j = A\cos(\alpha+\beta) = \cos(\alpha)\cdot A\cos(\beta) - \sin(\alpha)\cdot A\sin(\beta) = I_r \cdot A\cos(\beta) - Q_r \cdot A\sin(\beta) \quad (3.6)$$

Depending on the arrival time of the radar pulse, the β value will be obtained from the profile and applied to the I_r and Q_r channels to obtain I_j and Q_j. The signal will then be delayed the appropriate time before being sent for up conversion.

Application of noise jamming is straightforward. Once the leading edge of a radar pulse is detected, a fixed number of noise samples are sent for up conversion. Prior knowledge of the sampling rate and radar PRI allows for accurate placement and duration of the noise mask.

3.6 Simulation Results

Jamming techniques were applied in simulation to the radar waveform they were designed to counter. The output of the simulations was primarily studied in the frequency domain to verify that the false target pulses had the correct Doppler or noise spectrum. For noise masking, the output pulse was also viewed in time to verify that jamming pulses were longer than transmitted radar pulses. The up conversion process was done in Matlab by multiplying the complex baseband data by a cosine tuned to the IF. A complex Fast Fourier Transform (FFT) was done on the data to produce the spectrums shown.

In the first example, the early warning radar from Table 3.1 was used as the input waveform to the jammer. A noise jamming technique, meant to hide both Doppler and range bins, was selected. For demonstration purposes, it was decided to mask 10 range bins up-range and 5 range bins down-range, for a total mask size of 15 range bins. This corresponded to a total mask time of 150 μs. The frequency bandwidth of the noise was determined by knowing the maximum velocity the jammer platform would travel, as well as the highest carrier frequency expected. In this case, it was assumed the radar would operate at frequencies lower that 5 GHz, and the maximum velocity of the jammer was

1500 km/h, giving a Doppler bandwidth of approximately 30 kHz. Therefore, the noise bandwidth of 60 kHz was deemed sufficient to cover the Doppler produced at all possible velocities. Figure 3.10 shows the IF jammer output.

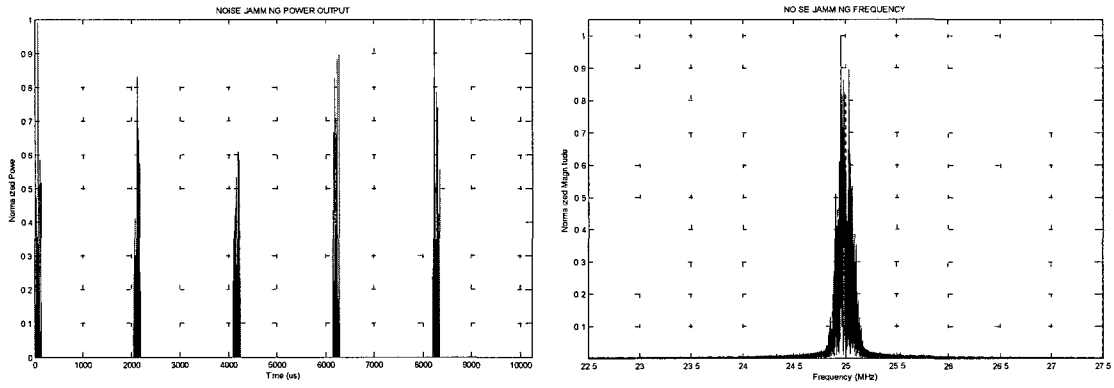


Figure 3.10: Jammer output pulses power and frequency plots

Next, the CRV in Profile 3 (Figure 3.8) was applied to the fire control radar in order to verify the implementation of artificial Doppler signals. The carrier was specified at 15 GHz. The true velocity of the jammer was 1234.8 km/h and final false velocity was set to 600 km/h. While it is true that a pulse from the fire control radar would arrive each PRI, for the purpose of clarity, Doppler results are shown for radar pulses arriving at precisely every two seconds of the profile time. The results are shown graphically in Figure 3.11 and summarized on Table 3.3. It was found that the artificial Doppler applied at baseband produced the desired frequency changes at IF.

Pulse	1	2	3	4	5	6
Pulse Arrival Time (s)	0	2	4	6	8	10
Desired Baseband Doppler Modulation (kHz)	0.000	-3.527	-7.053	-10.580	-14.107	-17.633
Desired Up Converted IF (MHz)	25.00	24.997	24.993	24.990	24.986	24.982
Measured Up Converted IF (MHz)	25.00	24.997	24.993	24.990	24.986	24.982

Table 3.3: Doppler results for six pulses after applying profile 3 to fire control radar

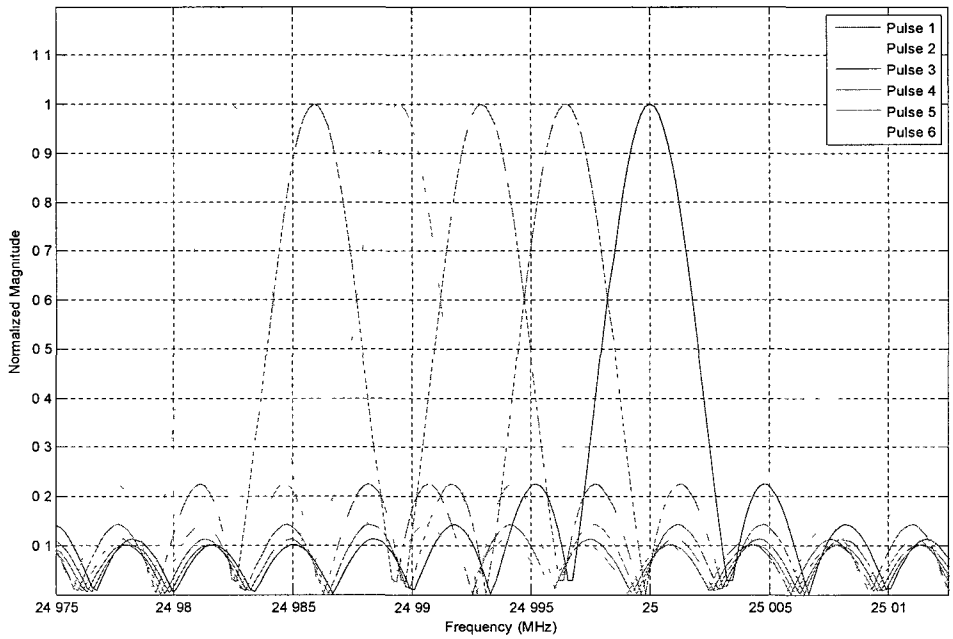


Figure 3.11: Overlaid frequencies of jammer pulses for received radar pulses

A similar test was done to verify the production of false Doppler for radars using pulse compression. The CRV from Profile 4 (Figure 3.9) was applied to the surveillance radar. Doppler shift was more difficult to measure in the pulse compressed waveform since the spectrum was not at maximum at IF. Instead, the spectrum was symmetric about the IF, with maximums at plus and minus the chirp bandwidth. It was decided to

use a reference point from Pulse 1 (which had no artificial Doppler applied), to measure the Doppler shift on the remaining pulses. Any consistent reference point along the spectrum could have been used, but for the sake of convenience, the left-sided maximum was selected. Results are provided in Table 3.4 and Figure 3.12.

Pulse	1	2	3	4	5	6
Pulse Arrival Time (s)	0	2	4	6	8	10
Desired Baseband Doppler Modulation (kHz)	0.000	1.067	2.133	3.200	4.267	5.333
Measured Right-sided peak of Upconverted IF (MHz)	22.299385	22.300529	22.301483	22.302628	22.303581	22.304726
Offset frequency from Pulse 1 (kHz)	0.000	1.144	2.098	3.242	4.196	5.341
Error (Hz)	0.0	77.7	-35.2	42.5	-70.5	7.2

Table 3.4: Doppler results for six pulses after applying profile 4 to surveillance radar (using a 524K point FFT)

One final observation was that the number of points in the FFT needed to be carefully considered when analyzing Doppler shifts. In general, the Doppler shifts required by the jamming profiles (generally measured in kHz) are small relative to the IF (generally measured in MHz). The number of points in the FFT should be determined such that there is adequate frequency resolution in each FFT bin. The FFT bin width, given by the sampling rate divided by number of points in the FFT, should be less than the artificial Doppler shift between measured points. Otherwise, the Doppler shift may not be accurately measured, as demonstrated in section 5.3.

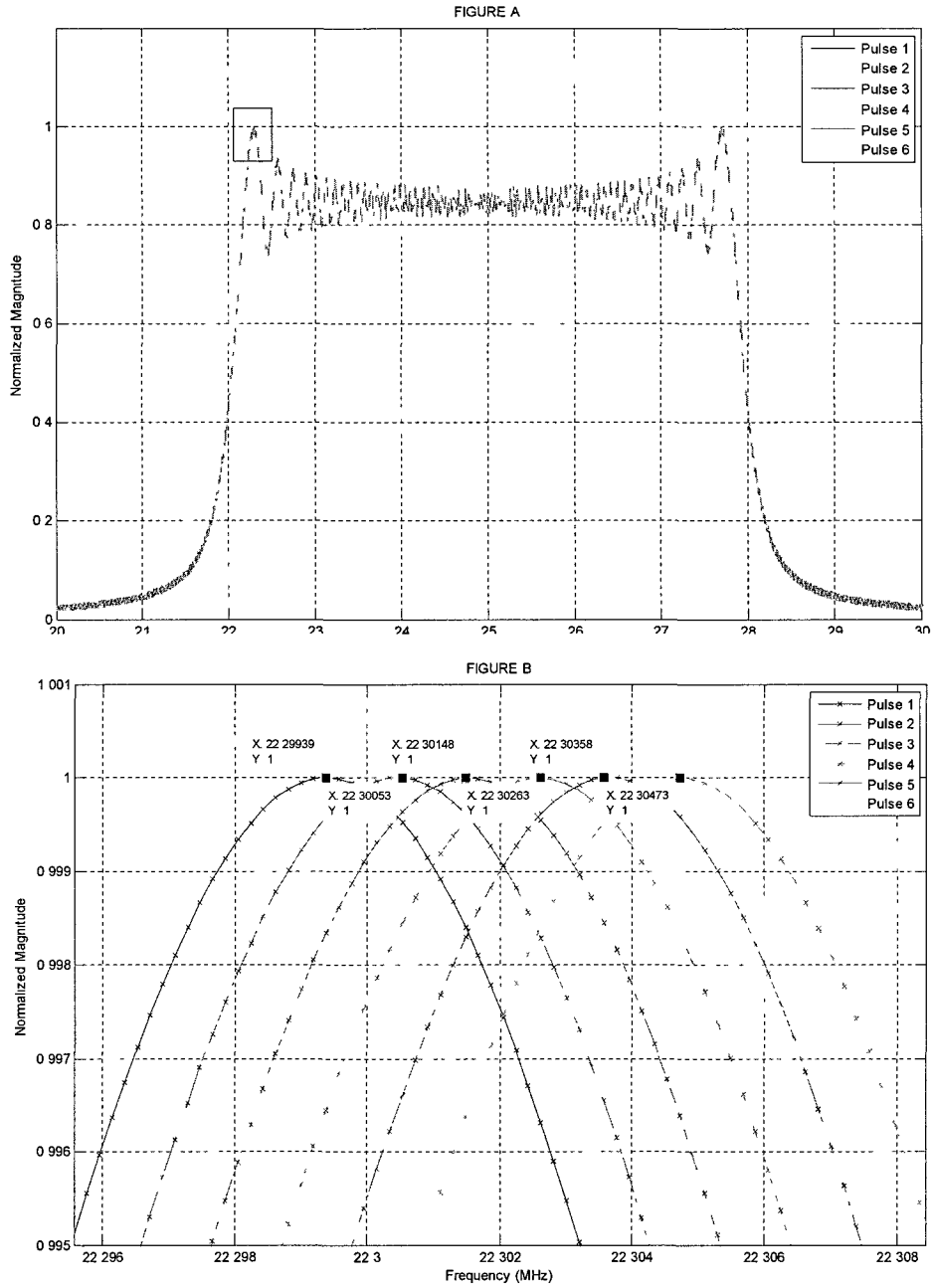


Figure 3.12 a &b: Overlaid IF spectrums for FM Chirp. Figure b shows a zoomed in view of the boxed area

3.7 Areas of Concern

Since the simulations did not stress the "real time" nature of the jamming application, the main concern is that software may not be able to keep up with real data rates. For example, consider the application of Doppler. Rather than arbitrarily selecting a few pulse arrival times, this algorithm would be applied to thousands of pulses in a single jamming profile for an actual implementation.

Another concern with real time application is related to profile resolution. The profiles shown in section 3.4 were generated with a relatively small number of data points (the time between points was 0.1 seconds). Since radar PRI are much smaller, the time resolution of the profiles would have to be increased significantly to create smooth pull-offs. This will likely not be a concern in terms of memory size, however, it could impact the indexing process required to obtain the time and Doppler data from the profile.

The application of profiles would also require additional consideration. In simulation, the Doppler algorithm was applied to the pulse train, rather than individual pulses. In reality, each received pulse would receive a different Doppler and be up converted and transmitted individually. It was evident that a detection mechanism would be required to find the leading and trailing edge of pulses. For the noise jamming technique, a method of producing noise would be required. Both noise and pull-off techniques would require a stable clocking mechanism would be needed during implementation to accurately place false targets either up or down-range.

Lastly, additional noise and signal corruptions would be added from the system during implementation, which could impact the results. The implementation will study both signals with and without artificial noise added.

3.8 Summary

The main confirmation from simulations was that the baseband algorithm was correctly implementing the specified profile Doppler shifts. It was shown to be successful for both rectangular pulsed waveforms and as well as linear FM compressed pulses. Two other important conclusions were that profile data was being generated correctly. This meant the profile code could be re-written in C++ as part of the jamming software module. Also, having generated the radar pulses in Matlab, the data could be passed to an ADC to produce analog radar signals at IF. Both of these steps were done as part of the hardware implementation.

Chapter 4

Implementation

4.1 General

In this chapter, details of the hardware and software implementation are discussed. They include the production of artificial radar signals that feed into the jammer, management of sampled data, and the framework for the custom jamming software.

The hardware selected for implementation of the Software Jammer was the D-TA suite of sensor processing equipment. Although the D-TA hardware was developed as a generic sensor processing system, it has two distinct features that make it suitable to use for jamming applications. First, the hardware is able to handle high data rates without loss of data during transfer. The second advantage is that the D-TA software architecture is built such that custom user applications can be easily added and integrated into the system. This allows for specialized jamming applications to be implemented.

The D-TA sensor processing system, as illustrated in Figure 4.1, consists of a front-end RF receiver (DTA-3200), an IF/Baseband transceiver (DTA-2300), and a data storage and processing unit (DTA-1000 or DTA-5000). Since the RF front end is used only for up and down frequency conversion, it does not affect the applied baseband artificial Doppler or timing of the jamming pulses. Consequently, in order to focus on the IF processing, the RF front end was deemed to be beyond the scope of the thesis. The

IF to digital conversion is implemented using the state-of-the-art DTA-2300 IF Radio Transceiver. Depending on the model, the DTA-2300 can have 1, 4, 8, or 16 transmit and receive channels, with each channel featuring a 130 MHz, 16-bit ADC and a 500 MHz, 16 bit-DAC. The 16 channel system was used, although only one of the channels was required for this jammer. Within the DTA-2300, an internal Digital Down Conversion (DDC) is available in the FPGA core, separating the input data into I and Q channels (refer to Figure 3.1). The backend consists of either the DTA-1000 processing server or the DTA-5000 Record and Playback module. In this case, the DTA-1000 processing server was used to perform all real time processing. The server was a quad core Linux CentOS 5.4 Server with 8 CPU, each running at a processing speed of 2 GHz. In terms of memory, 7 GB of RAM were available and the disk space was 250 GB. The data transfer between the DTA-2300 and server was done over a 10GbE optical cable, which allows for real time transfer of data, up to 100 Msps per channel, or equivalently, 800MB/s on four simultaneous channels [26]. The maximum bandwidth per channel was 40 MHz. A photograph of the actual setup is shown in Figure 4.2.

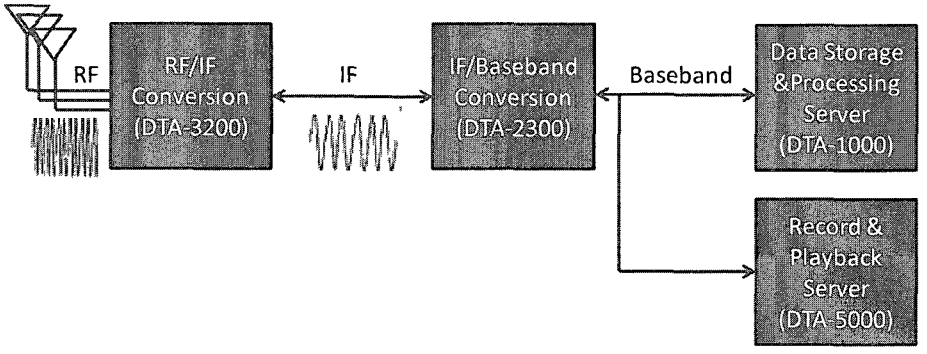


Figure 4.1: D-TA sensor processing system components

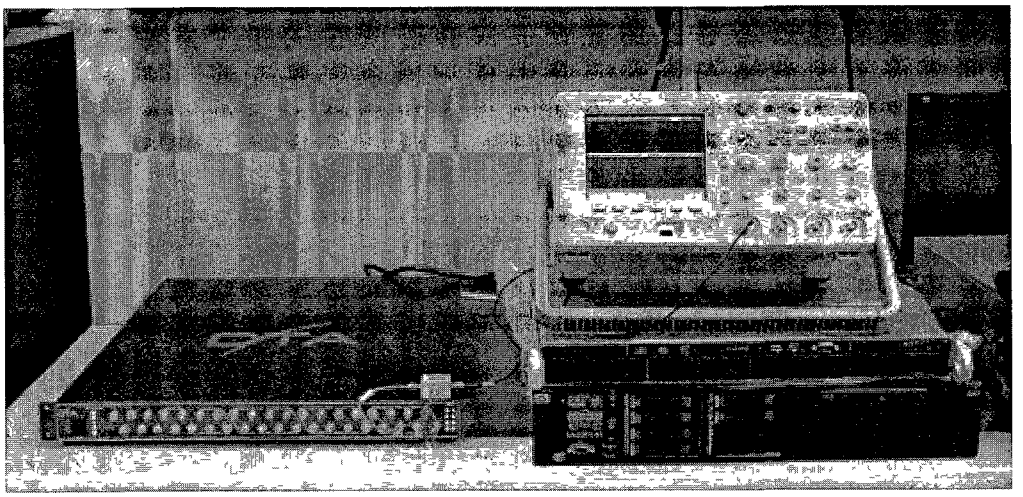


Figure 4.2: DTA-2300 and DTA-1000 used in the implementation of the software jammer

4.2 Hardware Architecture

4.2.1 Production of Input Radar Signals

Without having access to actual radar systems, a means of artificially producing radar signals was first required. Recall from section 3.3 that three types of radar signals were created in Matlab, representing early warning radar, surveillance radar, and fire control radar. These simulated signals were converted to analog signals using the DAC chip in the DTA-2300. To do this, the necessary header information required by the DTA-2300 was included in the Matlab radar signal data, and then saved on the DTA server. Then, by repeatedly looping the data through the DAC, a continuous train of analog radar pulses were produced. Detailed information regarding the TI DAC5687 chip and data transfer mechanism can be found in [24] [27], and is summarized below.

Figure 4.3 shows the general structure of a signal packet for data transfer used by the DTA-2300. The data transfer follows a User Datagram Protocol (UDP), meaning data is transferred between the source and destination without any handshaking. This makes UDP preferable for real time or time sensitive applications. Large UDP datagrams are used to transfer data between the DTA-2300 and DTA-1000. These datagrams, more commonly referred to as packets, are broken up into up to 7 frames, with each frame having up to 4096 samples. Since each sample is 2 bytes, the maximum content was 57344 bytes of data per packet. A 32 byte header is included for each datagram, making the total size of a packet 57376 bytes, or approximately 56 kB. If more packets are required to fit all the radar pulse data points, the header information is simply included between each packet. Among other information, the header provides the number of samples per frame and frames per packet to the DAC.

From the DAC data sheet, it is known that a full scale signed 16-bit signal (meaning the digital amplitude ranges from -32767 to +32767) corresponds to a 3 dBm maximum output power [27]. From section 3.3, it was decided to produce the analog input signals with a peak power of about -10 dBm. An amplitude reduction factor of 2 reduced the power by a factor of 4, or equivalently 6 dB, compared to the maximum output power. Therefore, by scaling the Matlab signal to 2^{13}, the power was reduced to 3dBm-12 dB, or -9 dBm, approximately the desired peak power level.

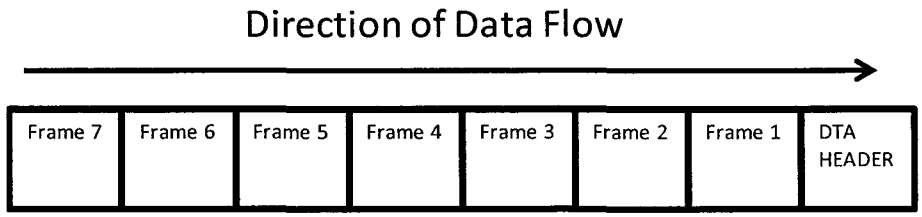


Figure 4.3: DTA-2300 packet structure showing 7 frames of data

Using this approach, the radar waveforms from section 3.3 were converted to analog and used as the IF representation of radar waveforms. In order to verify the generation of the IF analog radar signals, the output from the DAC was viewed on the oscilloscope and spectrum analyzer. Screen captures from the oscilloscopes and spectrum analyzer are found in Appendix A. Comparison of the measured versus desired parameters from section 3.3 confirmed the accuracy of the waveform generation process.

4.2.2 Analog to Digital Conversion

The ADC function is implemented within the DTA-2300 using the Linear Technology LTC 2208 chip, and has a sampling rate up to 130 Msps [28]. To shift the digital spectrum to baseband, a DDC is performed on the ADC data. The process involves mixing the signal with an NCO, filtering, and signal decimation. The DTA-2300 has possible decimation rates of 2, 4, 8, 16, and 32. Decimation by 2 maintains the same data rate since each sample has both a real and imaginary part. However, the effective complex sampling rate, F_{eff}, is given by F_s/D, where F_s is the ADC sampling rate and D is the decimation. The filtering process removes signal alias' outside the bandwidth. The filter coefficients are selected by default based on the decimation rate,

but can be adjusted if required. The data is then decimated by removing every D-1 sample.

From Table 3.1, it was known that the analog IF spectrum was centered at 25 MHz with a maximum bandwidth of 6 MHz. With this information, it was determined that the analog IF signal could be under-sampled without introducing adverse effects from aliasing. Minimizing the sample rate is important since it reduces the data speed and therefore allows the software more processing time between received samples. To under-sample, it was decided to set the ADC sampling rate, F_s, to 32 Msps. This resulted in the digital spectrum being centered at 7 MHz, as well as the expected signal images. A DDC was then performed to mix the data down to baseband. Using decimation by 2, the effective (complex) sampling rate, F_{eff}, was 16 MHz. After mixing, a LPF was used to remove the signal images, leaving a single spectrum. Figure 4.4 illustrates the spectrum produced through the ADC and DDC processes. After the down conversion, the digital baseband data (I_r and Q_r) was sent interleaved to a 10GbE data pipe for processing. Note that the standard D-TA header was also added between each packet of data. This header contains information such as the number of samples per frame, frames per packet, and time stamp data of when the header was created. The stamp is accurate to 6.4 ns.

The default cutoff frequencies for the LPF assuming an ADC sampling rate of 32 Msps is shown in Table 4.1. Comparing these values with the radar specifications from Table 3.1, it is clear that higher decimation rates may not be effective. Specifically, in some instances, the signal spectrum is cutoff by the LPF. In other cases, the effective

sampling rate does not satisfy the Nyquist Sampling Theorem. Note that according to the Sampling Theorem, a signal of bandwidth B must be sampled at a rate of $2B$. However, since the effective sampling rate is a complex sampling rate, it is effectively doubled. Therefore, a complex sampling rate of B or greater is required for signals of the same bandwidth [1].

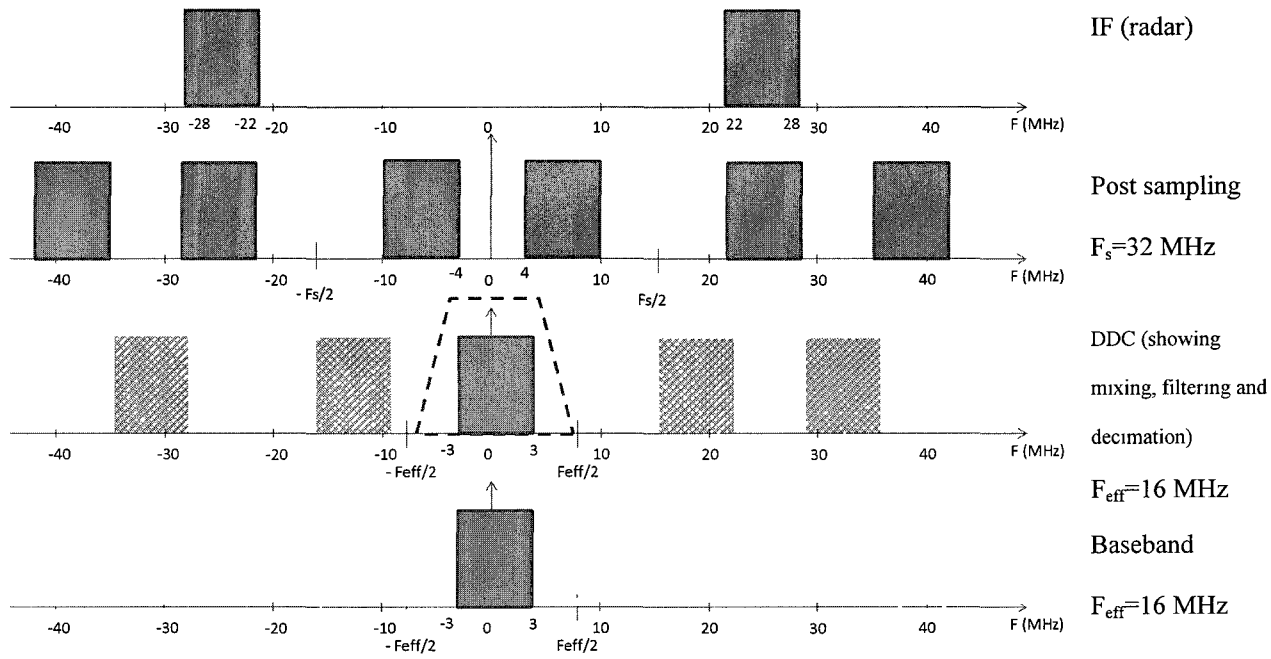


Figure 4.4: Spectrum illustrations of the ADC and DDC process

ADC Sampling Rate (Msps)	32				
Decimation Rate	2	4	8	16	32
$F_{effective}$ (Msps)	16	8	4	2	1
Default LPF cutoff (MHz)	5.6	2.4	1.2	0.64	0.40

Table 4.1: DDC parameters for various decimation rates assuming ADC sampling rate of 32 Msps

4.3 Software Architecture

4.3.1 General

The software framework associated with the DTA-2300 can be separated into Control and Data Software groups based on functionality [25]. The Control Software is primarily used to input settings into the hardware without having to know register structures. The Data Software is designed to receive/transmit data on the 10GbE datalink between the DTA-2300 and server, as well as perform real time data processing. The Data Software includes several pre-existing D-TA software modules, where each module is designed to perform a specific task. Depending on the complexity of the task, modules can be single or multi-threaded, meaning that data processing within that module is done in parallel. Customized modules can be developed and integrated into the existing software architecture.

A new software Jamming Module was created and incorporated with three existing D-TA modules. The three D-TA modules include the ADC Server Module, the DAC Client Module, and the DAC File Read Module. The ADC server module receives the sampled data from the hardware and checks for dropped data, while the other two modules are responsible for reading the Matlab radar file and continuously feeding it to the ADC in order to produce the simulated radar signal. The customized Jamming Module is responsible to perform all jamming functions. All of these modules are single threaded. A block diagram of the interaction between software modules and hardware is shown in Figure 5.13.

The Jamming Module was designed to receive real time data from the ADC Server module. Data transfer between modules was accomplished using data pipes. Each pipe consists of a ring buffer, broken down into equal sized blocks. By default, each ring buffer has 5 blocks, each with a size of 128 MB. The structure of blocks, packets, and frames in each turn of the ring buffer is illustrated in Figure 4.5. A write pointer tracks the progress of the ADC Server module writing to the buffer, just as a read pointer tracks the progress of the Jamming Module reading the data. Data is simultaneously being written and read from the buffer, but under the limitation that reading and writing cannot be done concurrently within the same block.

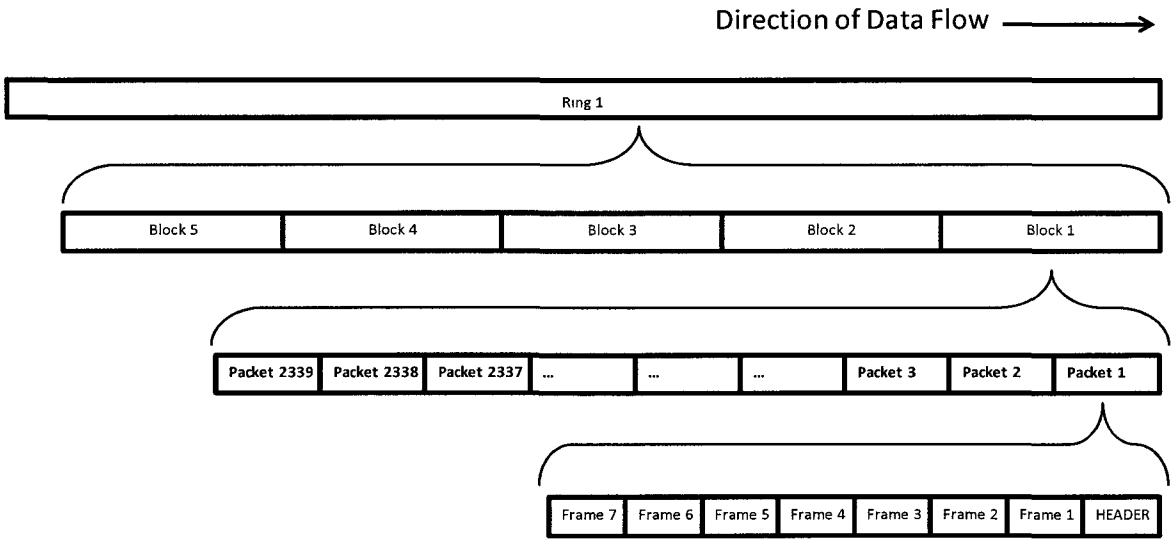


Figure 4.5: Data structure breakdown between software modules

4.3.2 Customized Jamming Software

As shown in Figure 4.6, the Jamming Module operates in four sequential stages. In the first stage, the software is idle in the sense that no data from the ADC flows into

the ring buffer. The information to create the jamming profiles is entered or modified, and the input radar can be selected by changing the data file read by the DAC. Changes can also be made to the ADC sampling rate, decimation, filter coefficients, or output display options. In terms of the jamming profile, recall that the control parameter is time. Knowing the effective sampling rate, time can be given in terms of received sample count. For a 10 second profile, and a sampling rate of 32 Msps with decimation by 2, there would be 160 million received samples (62.5 ns between samples), with the same number of points on the Doppler and time delay arrays. This represents the maximum profile resolution that can be achieved, but is impractical since such a fine resolution is not required for most profiles. Instead, by considering the shape of the profile and smallest expected PW, it was decided that the time resolution on the profiles should be 1 μs. This meant 10 million possible Doppler and time delay values.

In the second stage, data flows from the ADC to the ring buffer. The time it takes to fill the buffer depends on the ADC sampling rate and the decimation factor in the DDC. For example, if the ADC is set to 32 Msps, and the decimation is 2, it takes approximately 10.5 seconds to fill the 640 MB ring buffer. Since there is a requirement to be able to detect individual jamming pulses (which was not done in the simulations), a simple but effective envelope detection scheme is used. This is achieved by performing a power calculation on each complex sample for the duration of two rings around the buffer. By default, the detection threshold is set to a level based on 25% of the measured peak power. Since power is being calculated from the complex samples (*ie.* I_r and Q_r

data in Figure 3.1), the power will remain above the threshold for the duration of the pulse.

In the third stage, the leading and trailing edges of the pulses are found by comparing the power to the detection threshold. The power in the jamming pulse is raised linearly by a factor of 10 over the course of one ring to capture the range/Doppler gate (see section 2.6). Furthermore, time measurements for PW and PRI can be made by knowing the sample count at the leading and trailing edges and the effective sampling rate. Detection of the leading edge is also important because it creates a time reference which allows for the placement of false targets up and down-range.

Finally, the fourth stage produces the actual pull-off effect. For the duration of the technique time, the pulse leading edges are detected. For deception jamming, the leading edge time is indexed with the jamming profiles to obtain the desired Doppler modulations and time delays/advancements. Then, each sample with an instantaneous power above the detection threshold is frequency shifted. Up and down-range false targets are realized by holding the frequency shifted data by the appropriate number of samples. For disruptive noise jamming, the leading edge of a pulse is used anticipate the arrival of the next pulse. Noise is then introduced into the I_j and Q_j channels at the appropriate time to mask the echo signal in time and frequency. Upon termination of the jamming, the module returns to stage one.

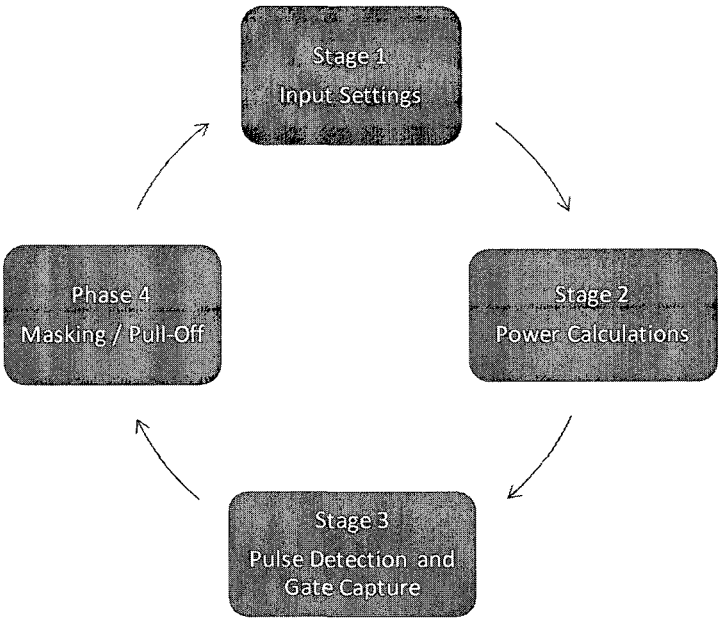


Figure 4.6: Jamming Module software stages

It should be noted that only minor changes were made to the D-TA Control Software to allow for new menu options related to selection of jamming method.

4.4 Up Conversion

Ideally, the data at the output of the jammer would flow back through the DTA-2300 and the RF front. Since the processing is done on complex baseband data, a Digital Up Conversion (DUC) must be performed to mix the signal to IF. The DUC process is performed in the DTA-2300 DAC, and includes steps for signal interpolation, low-pass filtering, and mixing with an appropriately tuned NCO. The interpolation factor, I_x, pads the baseband signal with I_x-1 zeros between samples, and has the possible values of 2, 4, or 8. After interpolation, the signal is mixed with a complex exponential tuned to the desired IF. Either the real or imagery data from the mixed signal can be sent to the DAC to produce the output analog signal.

The minimum interpolation factor can be calculated based on the ADC sampling rate, decimation, desired IF and signal bandwidth. The effective complex sampling rate, F_{eff}, is given by F_s/D, where F_s is the ADC sampling rate and D is the decimation. During the up conversion, F_{eff} is increased by a factor of I_x due to the interpolation process. Finally, to satisfy the Nyquist sampling theorem, the up conversion sampling rate should be at least twice the desired IF plus half the signal bandwidth. The following equation is then obtained, where B is the signal bandwidth.

$$F_s \frac{I_x}{D} \geq 2(IF + B/2) \tag{4.1}$$

Substituting the ADC sampling rate of 32Msps with a decimation by 2, 25 MHz for the IF, and the largest expected bandwidth of 6 MHz, the minimum interpolation is found to be 4. After the DUC process, data from either the I_j or Q_j channel is fed through the DAC to produce the analog IF signal. The signal spectrum during the DUC is illustrated in Figure 4.7, where F_{eff} is 16 MHz, and I_x equals 4.

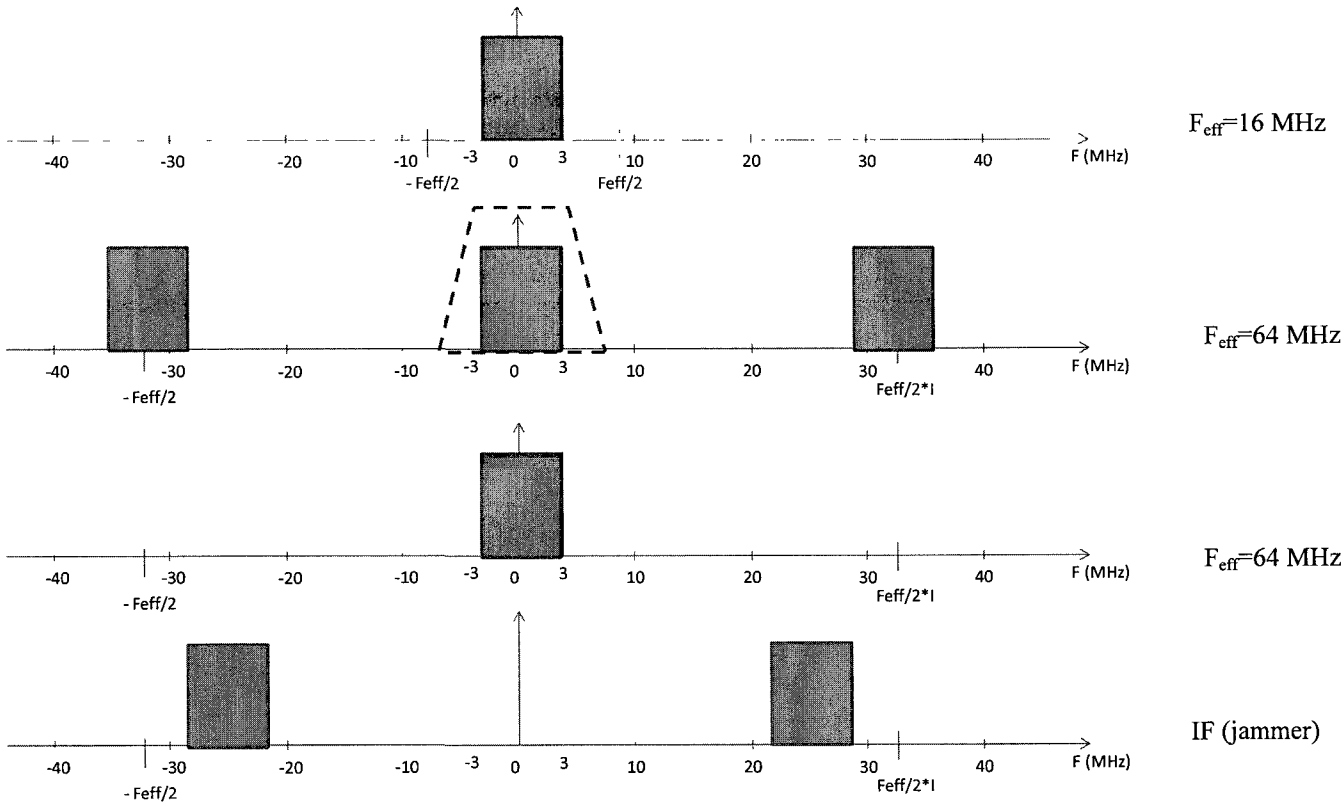


Figure 4.7: Spectrum illustrations of the DUC and DAC process

Unfortunately, the up conversion process was not possible for this implementation since the DAC was already employed to produce the simulated input radar signal. If actual radar data or a versatile signal generator was available to produce the analog IF signal, it could be directly fed into the ADC, thereby freeing up the DAC resource. Under the constrain of this set-up, two other options were considered. The first option involved using two channels in the DTA-2300, where the digital data from the first channel could be passed to the second for up conversion. Implementation of this option would require the creation of another software thread in order to pass data between channels. The second option involved exporting data into Matlab for analysis. This option would give much more flexibility to validate the performance of the jammer, since

the data could be viewed in the time and frequency domain, as well as be compared to desired profile. The downside is that the up conversion process would not be performed in real time. Given these choices, and considering the time and resources available, option two was selected.

4.5 Real Time Implementation Challenges

Although the up conversion was not done, there were several challenges in maintaining software functionality at data rates up to 32Msps. One challenge was to find an accurate method of holding jammer data for short periods of time in order to produce up or down-range targets. As dictated by the jamming profiles, the delay times were on the fractions of microseconds. One option was to use a time stamp function from a pre-existing C++ library. However, it was found that the clock resolution (a single microsecond at best), would not allow for the accurate placement of false targets. A second option would be to use of the CPU processor clock, operating at a frequency of 2 GHz. Theoretically, the time resolution of this clock is 1/2GHz, or 0.5 ns, much finer than required by the profiles. However, it was found that since the CPU clock is shared between the thousands of processes running in the server, it could not be dedicated to the software without having adverse effects on concurrent processes. The best option to measure time was to indirectly use the NCO from the DTA-2300 by counting the received samples. The data from the DDC was received every $1/F_{eff}$ seconds. Assuming F_{eff} was 16 MHz, this meant time could be measured to the nearest 0.0625 μs. Not only was this sufficient resolution, but the clock source was stable and dedicated. Therefore, by using the NCO clock, the time delay was realized by counting the number of received

sample after a LE. This allowed for the accurate placement of false targets up and down-range.

The manner in which the indexing was done played a significant factor in processing speed. Based on the received sample count, the profiles were searched for the closest time data point (recall the profile resolution was to the nearest microsecond). In the early versions of the jamming software, the array was searched using different methods. First, the array was compared from start to finish until the match was found. Unfortunately, this process was wasteful, especially as the technique time progressed, since the search was always started from the beginning of the profile time. Instead, the search could start at the middle of the technique time, and based on the difference, the error could be successively reduced in each search until matched. Another method to shorten the search time was to start the search from the last matched index. In the later versions of the software, it was found that indexing could be greatly improved by considering the received sample count and the profile time resolution. In this manner, the received sample count was appropriately rounded and divided by the count resolution to provide the index value. Essentially, this meant that the search was replaced by a calculation.

Finally, proper allocation and reallocation of memory was vital to the functionality of the software. Based on the known PRI, sampling rate, and technique time, memory could be pre-allocated before the start of jamming to store any data of interest. The memory was freed at the end of the jamming so that it could be reused in

the next jamming cycle. Undersampling in the ADC also minimized the data points over the PW and supported the software to keep up with the data flow.

4.6 Summary

Chapter 4 provided information on the hardware and software used to implement the jammer. The main components used consisted of the DTA-2300 IF Transceiver and the DTA-1000 Processing Server. The DAC in the DTA-2300 was used to simulate an analog radar signal, which was looped to the ADC for sampling. Although faster sampling rates were possible, it was decided to sample the signal at 32 Msps since the input radar signal bandwidth was known to be limited. Once sampled, a DDC was performed on the data to shift the data to baseband for processing. Two pre-existing D-TA software modules were used, and a new customized Jamming Module was created. The Jamming Module operated in four sequential stages that included input settings, power calculations, pulse detection and gate capture, and masking / pull-off. Since signal up conversion was not possible, the output of the jammer would be validated by saving the baseband data and analyzing it in non-real time using Matlab. Chapter 5 contains these results.

Chapter 5

Results

5.1 General

This chapter discusses the functionality of the implemented software jammer. Even though some simulations were carried out previously in Matlab (see section 3.6), the requirement for processing real time data added a number of new challenges. For example, unlike the simulations from chapter 3, a pulse detection mechanism was needed so that the Doppler algorithm could be applied to individual pulses. More significantly, considering the jammer received hundreds of thousands of radar pulses in a matter of a few seconds, the processing demand on the software was much higher.

As explained in section 4.4, it was decided to verify all of the results from the jammer at baseband frequencies. In order to do this, the jamming was allowed to perform in real time, but the data was saved as arrays instead of being up converted in the D-TA hardware. At the end of the jamming, the output of the jamming software, namely the I_J and Q_J data arrays, were exported to Matlab. In addition, when needed for debugging purposes, the raw I_r and Q_r radar input data, D-TA filter coefficients, sine and cosine modulation data, and profile data were also exported for analysis. Overall, the objective was to measure the timing and frequency of the jamming pulses in order to validate the production of either disruptive noise pulses or deceptive pull-offs. A second objective was to determine the throughput time and estimate at what sampling rate the jamming software module would not be able to process data in real time.

To mirror the simulations from chapter 3, results are shown for the application of noise to the early warning radar and CRV techniques from profiles 3 and 4 (see Figure 3.8 and Figure 3.9) to the fire control and surveillance radar, respectively. A notable difference in profile 4 is that it requires the production of up-range targets. The main observations are explained, with the additional results included in Appendices B through D.

5.2 Early Warning Radar

Noise jamming was used against the early warning radar, with the radar specifications listed in Table 3.1. The SNR of the radar signal was 10 dB. After determining the peak power of the signal in stage two of the Jamming Module, a detection threshold level was set to 25% of this value (see 4.3.2). The jammer was then able to measure the time each leading edge of a radar pulse was received. Since the PRI was constant, and knowing the duration of the jamming mask, the pulse leading edge was used as a time reference for masking the next pulse. Noise data with a frequency of 60 kHz was applied into both the I_j and Q_j channels.

The baseband data was collected for both channels during a technique time of 10 seconds. Figure 5.1 shows the frequency output for the first jamming pulse.

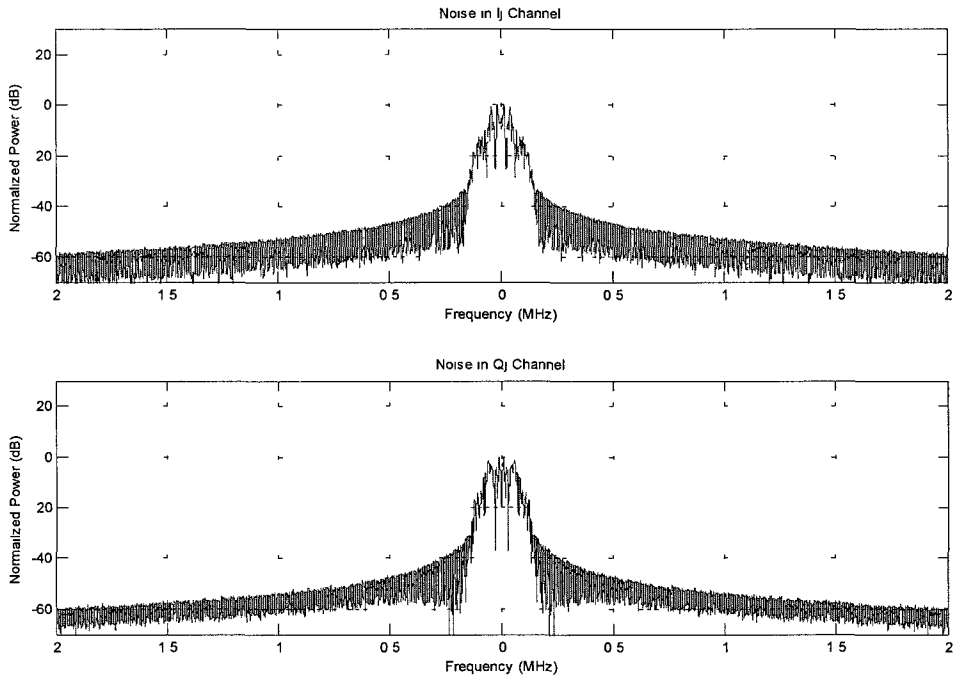


Figure 5.1: Frequency of noise generated in I_j and Q_j channels

Over the complete jamming time of 10 seconds, the jammer received 4877 radar pulses. To confirm that the correct mask size was produced, the data for every 500^{th} pulse is shown in Table 5.1. The noise mask size was measured for those pulses and was consistent with the desired value of 150 μs. Note that the timing of the noise outputted from the jammer in fact overlapped the intended radar pulse.

In graphical form, another way to show the results of spot noise is by overlaying the input radar pulses with the outputted jamming pulses. Figure 5.2 shows the power and timing of the first five radar pulses, along with the associated jamming pulses. The overlaid result confirms that the jamming pulses are outputted at the desired timings and with a higher output power.

Pulse received at Jammer	Sample Count at Leading Edge	Pulse Arrival Time (s)	Anticipated Arrival Time of next Pulse (s)	Jamming Pulse LE (s)	Jamming Pulse TE (s)	Mask Size (μs)
1	586	0.000037	0.002087	0.001985	0.002135	150
501	16,394,026	1.024627	1.026677	1.026575	1.026725	150
1001	32,787,466	2.049217	2.051267	2.051165	2.051315	150
1501	49,180,906	3.073807	3.075857	3.075755	3.075905	150
2001	65,574,346	4.098397	4.100447	4.100345	4.100495	150
2501	81,964,506	5.122782	5.124832	5.124730	5.124880	150
3001	98,357,946	6.147372	6.149422	6.149320	6.149470	150
3501	114,751,386	7.171962	7.174012	7.173910	7.174060	150
4001	131,144,826	8.196552	8.198602	8.198500	8.198650	150
4501	147,538,266	9.221142	9.223192	9.223090	9.223240	150

Table 5.1: Results of noise jamming

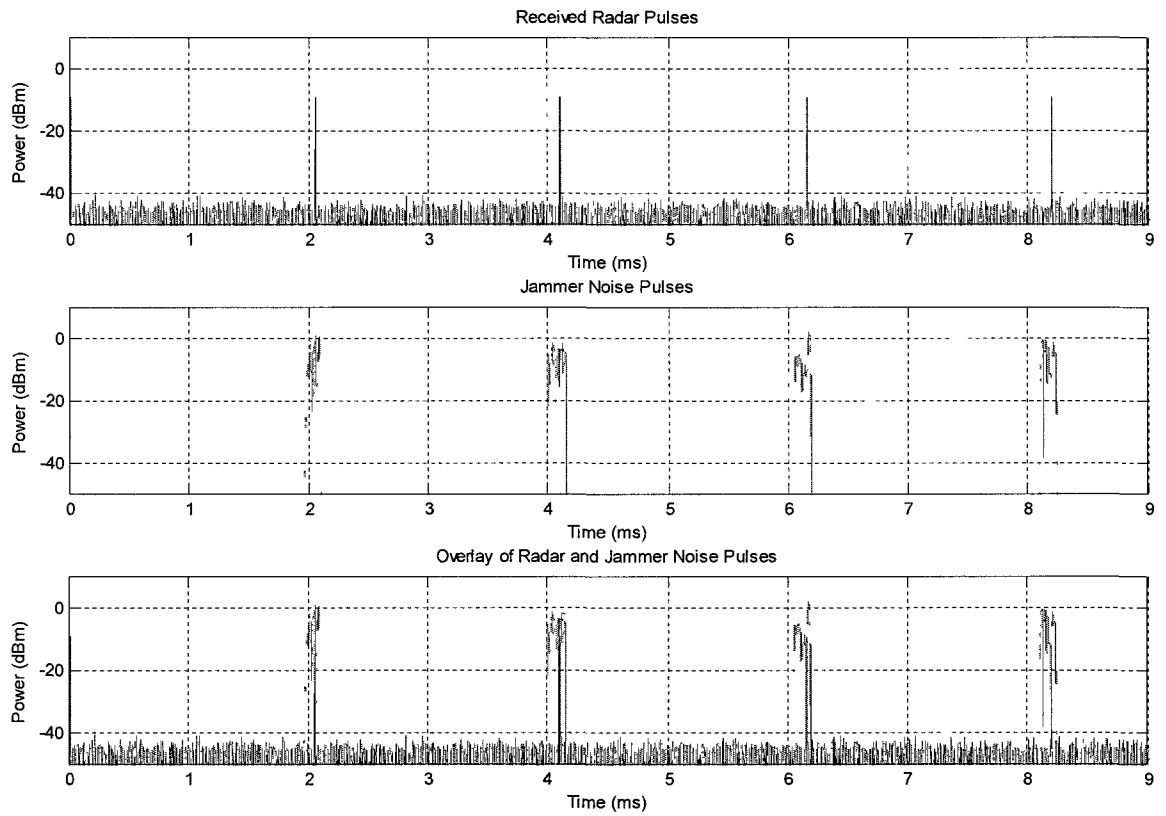
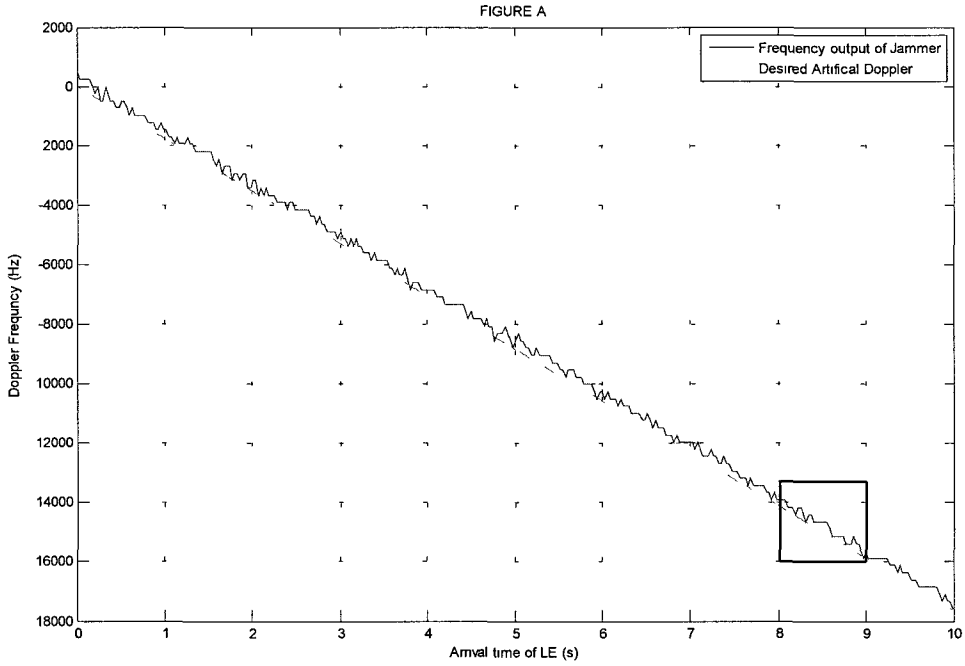


Figure 5.2: Power and timing of received radar and transmitted jammer pulses

5.3 Fire Control Radar

5.3.1 Radar Signal with High SNR

The profile 3 CRV pull-off was used against the fire control radar. Initially, no artificial noise was added to the radar signal. To accommodate memory limitations in Matlab, it was decided to view the results for every 1000th output pulse from the jammer, corresponding to a time of 30 ms between pulse data points and 333 pulses over the 10 second technique time. To confirm that the application of artificial Doppler shift were implemented correctly, a 65k point FFT was performed on the data from each pulse. The spectral peak was found for each examined pulse and the results were overlaid with the desired artificial Doppler values. The results for application of profile 3 to the fire control radar without the addition of noise for decimation by 2, 4, 8, and 16 are shown in Appendix B (decimation by 32 is not included since the effective sampling rate does not satisfy Sampling Theorem). Figure 5.3 shows the results when decimation by 2 is used in the DDC. Figure 5.3a shows the full technique time, while Figure 5.3b is a close-up of the frequency output between 8 and 9 seconds. Some interesting observations were noted.



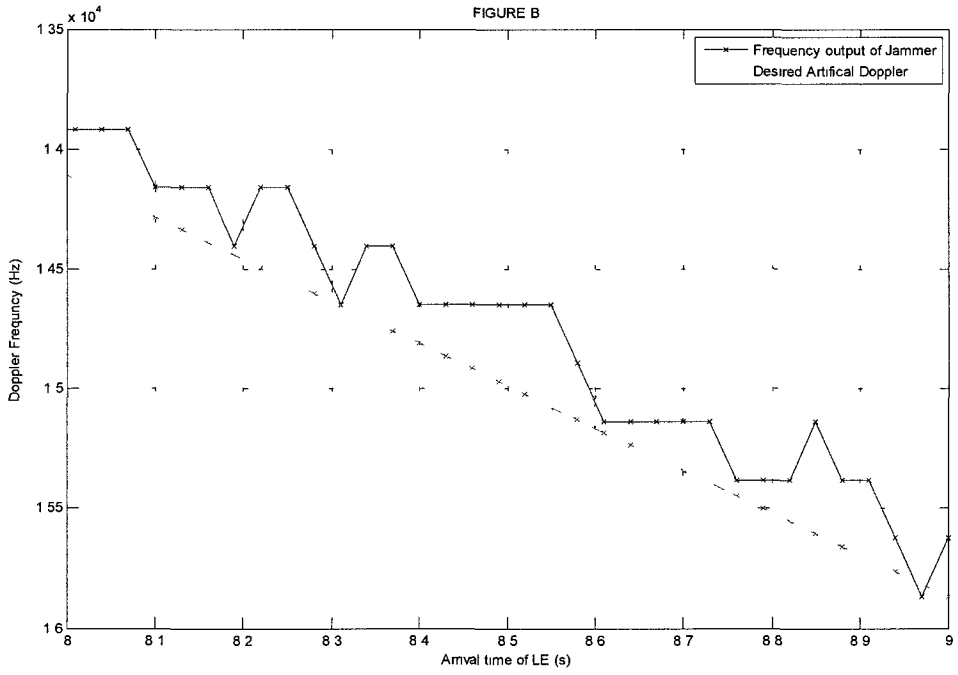


Figure 5.3 a & b: Frequency output of jammer applying profile 3 against fire control radar without additional noise, data decimation by 2

The results show that the frequency output from the jammer is composed of a discernable stepped pattern. The stepped plateaus can be explained by the fact that the frequency resolution of the 65k point FFT (given by F_{eff}/N_{FFT}, where N_{FFT} is the number of points in the FFT) is less than the Doppler difference between successive profile points. In this case, since the FFT frequency resolution was 244.1 Hz and the Doppler between successive points was 52.9 Hz, we expect to see about $244.1/52.9 \approx 5$ data points in each plateau before a noticeable frequency shift. This is confirmed by Figure 5.3b.

A second observation is the readily apparent and unexpected frequency offset from the desired Doppler. For example, for the first pulse, which was received at the jammer at 11.6 μs, the applied Doppler shift was approximately 0 Hz. For this pulse, the outputs I_J and Q_J were essentially the same as the inputs I_r and Q_r (see equations (3.5) and (3.6)). Yet, there was already a noticeable frequency offset from 0 Hz. In this example, the spectral peak of the first pulse was found to be at about 488 Hz, instead of the expected 0 Hz. The same observation was made when other decimation values were used in the DDC (see Appendix B). There appeared to be no correlation between the offset amount and the decimation selection. However, it was noted that in all cases that the Doppler offset was approximately constant throughout the full jamming cycle. Thus, the most likely cause was that the down conversion process was not centering the data exactly at baseband. To compensate for this effect, a fixed offset correction can be applied to account for the relatively constant baseband offset. In this case, the average difference between the measured and desired frequencies was found to be 266.3 Hz. With the offset correction applied and the FFT points increased to provide adequate

frequency resolution, the new result is shown in Figure 5.4, and matches very closely with the desired Doppler modulations.

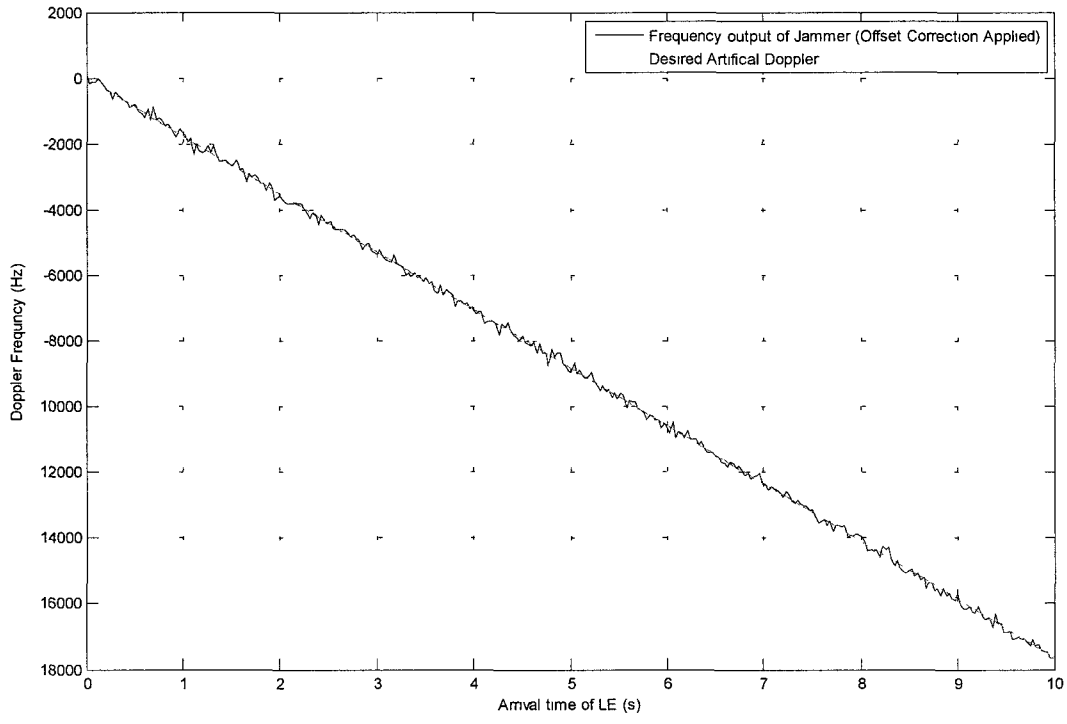
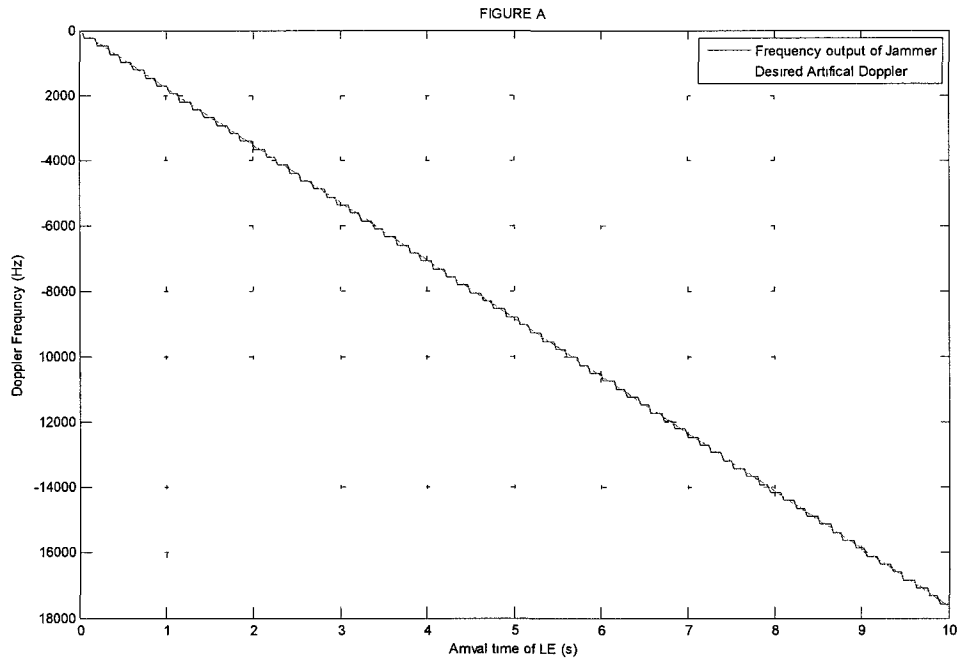


Figure 5.4: Frequency output of jammer applying profile 3 against fire control radar without additional noise, using data decimation by 2, 524k point FFT and offset correction

To determine if the frequency offset was always present when down converting to baseband, the PW of the fire control radar was increased to 5 μs, with all other parameters remaining the same. The same jamming profile was applied, and the resulting frequency plots are shown in Figure 5.5 for 65k and 524k point FFTs. In Figure 5.5a, the stepped pattern is clearly visible over the full technique time, with an average offset of 63.4 Hz. In Figure 5.5b, the steps have been eliminated due to the improved FFT

resolution, and the average offset was found to be 23.3 Hz. The same process was repeated for increased pulse widths, and the offset remained negligible. Although the exact reason was not determined, the general conclusion was that the DDC process in the DTA-2300 had an offset that varied with the PW. For PW greater than 5 μs, the offset is negligible. However, for smaller PW, the difference can be in the order of hundreds of Hz.

Next, the time delay implemented to produce the effect of down-range targets was examined. The output also had a step like pattern, where each step corresponded to the smallest time delay possible (*ie*. a single sample count). Unlike the frequency results, the delay results matched more closely with the desired profile. However, it was found that the decimation rate impacted the accuracy of the delay resolution due to the method the time delay was being implemented. Specifically, since received samples were used to measure time, the decimation influenced the clock resolution. For example, when decimation by 2 was used, the time resolution was 0.0625 μs, compared to decimation by 32, where the resolution was 1 μs. Figure 5.6 compares the measured delay for the outputted jamming pulses for decimation by 2 and 32.



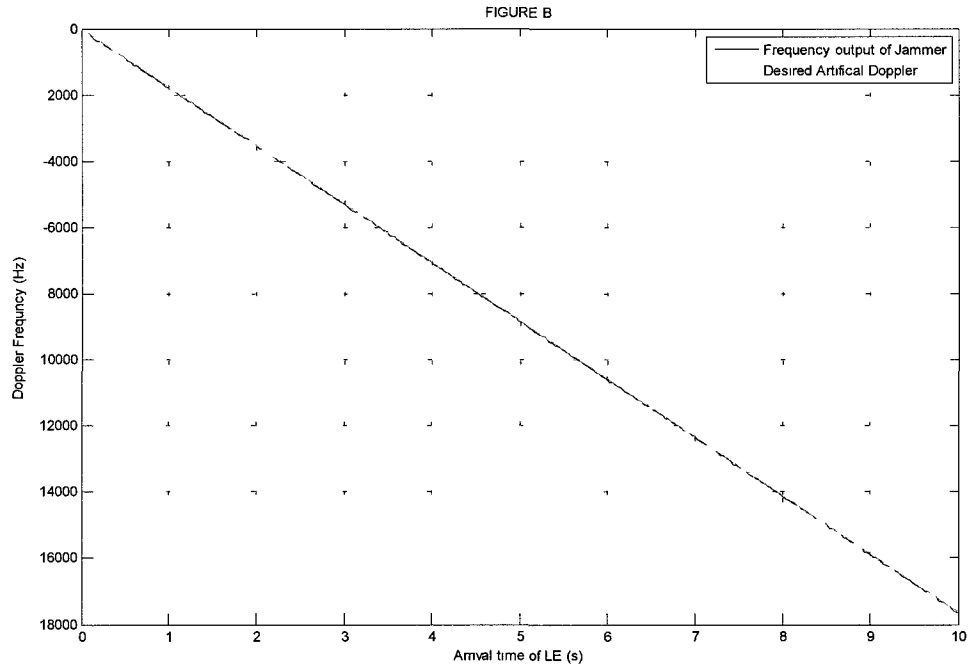
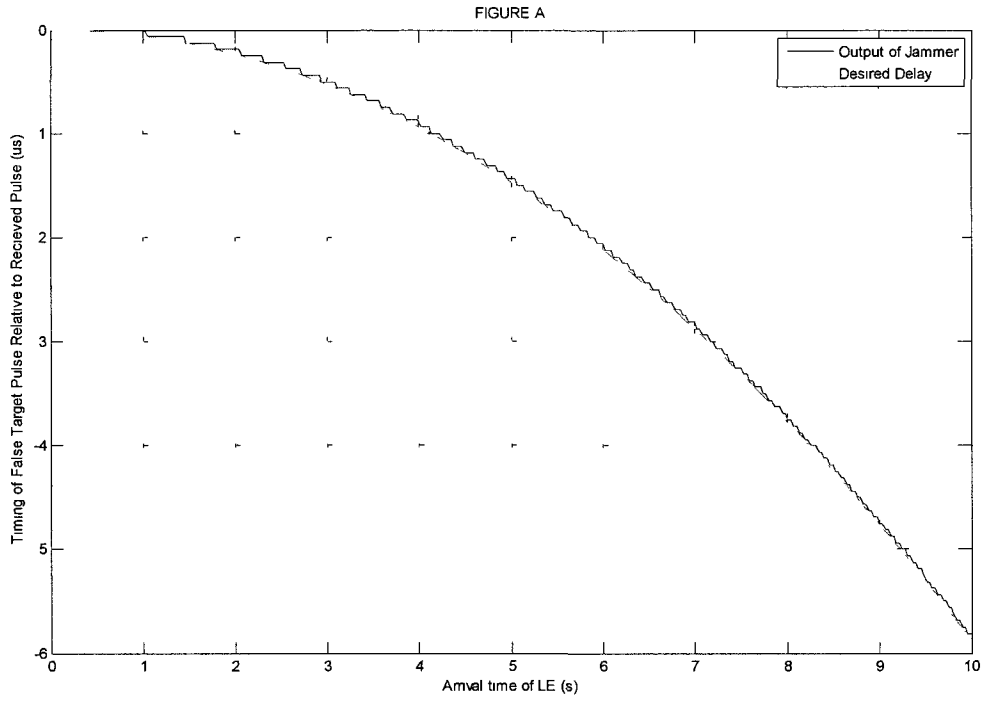


Figure 5.5 a & b: Frequency output of jammer applying profile 3 against 5μs fire control radar without additional noise, using data decimation by 2, 65k point FFT (figure a) and 524k point FFT (figure b)



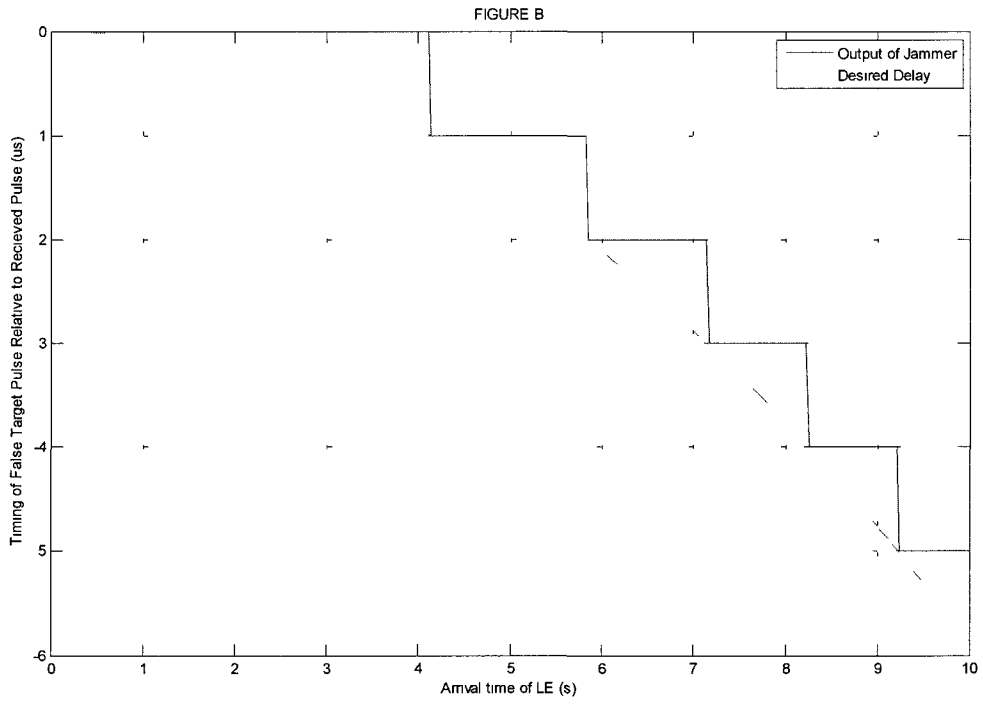


Figure 5.6 a & b: Time delay output of jammer applying profile 3 against fire control radar for decimation by 2 and 32

5.3.2 Radar Signal with 10 dB SNR

The same results were examined when noise was added to the radar signal such that the SNR was 10 dB at the processing stage. The addition of noise to the input radar pulses caused some profound differences between the desired and produced Doppler values, in part due to the way the analog radar pulse train was generated. On the other hand, the timing delays appeared not to be influenced by the additional noise in the signal. The results for decimation by 2 are given below, while Appendix C contains additional results for decimation by 4, 8, and 16.

Figure 5.7a compares the measured frequency of the modulated baseband signal with the desired artificial Doppler shifts. While the slope of lines agreed, the jammer output was periodic and had large fluctuations in produced Doppler. The periodic nature of the graph is due to a fixed number of radar pulses in a file being repeatedly looped through the DTA-2300 DAC. In this case, 7 pulses were looped to make the continuous pulse train, which matches the periodicity of the produced frequency. To confirm this hypothesis, the periodicity should be eliminated if a multiple of every 7^{th} pulse is examined. For example, in Figure 5.7b the frequency output of every 1015^{th} pulse is plotted. As expected, the periodicity no longer exists, and the plot appears similar to the results from the radar signal without noise (Figure 5.3a), with the offset caused by the small radar pulse width.

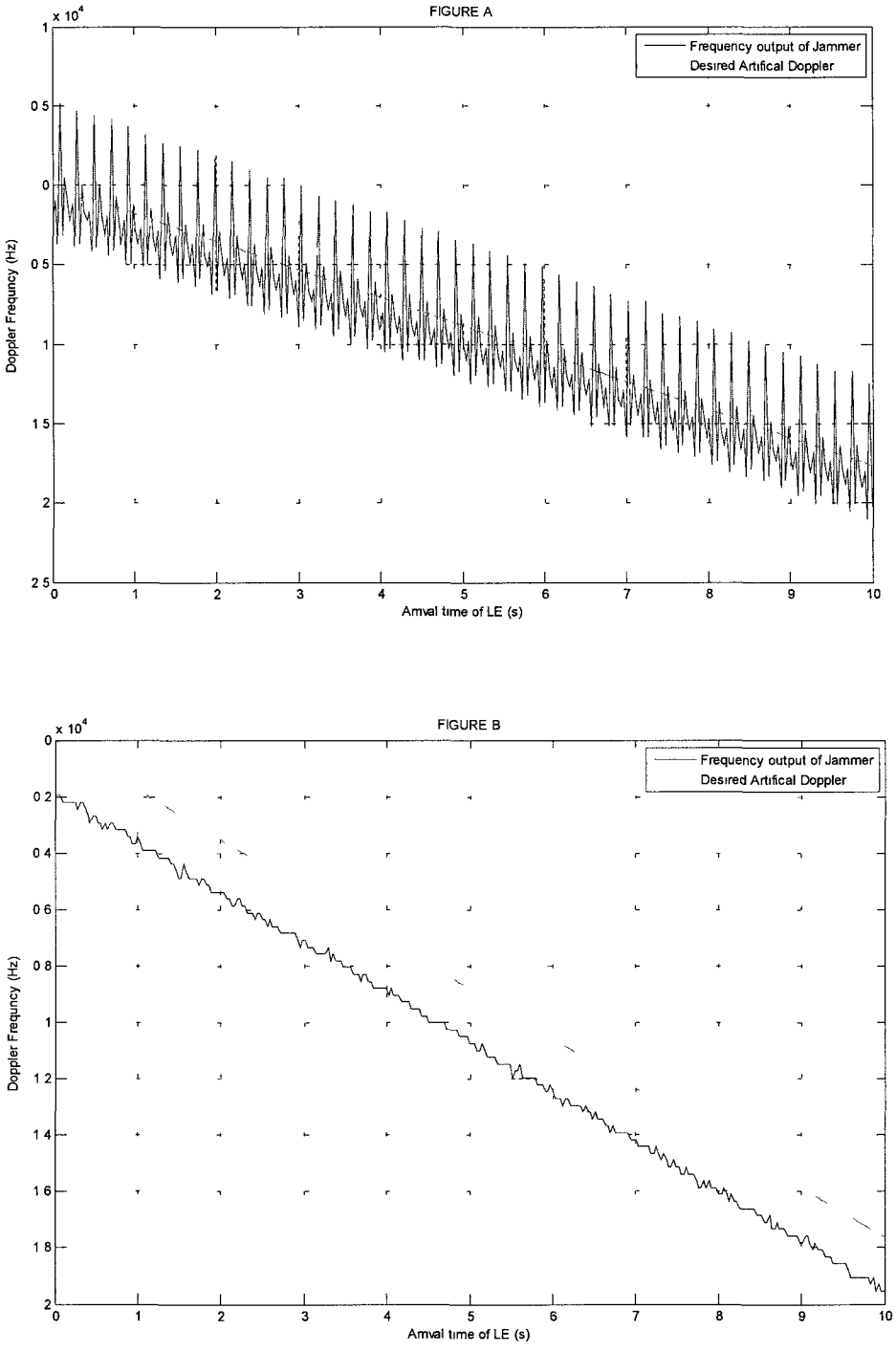


Figure 5.7 a & b: Frequency output of jammer applying profile 3 against fire control radar with 10 dB SNR, data decimation by 2

Referring back to Figure 5.7a, the large fluctuations seen in the Doppler are unexplained since earlier results indicated a relatively constant offset. To understand the cause, the input baseband I_r and Q_r data, prior to any Doppler modulations, were analyzed. It was again found that input baseband to the jammer did not have a spectral maximum at 0 Hz. However, rather than having a relatively constant error in the pulse train, each pulse was offset by a different amount, as shown in Table 5.2.

Pulse from file	Measured baseband spectral peak of input radar data (Hz)
1	-1,801
2	-702
3	-3,510
4	5,310
5	-3,052
6	702
7	-1,312

Table 5.2: Baseband frequency offset for raw radar data used to make the continuous pulse train for the fire control radar

The reason each pulse was offset by a different amount was that when adding noise in Matlab, the generated signal was not always at maximum amplitude at the desired frequency. Instead, in most cases, it was within ±2 adjacent peaks of the desired IF. As an example, for the same radar PW, PRI, and SNR, the generated IF Matlab spectrum is shown in Figure 5.8. It can be seen that the peak of the signal is not at the desired IF of 25 MHz. Instead, the peak was measured at 25.0333 MHz. This difference of 33.3 kHz, which remains constant as the spectrum is down converted to baseband, is significant when considering the precision required for the applied Doppler. With the

addition of noise, each radar pulse from the pulse train may have its spectral peak at a different point, which accounts for the fluctuations seen at baseband.

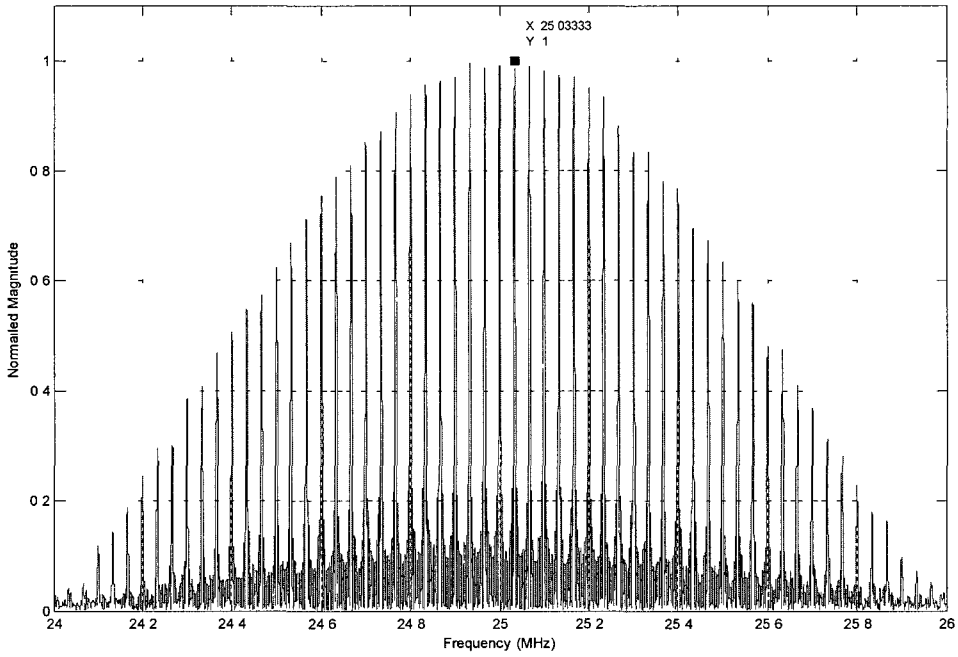


Figure 5.8: Generated IF signal with a 10 dB SNR

To confirm if the baseband offset was indeed responsible for the Doppler fluctuation, the results for the first 7 output pulses from the jammer were compared to the measured baseband frequency. In Table 5.3, columns D and E are the desired and measured Doppler modulations. Column F can be considered the expected offset, and was obtained from Table 5.2. Therefore, the relative Doppler modulation indicated in column G is the difference of columns E and F. The error in column H is the difference between the expected and measured Doppler. The average error was found to be less than 73 Hz. Plotting the relative produced Doppler versus the desired artificial Doppler over the complete jamming time, as shown in Figure 5.9, it can be seen that both the

fluctuation and offset have been eliminated. The critical conclusion is that the Doppler modulations are being applied correctly relative to the measured frequency of the input pulse.

	A	B	C	D	E	F	G	H
Pulse received at Jammer	Pulse from file	Sample Count at Leading Edge	Pulse Arrival Time (ms)	Desired Baseband Doppler Modulation (Hz)	Measured Baseband Doppler Moduation (Hz)	Expected Offset (Hz)	Relative Produced Doppler (Hz) E-F	Error (Hz) G-D
1	1	186	0 012	0	-1801	-1,801	0	0
1001	7	480186	30 012	-53	-885	-702	-183	-130
2001	6	960186	60 012	-106	-3693	-3,510	-183	-77
3001	5	1440186	90 012	-159	5157	5,310	-153	6
4001	4	1920186	120 012	-212	-3143	-3,052	-92	120
5001	3	2400186	150 012	-265	427	702	-275	-10
6001	2	2880186	180 012	-317	-1465	-1,312	-153	165

Table 5.3: Frequency offset for each of the pulses looped to produce the pulse train

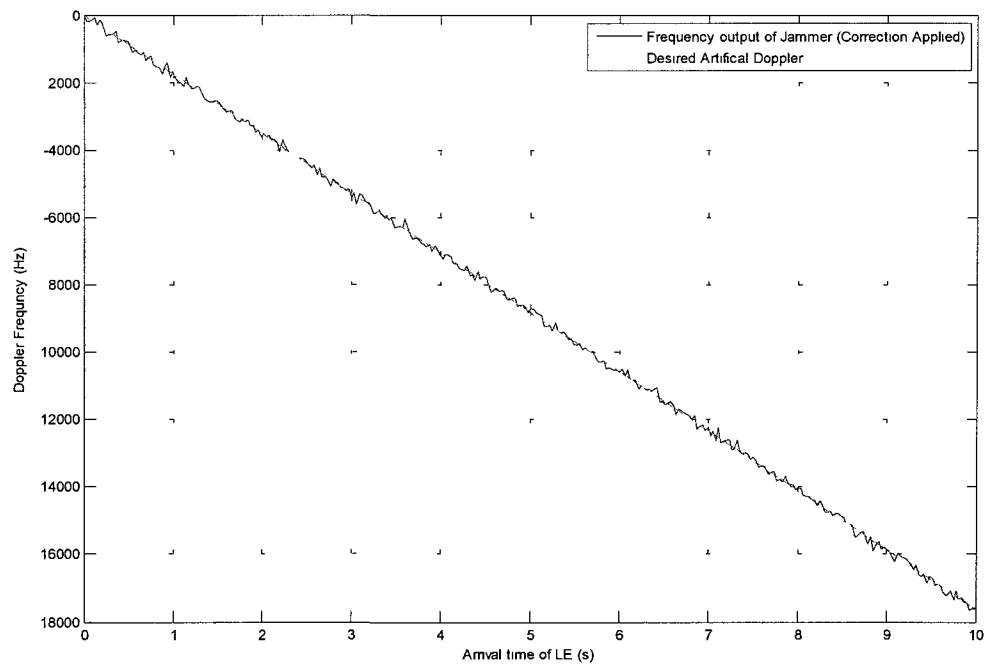


Figure 5.9: Frequency output of jammer applying profile 3 against fire control radar with 10 dB SNR, data decimation by 2, individual pulse correction applied

In terms of the time delay, the addition of noise to the signal did not impact the results. The discrete time delays produced by the jammer for a noisy signal are included in Appendix C.

5.4 Surveillance Radar

Profile 4, shown previously in Figure 3.9, was applied to surveillance radar waveform with an SNR of 10 dB. Unlike the CRV technique examined in the last section, profile 4 required prior knowledge of the PRI since up-range false targets were desired. A positive Doppler shift was applied in order to synchronize the range pull with the apparent velocity of the false target. Since the surveillance radar signal was frequency modulated (linear FM chirp), another consideration was that the Doppler modulation could not simply be obtained by finding the spectral peak. Instead, a constant reference point was required. In this case, since the first radar pulse had effectively no modulation applied to it (*ie*. the spectrum of the first radar pulse was the same as the first jammer pulse), the first jammer pulse was used as the reference point. Subsequent jammer pulses were compared against this reference to measure the applied Doppler modulation. Figure 5.10 shows the spectrum of the reference jammer pulse. Specifically, the right sided maximum marked by the arrow and red 'x' was used as the reference point. The results were collected every 3000th pulse for a 10 second jamming cycle, and are shown in Table 5.4.

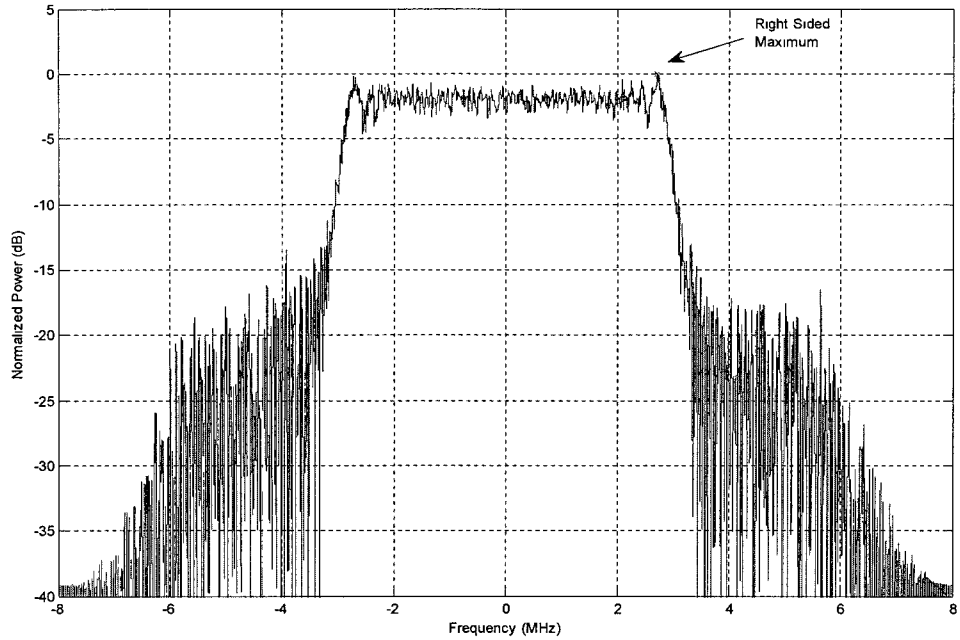


Figure 5.10: Baseband spectrum of surveillance radar

	A	B	C	D	E	F
Pulse received at Jammer	Sample Count at Leading Edge	Pulse Arrival Time (s)	Desired Baseband Doppler Modulation (Hz)	Frequency of reference point (MHz)	Measured Baseband Doppler Modulation (Hz)	Offset (Hz)
1	1,146	0.000072	0	2.695374*	0	0
3001	14,393,946	0.899622	480	2.695892	519	39
6001	28,789,146	1.799322	960	2.696350	977	17
9001	43,181,946	2.698872	1439	2.696838	1465	25
12001	57,577,146	3.598572	1919	2.697296	1923	3
15001	71,969,946	4.498122	2399	2.697815	2441	42
18001	86,365,146	5.397822	2879	2.698273	2899	20
21001	100,757,946	6.297372	3359	2.698730	3357	-2
24001	115,153,146	7.197072	3838	2.699219	3845	7
27001	129,545,946	8.096622	4318	2.699707	4333	15
30001	143,938,746	8.996172	4798	2.700195	4822	24
33001	158,333,946	9.895872	5278	2.700653	5280	2

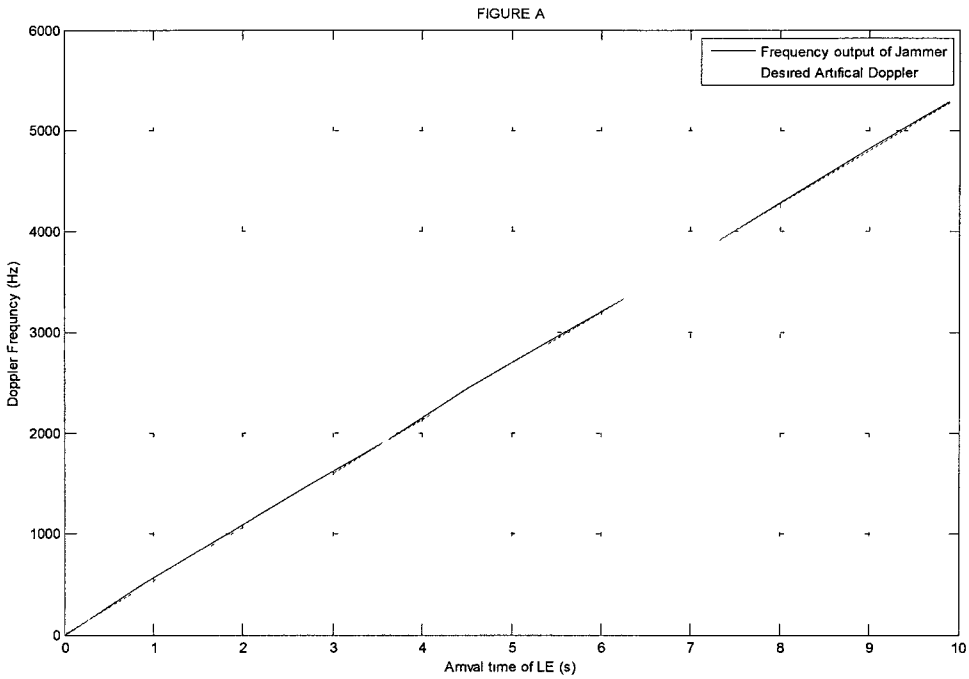
* denotes the reference point used for measured Doppler calculations

Table 5.4: Jamming results for applying profile 4 against surveillance radar

As seen from Table 5.4, the desired and produced baseband modulations are within 42 Hz, with an average absolute offset calculated to be less than 17 Hz. The Doppler and time results are plotted in Figure 5.11.

Compared to the results from the CRV pull-off on the fire control radar, there are two different observations. First, note that a frequency offset is not significant. This meant that the down conversion process was centering the data at 0 Hz, and supports the earlier conclusion that an offset is not present for longer pulse widths. Second, there is an absence of fluctuations in the Doppler profile, as compared to Figure 5.7. This is explained by the fact that this signal was generated by looping a single pulse, and so the exact same radar pulse data was modulated for each output pulse from the jammer.

The same results were examined for higher decimation values. One important observation was that when decimation values were applied for the 10 dB SNR surveillance radar, the pulse detection scheme had to be more carefully considered. It was found that the signal power during the rising and falling edges tended to fluctuate, causing inaccurate leading and trailing edge detections. For example, with decimation by 4, the input radar pulse power is shown in Figure 5.12. The simplest method of correction was to adjust the detection threshold power level below these fluctuations. Alternately, a counter to search for a minimum number of consecutive points required above and below a threshold to signify the leading and trailing edges could also be implemented.



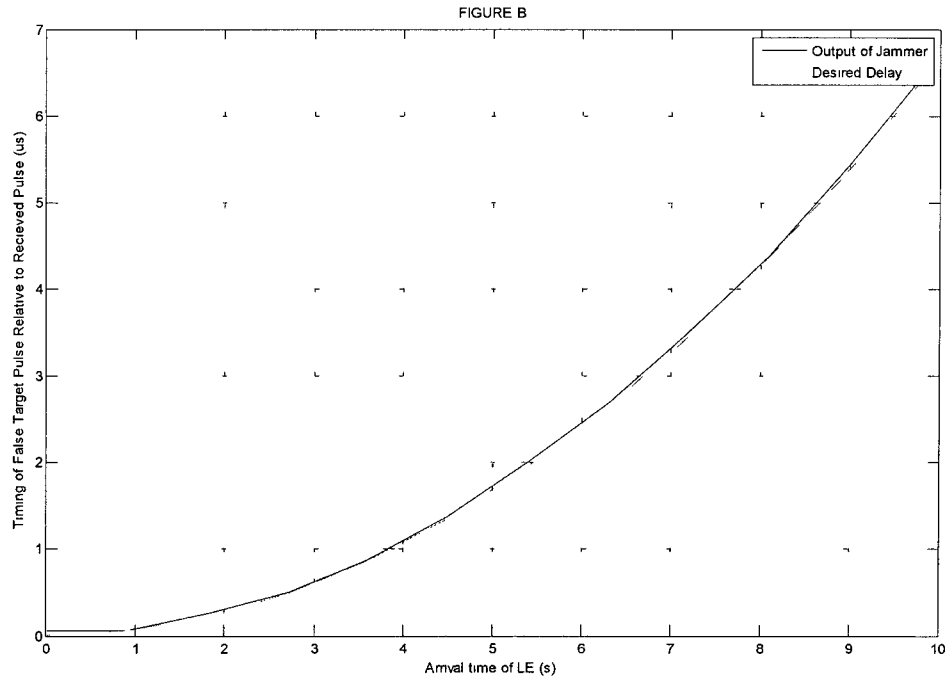


Figure 5.11 a & b: Frequency and time delay output of jammer applying profile 4 against surveillance radar with 10 dB SNR, data decimation by 2

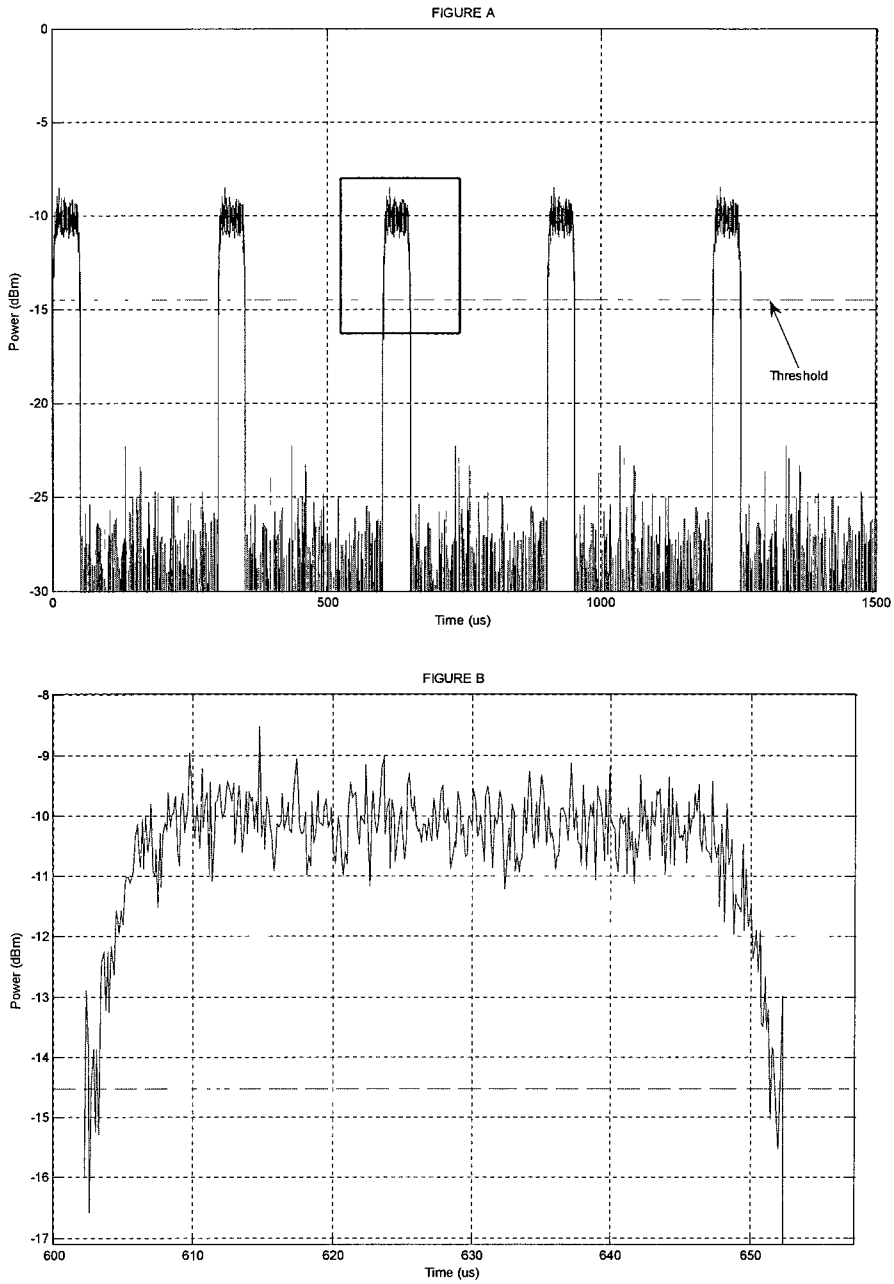


Figure 5.12 a & b: Signal power measurement for decimation by 4 illustrating power fluctuations during the leading and trailing edges (figure a) and close-up (figure b)

Since the bandwidth of the surveillance radar was 6 MHz, the sampling rate needed to be a minimum of 12 Msps. Therefore, only decimation by 2 and 4 met this requirement and yielded accurate results. These plots are shown in Appendix D.

5.5 Throughput Calculations

An important jammer specification is the throughput delay, which is essentially a measurement of the processing speed of the jammer. For example, assuming that no intentional time delay is applied, the throughput can be measured by finding the time it takes to process the radar pulse. This time will also correspond to a fixed distance between the true echo return and the transmitted jammer pulse. Jammer designers seek to minimize throughput time since it results in an unwanted delay of the transmitted false target. In this thesis, since RF up or down conversion was not considered, the throughput time delay was calculated between the signal input to the ADC and the time the processed jammer data was available for up conversion, represented as points A through D in Figure 5.13.

The time between points A and B was expected to be the sampling period of the ADC. However, since a DDC was performed and header information was being added between the data, there was a chance that the sampled output from the DTA-2300 was slower than the ADC sampling rate. To confirm if the packetized output matched the sampling rate, the fine time stamp built into the header was extracted. The fine time stamp has a resolution of 6.4 ns. The time between consecutive packets, averaged over 1000 packets, was then found for all possible decimation rates. Measured and expected results are shown in Table 5.5, column A. For example, with decimation by 2, the time between consecutive packets ranged from 895.987 to 896.064 μs, and averaged to 895.995 μs. Since there were 4096 x 7 samples per packet and the sampling rate was 32 MHz, the expected time between packets was 896.000 μs. The difference of -0.005 μs is

unexpected, but may be explained by a closer examination of the relationship between the time stamp and buffering process at the output of the ADC. Regardless, since these values closely agreed for all decimation rates, it was concluded that no noticeable delay is introduced by including the D-TA header in the sampled data.

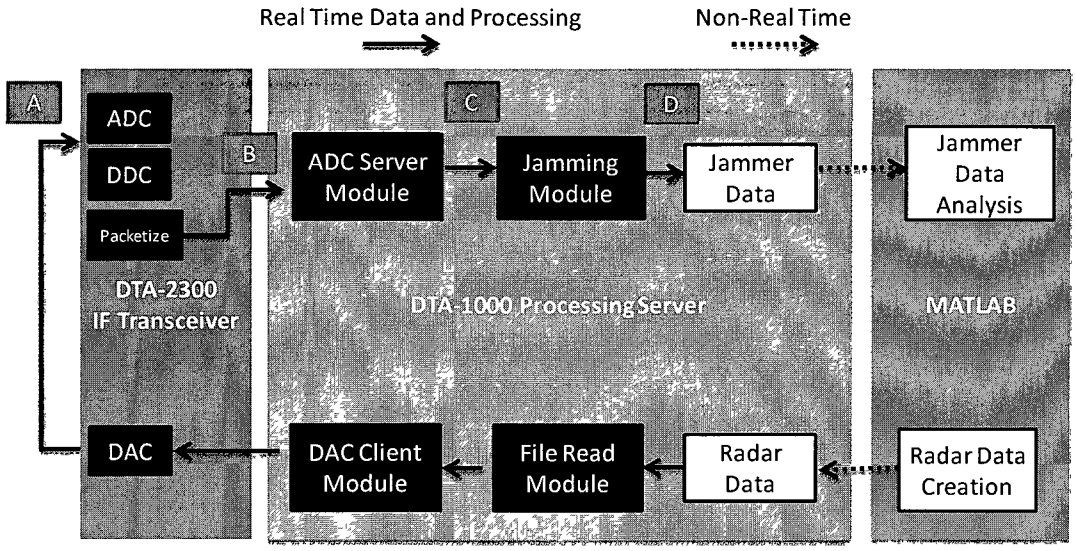


Figure 5.13: Throughput time measurement locations

Between points B and C, the sampled data is read by the ADC Server Module and sent to a ring buffer. Recall from section 4.3.1, data cannot be written and read concurrently from the same block within the ring buffer. In other words, a block must be completely full before any processing can be done on that data. The time required to fill a block of data can be theoretically calculated knowing the block size, sampling rate, decimation, and ring buffer size. If the default buffer of 640 MB is used, each block is 128 MB, and the delay time is calculated by equation (5.1). F_s represents the ADC sampling rate and the D is the decimation factor in the DDC. This equation was used to obtain the expected values in Table 5.5, column B.

$$Time_{BC} = 128MB \cdot \frac{(1024)^2 bytes}{MB} \cdot \frac{samples}{4bytes} \cdot \frac{seconds}{F_s / D\ samples} \tag{5.1}$$

To actually measure this time, an existing C++ 'gettimeofday' function was used [7]. Using this function on the DTA-1000, software running time could be measured with millisecond resolution. Start and stop time point measurements were inserted into the ADC server module between successive blocks. These are shown as measured results in Table 5.5, column B. It was again noticed that the measured times were less than the estimated calculations.

	Column A - Sampling Times		Column B - ADC Server Module	
Decimation	Measured time/packet from A to B (μs)	Expected time/packet from A to B (μs)	Measured processing time from B to C (ms)	Expected processing time from B to C (ms)
2	895.995	896.000	2095	2097
4	1791.970	1792.000	4189	4194
8	3583.960	3584.000	8380	8389
16	7197.920	7168.000	16759	16777
32	14335.800	14336.000	33518	33554

Table 5.5: Measured and expected times between ADC sampling (point A) and output of ADC Server Module (point C)

Next, the same 'gettimeofday' function was used to measure the processing time within the Jamming Module. Considering that data was being passed to the Jamming Module in full blocks, it made sense to measure the processing time for all the samples in that block of data. In order to consider the worst case scenario, the throughput time was measured during the fourth stage of the jamming (refer to 4.3.2), where the greatest processing demands were placed on the Jamming Module. Intuitively, the processing time between C and D is a function of the input radar PW and PRI, as well as profile

indexing method. The greater the PW, the more times the Doppler algorithm is applied, meaning increased processing time. Conversely, a greater PRI means fewer indexing operations are required. For the three jamming techniques used, the time was measured between processing of the first and 2339th packet of data, just before a new block of data was processed. The results are shown Table 5.6, where the shaded blocks represent cases where the effective sampling rate did not satisfy the Nyquist sampling criteria. Note that to find the throughput per sample, the times listed in Table 5.6 should be divided by the number of samples per block. Therefore, the worst case throughput time per sample was calculated to be 0.04 μs / sample.

	Measured processing time from C and D (ms)		
Decimation	Noise Masking vs EW Radar	Profile 3 vs Fire Control Radar	Profile 4 vs Surveillance Radar
2	682	826	1449
4	646	769	1353
8	625	761	
16	620	754	
32	608		

Table 5.6: Jamming Module throughput times per block of data for implemented radar versus jammer scenarios

As expected, the greatest processing time was needed for the surveillance radar. It can also be seen that processing times varied with decimation, since higher decimation values had fewer points to process over a PW. Note that since the Jamming Module operates concurrently with the ADC Server Module, the actual throughput time of the present implementation is given by the measured processing time in column B of Table 5.5.

To make good use of this information, calculations can be made to reduce throughput times. Ideally, the software processing times in both modules should be the same so that neither module waits on the other. In this case, since the processing time in the ADC Server module is greater than the Jamming Module, the Jamming Module is idle between the time the last packet is processed and the next block of data is received. Theoretically, this also implies that the jamming technique time can be indefinitely increased without dropped data by the Jamming Module. An immediate improvement can be made by selecting a higher sampling rate. As a preliminary calculations using equation (5.1), setting the $Time_{BC}$ to equal the processing times in Table 5.6, will indicate how much the sample rate can be increased without any adverse effects on the Jamming Module. For example, when the surveillance radar is used with a decimation by 2, the sampling rate can be increased from 32 Msps to approximately 48 Msps to match processing times for the ADC Server and Jamming Module. Consequently, the throughput in the ADC Server will be reduced from 2097 ms to approximately 1397 ms, a reduction of about 33%. A second option to improve throughput would be to decrease the size of the block size from the default 128 MB. For example, if the block size was reduced by a factor of 10, the time to fill the block should be reduced by the proportional amount. Further investigation of reducing software throughput times is left as future work.

A general conclusion can also be made regarding design principle. In this thesis, since the maximum radar bandwidth was known, the jammer was purposefully designed to operate at the lowest sampling rate possible in order to give the software as much time

as possible to process the real time data. However, after the throughput times were measured, it was realized that the Jamming Module software processing speed was adequate. In fact, the largest delay was due to the buffering of the data between the ADC Server, causing at least an undesired 2096 ms lag. In retrospect, had this limitation been anticipated, it would have been better to design the jammer at the highest possible sampling speed so that the ADC Server buffering time would be reduced. A higher sampling speed would also allow the jammer to function against higher bandwidth radar waveforms and make use of the various decimation levels in the DDC to slow the data rate as needed. In the current implementation, although results were collected for different decimation rates, there is no requirement to use a decimation rate greater than two since the Jamming Module software is always waiting on the sampled data.

5.6 Summary

The results obtained in this chapter validated the output of the jamming software. For noise masking, the created jamming pulse data was shown to have the correct noise bandwidth and size, and timed to overlap the subsequent anticipated radar pulse. For the two CRV profiles investigated, it was found that the radar PW and SNR influenced the artificial Doppler modulations. For the 1 μs PW fire control radar, the DDC process was found to have a frequency offset from baseband, which was not observed for PW of 5 μs or greater. When the signal had an SNR of 10 dB, the baseband spectrum was found to have an offset that varied pulse to pulse. Despite these concerns, the jammer pulses were shown to have the correct artificial Doppler relative to the frequency of the input pulse, and thus validated the baseband algorithm. Provided the Nyquist sampling criteria was

met, the algorithm worked for signals with SNR of 10 dB or higher for all decimations. The desired time delays/advances from the jammer were also found to be accurate, regardless of radar SNR. On the other hand, after investigating the throughput times, it was obvious the outputted jammer pulse would have a much larger fixed delay. Improvement on the throughput can be made by increasing the ADC sampling rate and reducing the size of the buffer.

Chapter 6

Conclusion

6.1 Summary of Work

The main objective of thesis was to investigate the hardware and software architecture required for a single channel, software based laboratory jammer. The project was meant to address the common restrictions and limitations found in commercially available laboratory DRFM systems. Before this goal could be achieved, a detailed study of three classes of modern radar systems and DRFM jammers was completed to gain an understanding of their operations. A general scenario involving a self-screening aircraft encountering an early warning, surveillance, and fire control radar systems was considered. Disruptive and deceptive jamming techniques were reviewed and resulted in the creation of jamming profiles for RGPO, VPGO and CRV pull-offs techniques and noise masking. Without having access to various radar systems, Matlab was also used to create artificial radar signals of interest that replicated the typical PWs and PRIs expected, and in the case of the surveillance radar, also an intra-pulse linear frequency modulation. Simulations were done to learn how the jamming could be applied to the radar signals, and also served to identify some challenges associated with implementation and real time data processing.

The implementation of the software jammer was carried out using a commercial hardware system from D-TA Systems. Specifically, the DTA-2300 IF Transceiver was used to digitize and down convert the radar signals, and the DTA-1000 Processing Server

contained the C++ based software required for signal processing. A customized Jamming Module was created and integrated into the D-TA software architecture. This module performed all jamming functions such as allowing for the selection of jamming technique, input signal peak power measurements, and leading and trailing pulse edge measurements based on threshold detection. Doppler modulations were applied at baseband, allowing for a fixed RF up and down conversion process. Down-range false targets were realized by holding the modulated data a suitable number of samples before transmission. In a similar manner, since the radar PRI was known, up-range false targets were possible. Real time results were collected, analyzed, and discussed. Lastly, the throughput time of the jammer was measured at different stages to give an indication of the speed of the implemented jammer.

6.2 Contribution

Unlike commercially available laboratory jammers, the developed solution gives unprecedented flexibility and control to the user. The Jamming Module software is written in C++, and is easily accessed and modified. It is also designed as a modular system to allow for the introduction of new and more advanced jamming techniques, as well as expansion into a multi-channel system. In its current state, the jammer is able to apply deceptive jamming profiles and a disruptive spot noise technique.

Another unique aspect of this project is the manner in which artificial Doppler is applied. As suggested in [21], the baseband application of Doppler eliminates the

requirement for a variable LO during up and down conversion. The baseband algorithm was shown to be effective in all tested scenarios.

Arguably, the greatest strength of the jammer is the flexibility to adapt and adjust both the input radar signal and the jamming parameters. In terms of an input radar signal, the user is free to use available radar data or create artificial signals in Matlab. Using the latter option, the radar signal parameters such as PW, PRI, power, SNR, and intra-pulse modulation can be changed. In terms of the jamming parameters, any combination of the jamming technique can be tested against any input radar. Changes to the jamming parameters, such as technique time, pull-off distances and velocities, and direction of pull-offs, can also easily be made. Although there are some noted limitations, as described in the next section, the newly created jamming software is a stepping point for further development.

6.3 Noted Limitations and Future Work

Despite best efforts, there are some limitations of the jammer developed in this thesis. The first limitation is that the signal up conversion to IF is not possible in the present architecture. This is due to the fact that the DAC chip in the DTA-2300 is already tasked with the production of the input radar signal. For this reason, the output of the jammer was analyzed as baseband data, rather than an up converted analog jammer waveform. Unless other means of producing the input radar signal is available, the absence of an IF up conversion mechanism is the single greatest deficiency with the current jammer. One option for implementing real time IF up conversion is to send the

output jammer data to a second channel on the DTA-2300. In doing so, the additional DAC resource could be used to produce the analog IF jammer signal. A full RF up conversion process could then also be implemented using other D-TA hardware, namely the DTA-3200.

Second, the throughput delay through the existing system is much too long for any practical jammer. The main reasons for the long delay were the intentional under-sampling of the input radar signals and use of the default ring buffer size of 128 MB in the ADC Server Module. To improve this, the ADC sampling rate should be increased to the maximum rate allowed by the hardware. This would also increase the jammer bandwidth, allowing it to handle shorter radar pulses and greater frequency chirp ranges. Additionally, the ring buffer used by the ADC Server should be reduced from its default size until a satisfactory throughput time is achieved or another limitation is discovered.

Next, the jammer developed for this thesis was limited to a four deceptive jamming techniques and one disruptive jamming technique. This existing foundation of work has potential to be expanded upon. Specifically, more work can be done to produce different types of primary targets. For example, the ability to transmit revered and time segmented radar pulses, as shown in section 2.6.2 would be welcomed feature. In this thesis, profiling was limited to frequency and time. However, amplitude profiling would add yet another dimension of user control. Similarly, other types of jamming profiles, such as range and velocity bin masking and those that involve secondary targets, may also be considered.

Finally, another potential development is expansion into a multi-channel system. In doing so, the jammer would be able to produce overlaid targets, and thus greatly increase its abilities to exhaust radar processors. It is expected that as the processing demands are increased, the jammer software will need to migrate to a multithreaded architecture, where system threads can be run in parallel.

6.4 Final Remarks

Overall, the objectives of this thesis were met. Although a complete implementation of the jammer was not achieved, the idea of a software based jammer was shown to be a viable concept, and one that has tremendous potential for further improvement.

Appendix A – Oscilloscope and Spectrum Analyzer Plots

This appendix verifies the creation of the artificial radar signals as described in section 4.2.1. Figures A.1 to A.6 are oscilloscope plots of the three created radar signals, while Figures A.7 to A.10 show the spectrum analyzer outputs for the same radars. The SNR in all cases is 10 dB. Power was calculated from the measured peak-to-peak voltages. Note the comparison between these figures and the plots shown in section 3.3.

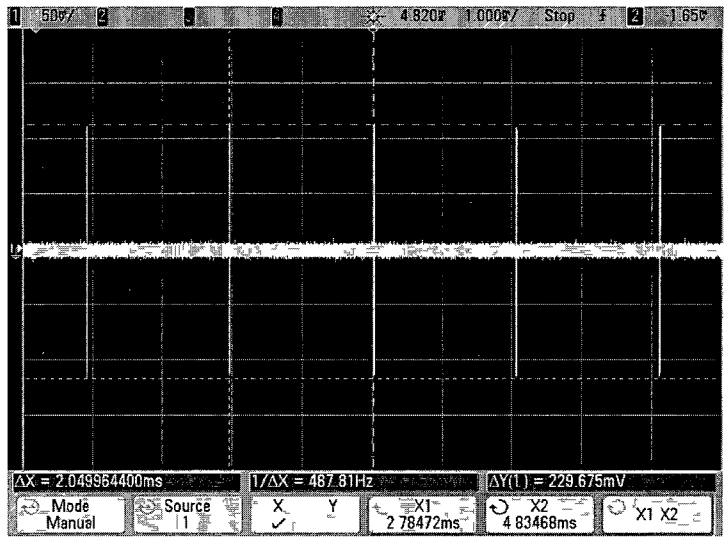


Figure A.1: Oscilloscope plot showing three pulses from simulated early warning radar with peak power of -8.81 dBm

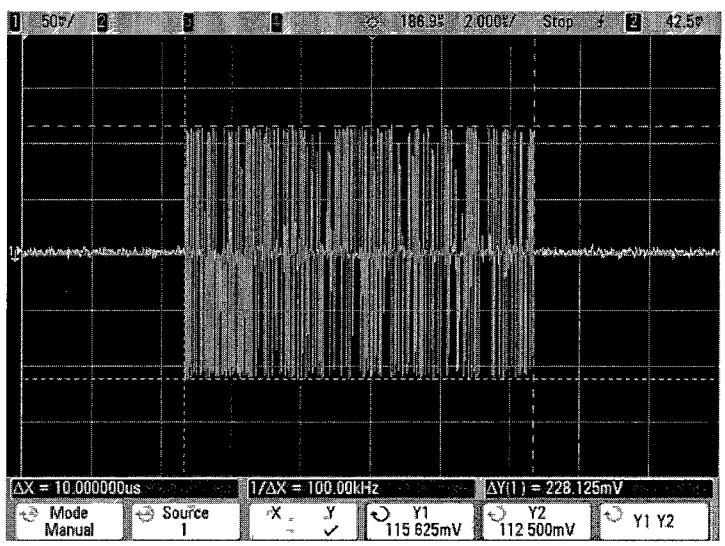


Figure A.2: Oscilloscope plot showing close-up of single pulse from simulated early warning radar with peak power of -8.81 dBm

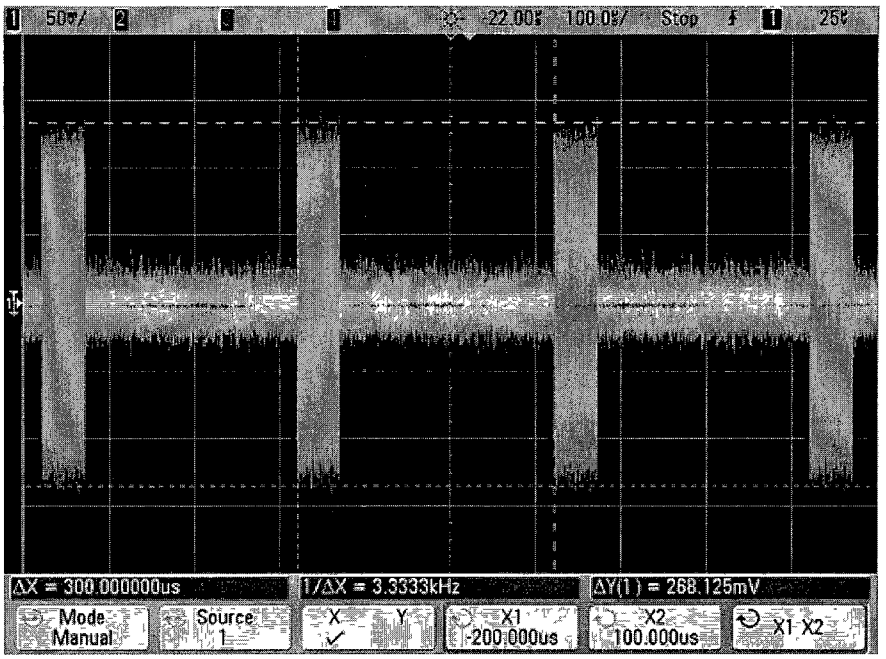


Figure A.3: Oscilloscope plot showing four pulses from simulated surveillance radar employing pulse compression with peak power of -7.45 dBm

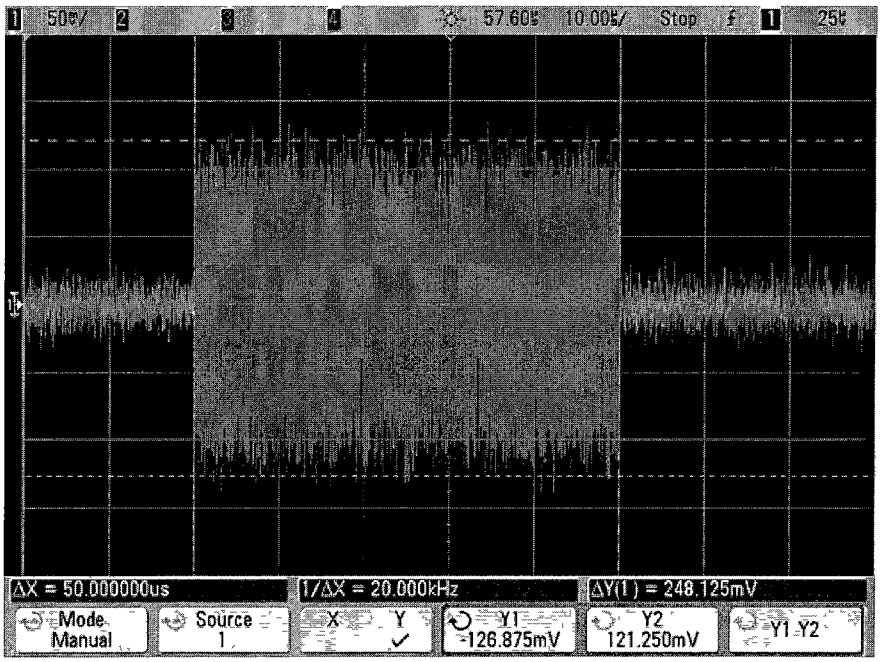


Figure A.4: Oscilloscope plot showing close-up of single pulse from simulated surveillance radar employing pulse compression with peak power of -7.45 dBm

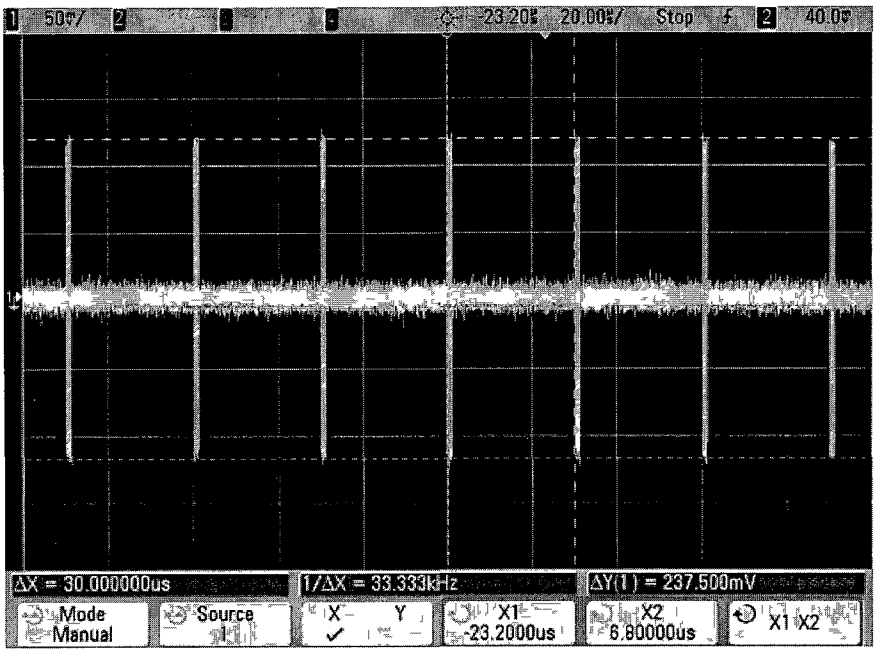


Figure A.5: Oscilloscope plot showing the pulse train from simulated fire control radar with peak power of -8.51 dBm

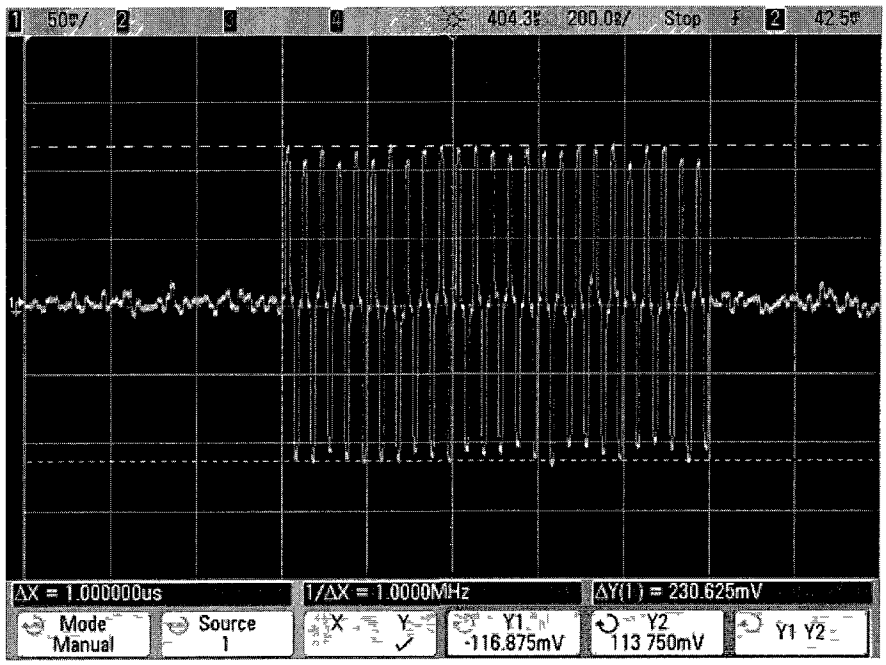


Figure A.6: Oscilloscope plot showing close-up of single pulse from simulated fire control radar with and peak power of -8.51 dBm

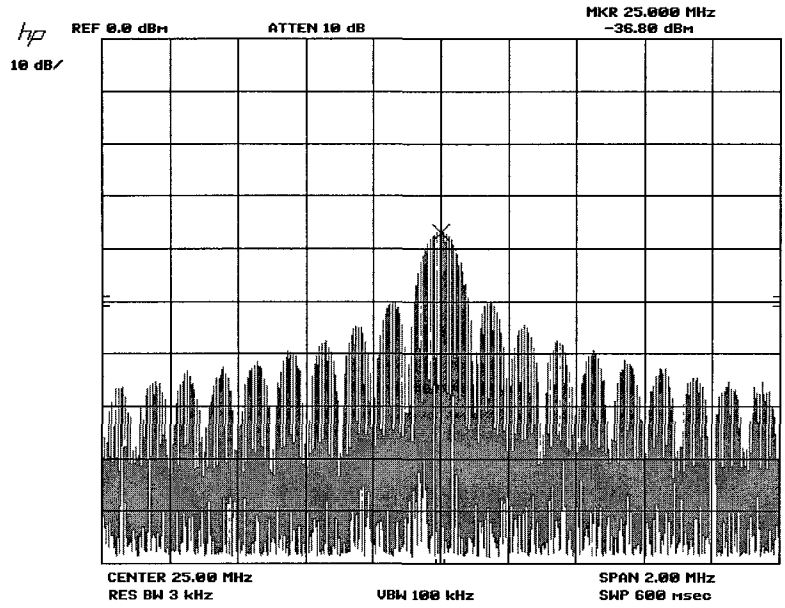


Figure A.7: Spectrum Analyzer plot showing the measured frequency spectrum of a simulated early warning radar

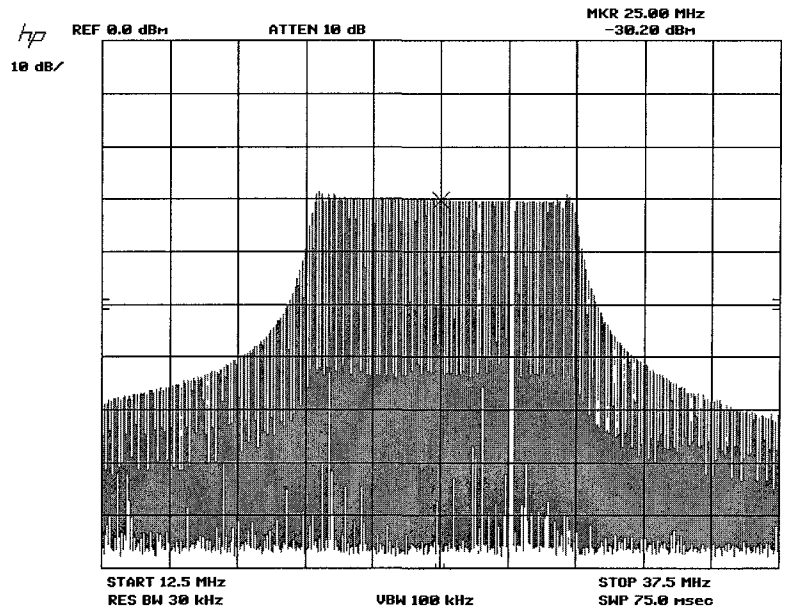


Figure A.8: Spectrum Analyzer plot showing the measured frequency spectrum of a simulated surveillance employing pulse compression

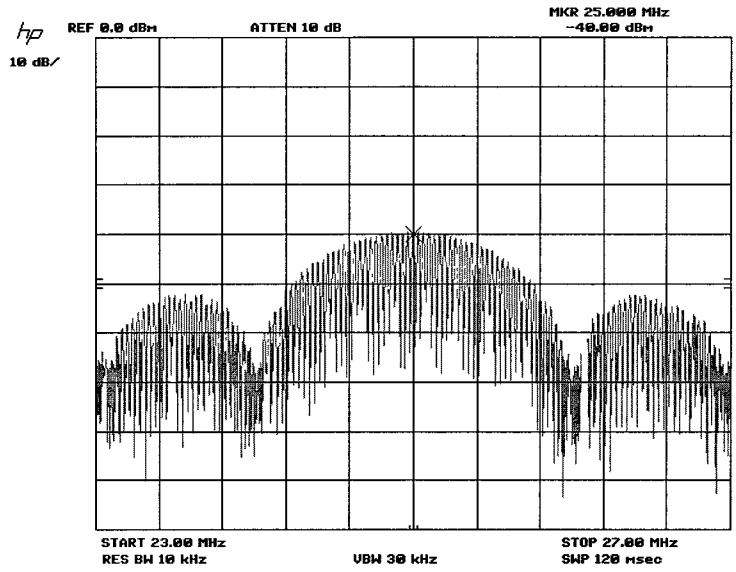


Figure A.9: Spectrum Analyzer plot showing the measured frequency spectrum of a simulated fire control radar

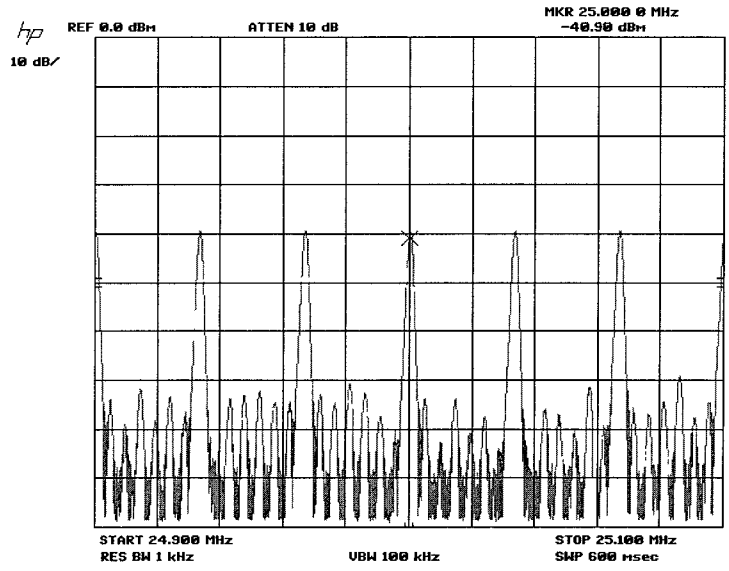
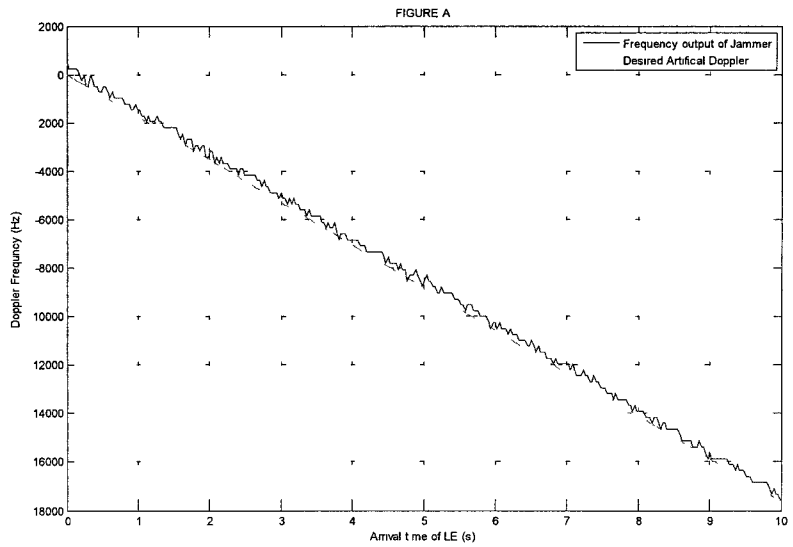


Figure A.10: Spectrum Analyzer plot showing a close-up of the measured individual spectral components from a simulated fire control radar

Appendix B – Results for Fire Control Radar Without Noise

The following figures show the frequency and time delay outputs of the jammer compared to the desired values obtained from the CRV profile 3. The input fire control radar signal was not corrupted by noise. As described in section 5.3.1, a frequency offset was observed due to the relatively small PW, with no apparent correlation between offset amount and decimation factor. Since the signal bandwidth was 2 MHz, decimation by 32 did not satisfy Nyquist sampling criteria.



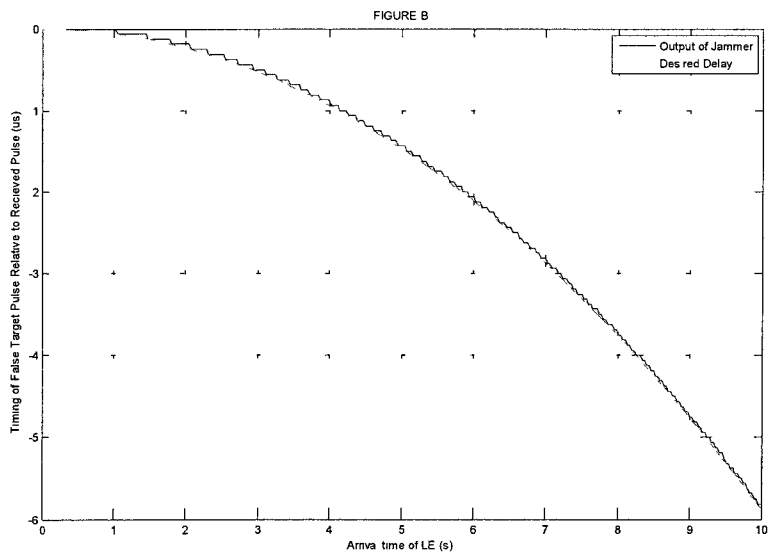
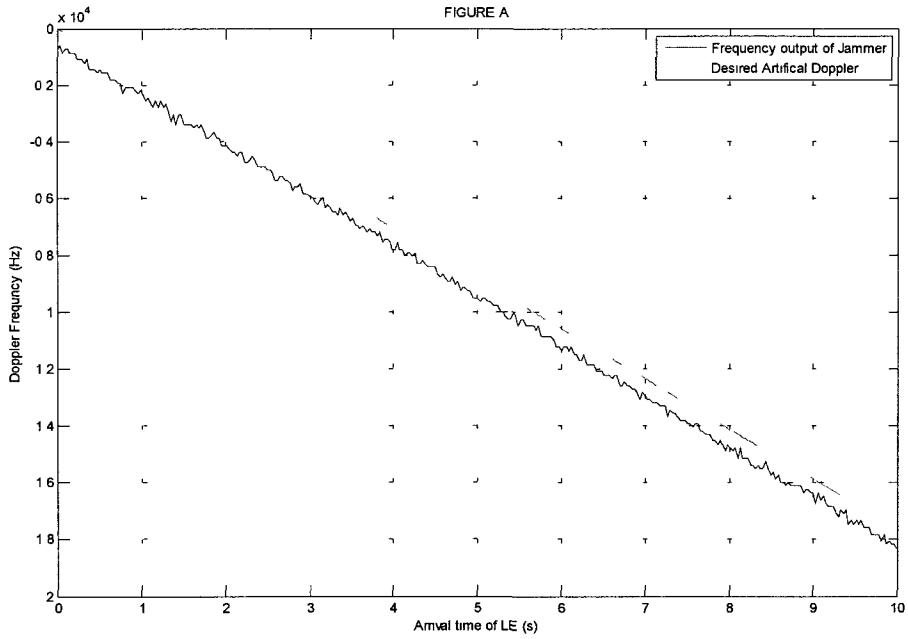


Figure B.1 a & b: Frequency and time delay output from jammer applying profile 3 against fire control radar without additional noise, data decimation by 2



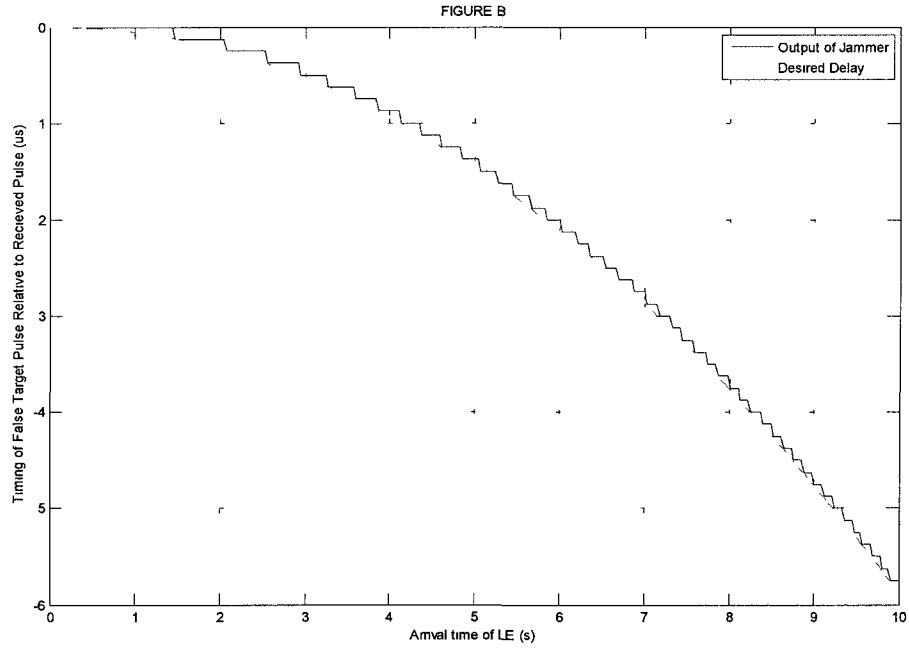
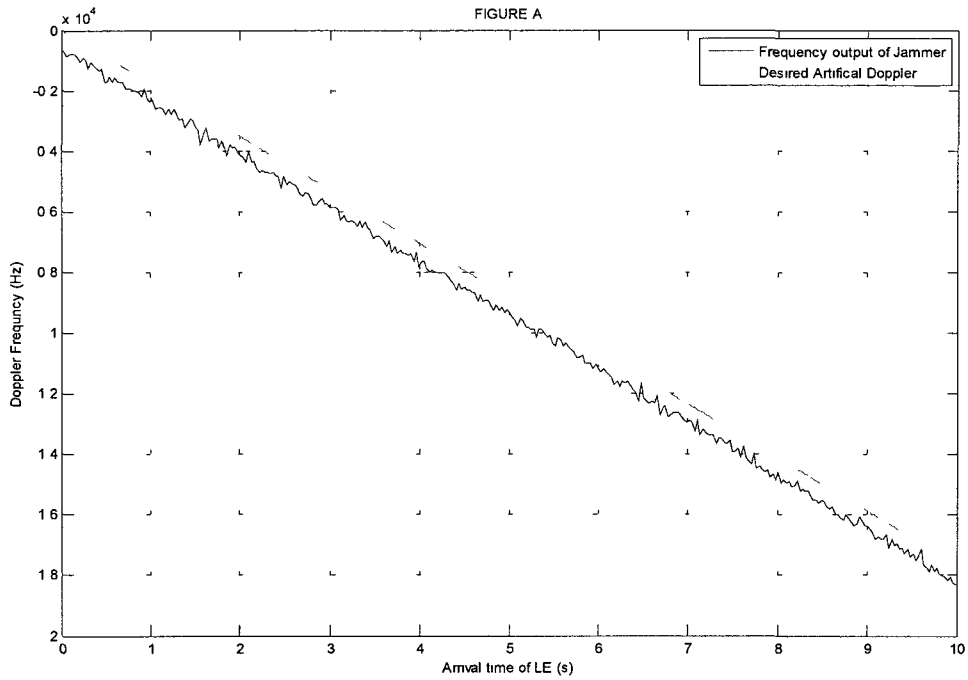


Figure B.2 a & b: Frequency and time delay output from jammer applying profile 3 against fire control radar without additional noise, data decimation by 4



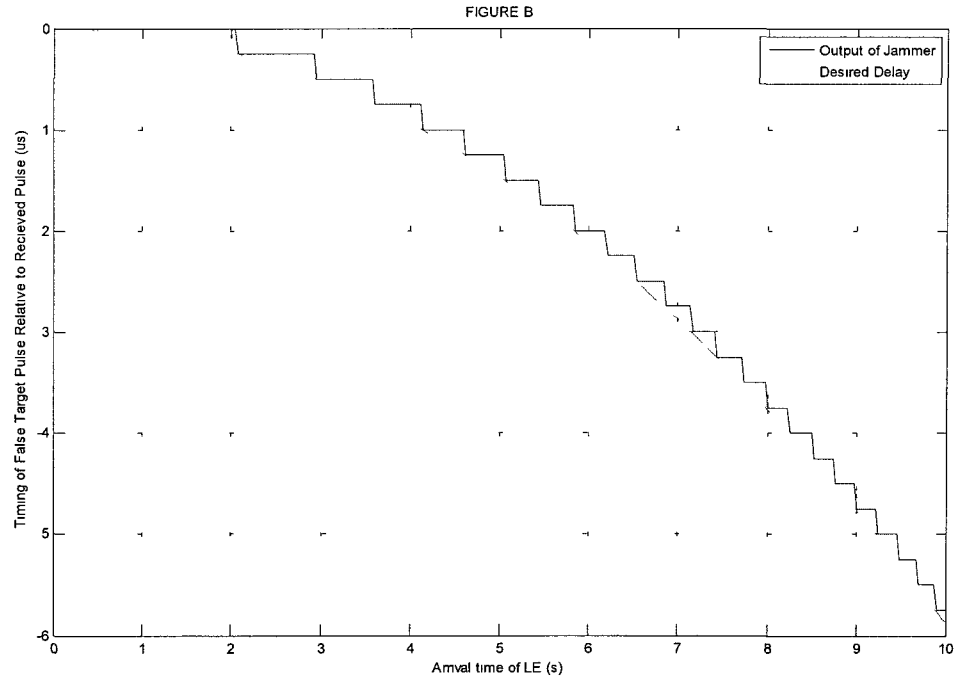
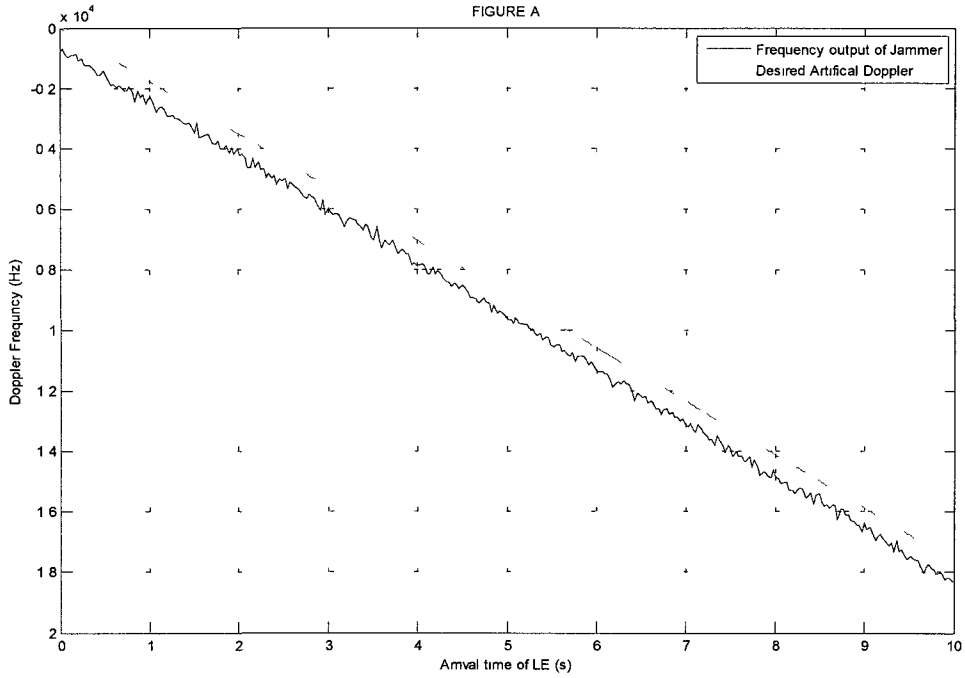


Figure B.3 a & b: Frequency and time delay output from jammer applying profile 3 against fire control radar without additional noise, data decimation by 8



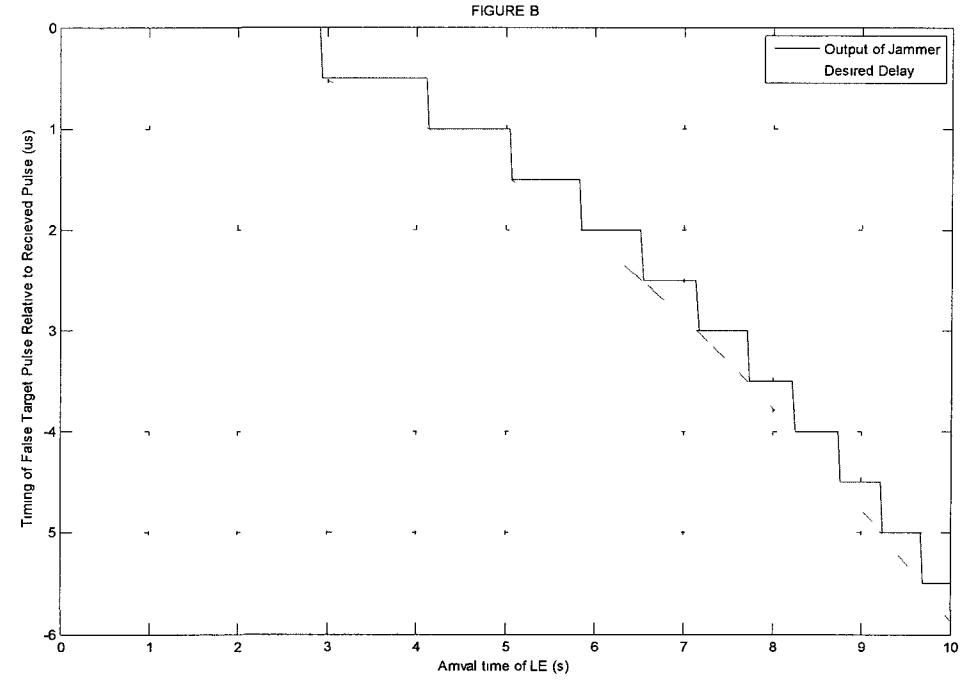
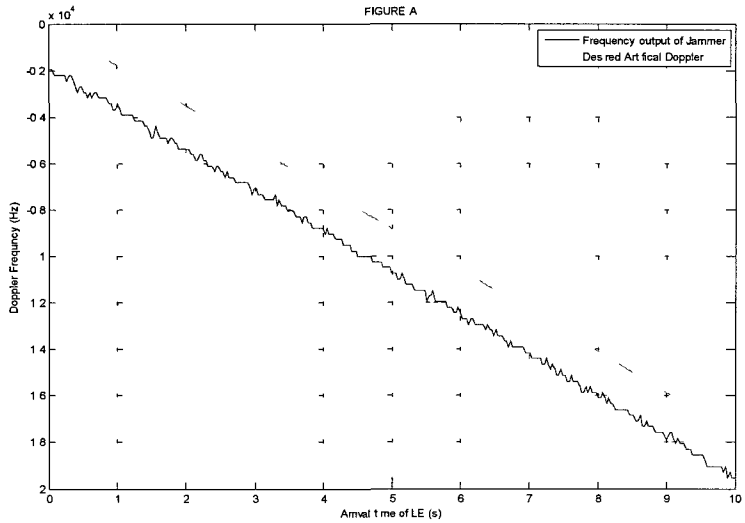


Figure B.4 a & b: Frequency and time delay output from jammer applying profile 3 against fire control radar without additional noise, data decimation by 16

Appendix C – Results for Fire Control Radar with 10 dB SNR

The following figures show the frequency and delay outputs of the jammer compared to the desired values obtained from the CRV profile 3. The fire control radar input radar signal had an SNR of 10 dB. As described in section 5.3.2, a multiple of every 7^{th} pulse was examined. Since the signal bandwidth was 2 MHz, decimation by 32 did not satisfy Nyquist sampling criteria.



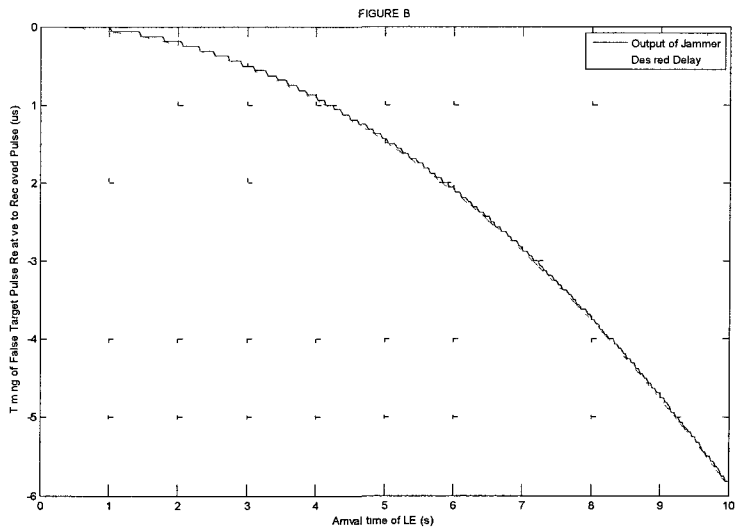
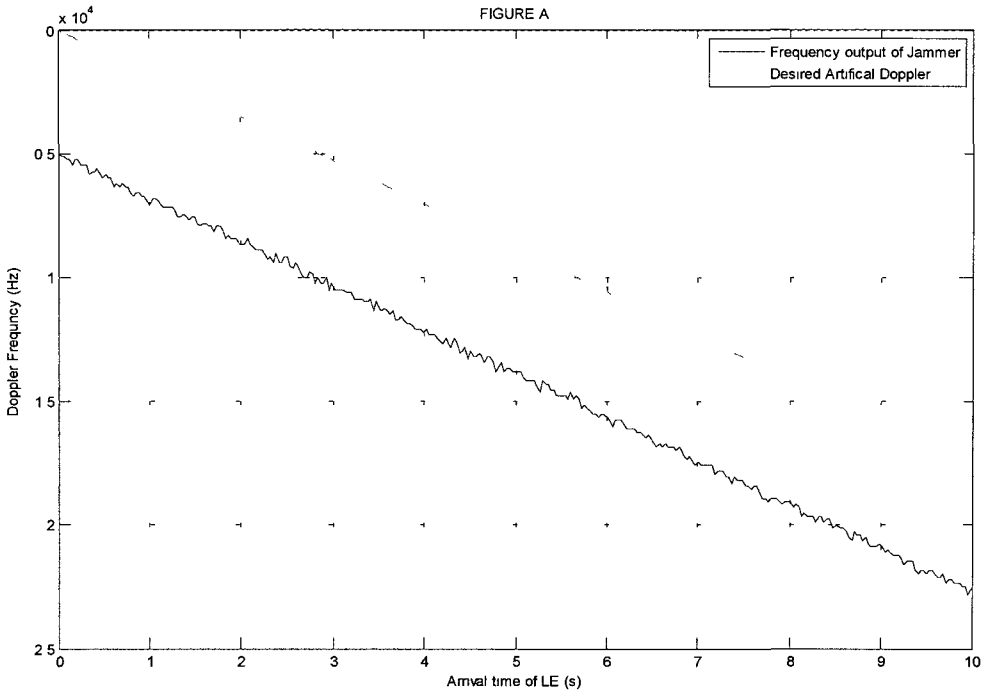


Figure C.1 a & b: Frequency and time delay output from jammer applying profile 3 against fire control radar with 10 dB SNR, data decimation by 2



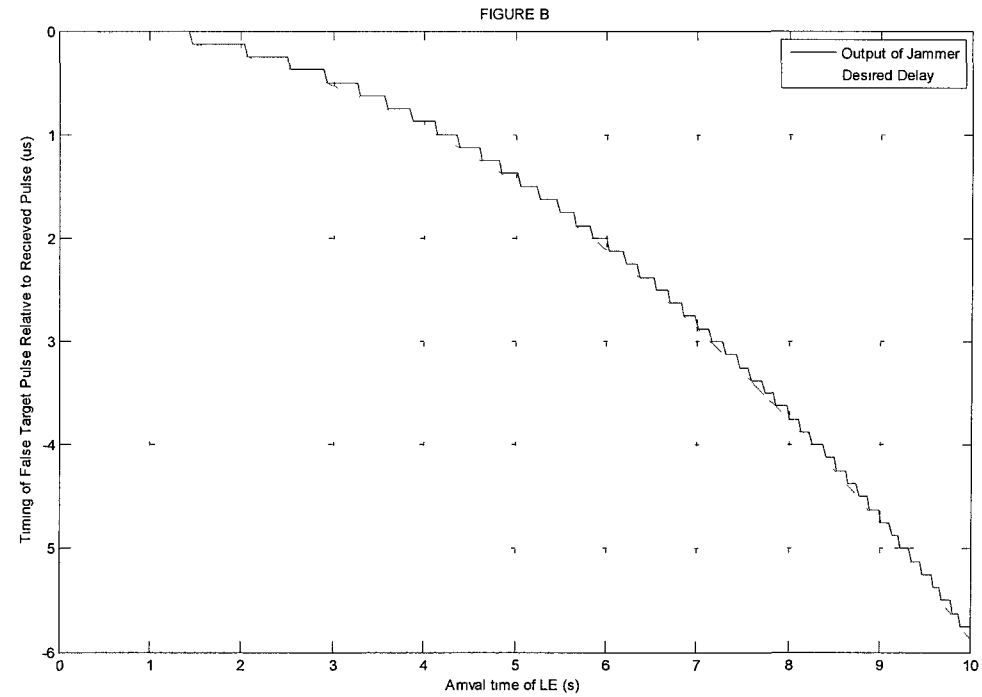
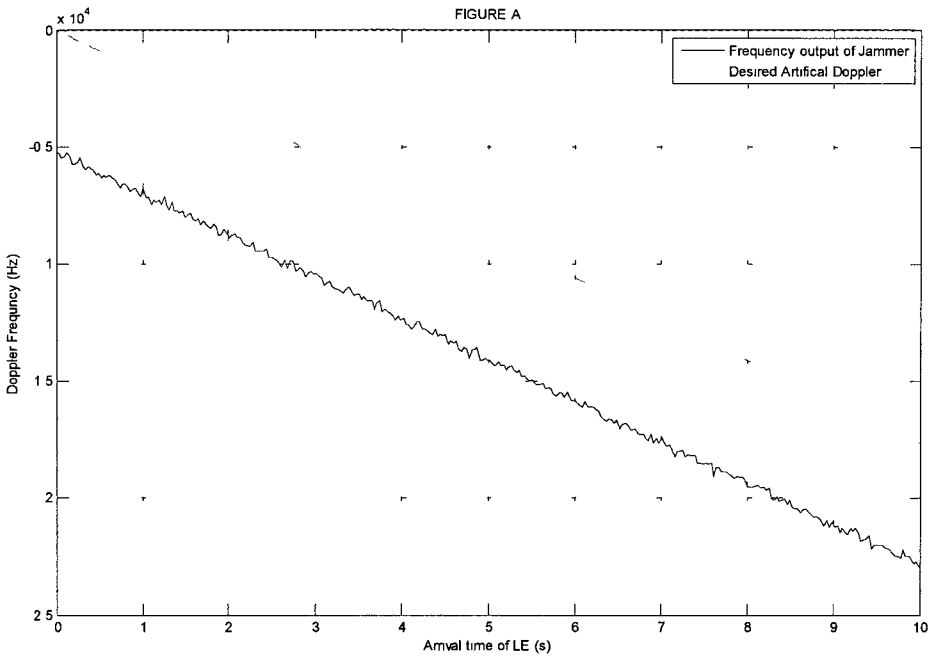


Figure C.2 a & b: Frequency and time delay output from jammer applying profile 3 against fire control radar with 10 dB SNR, data decimation by 4



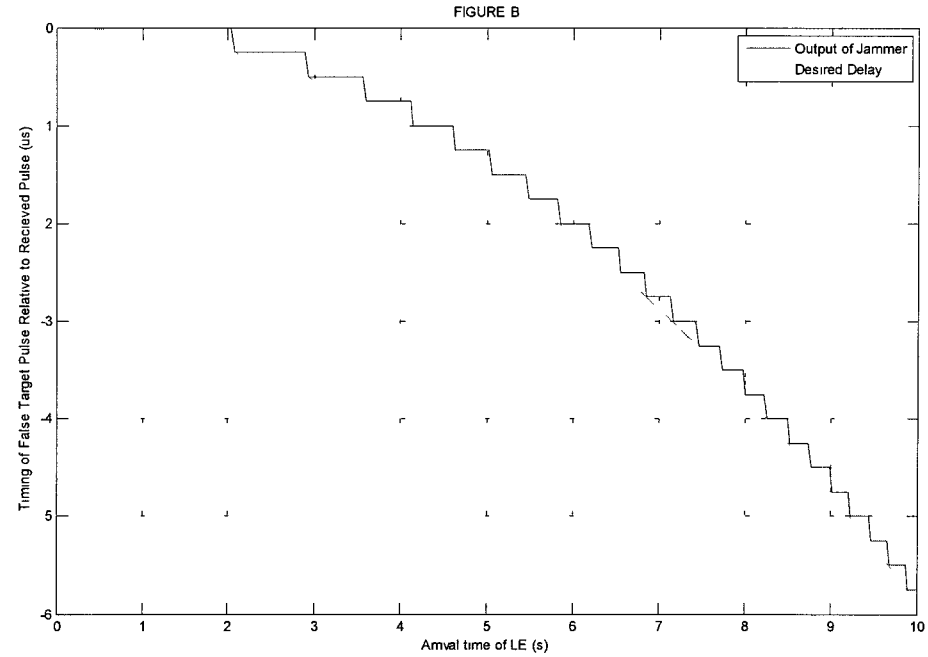
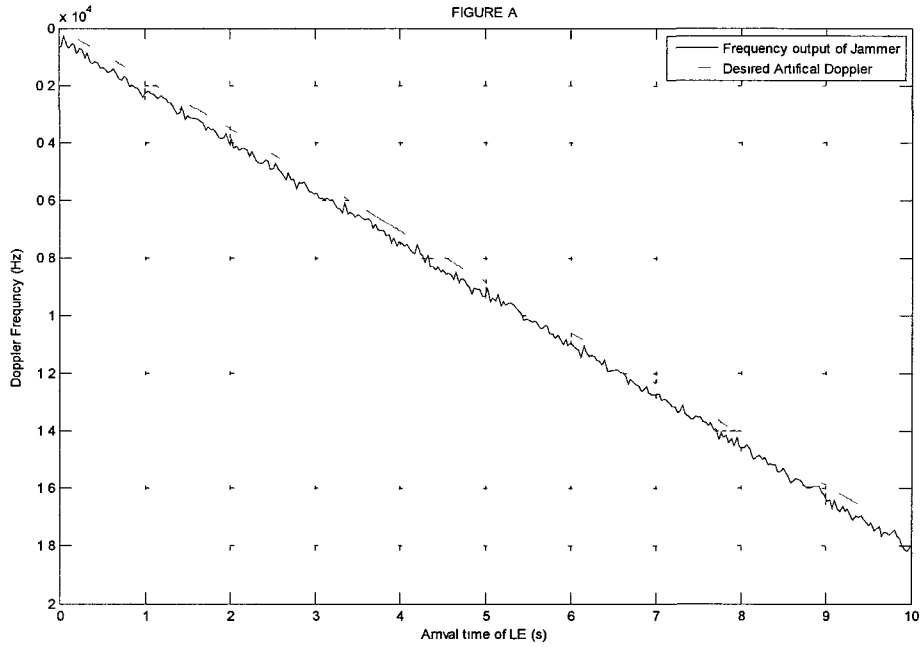


Figure C.3 a & b: Frequency and time delay output from jammer applying profile 3 against fire control radar with 10 dB SNR, data decimation by 8



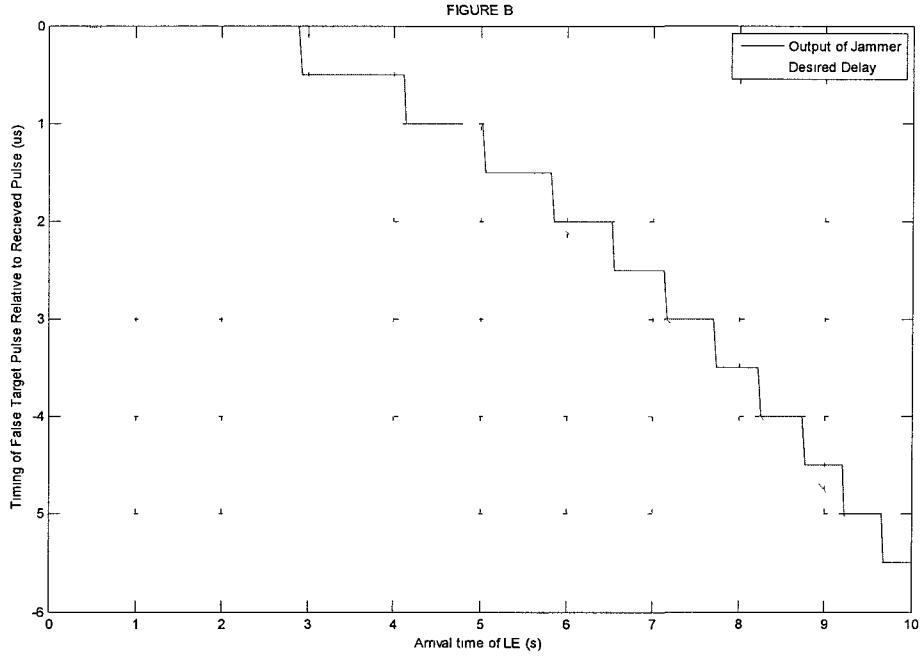
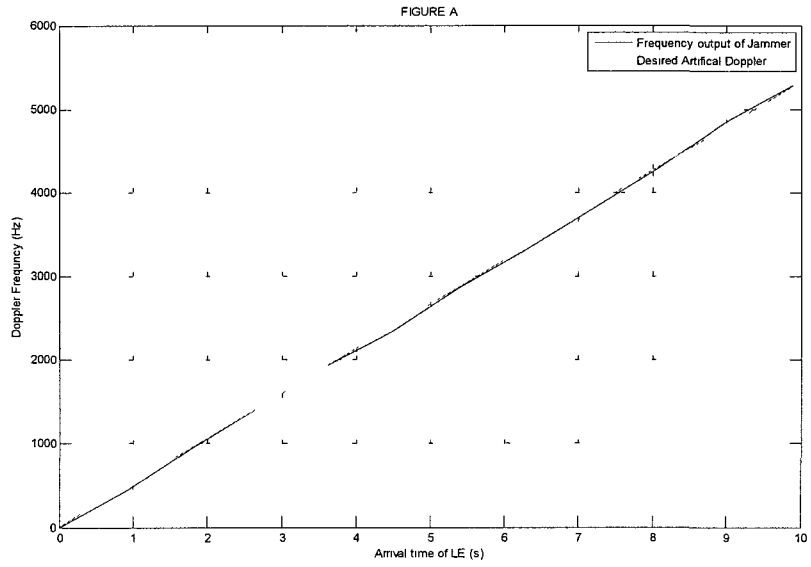


Figure C.4 a & b: Frequency and time delay output from jammer applying profile 3 against fire control radar with 10 dB SNR, data decimation by 16

Appendix D – Results for Surveillance Radar with 10 dB SNR

The following figures show the frequency and time advance outputs of the jammer compared to the desired values obtained from the CRV profile 4. The input surveillance radar signal had an SNR of 10 dB. Since the signal bandwidth was 6 MHz, the only decimation by 2 and 4 were possible to satisfy Nyquist sampling criteria.



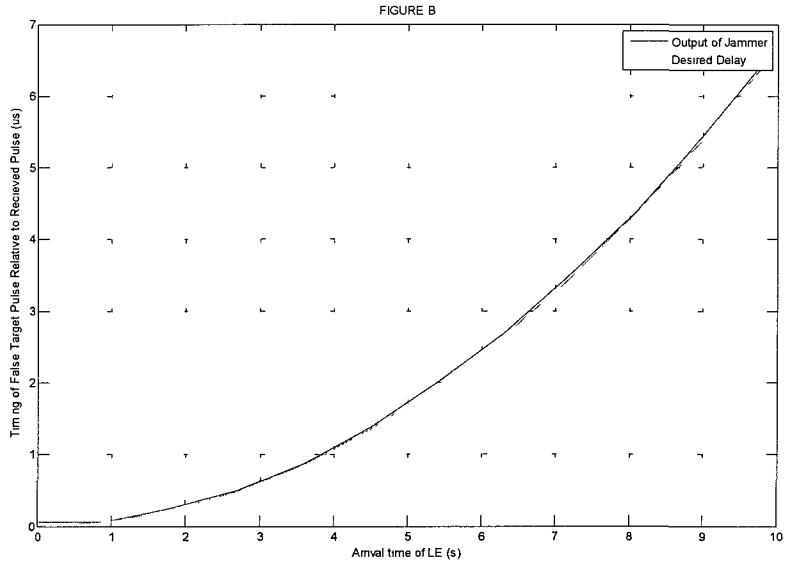
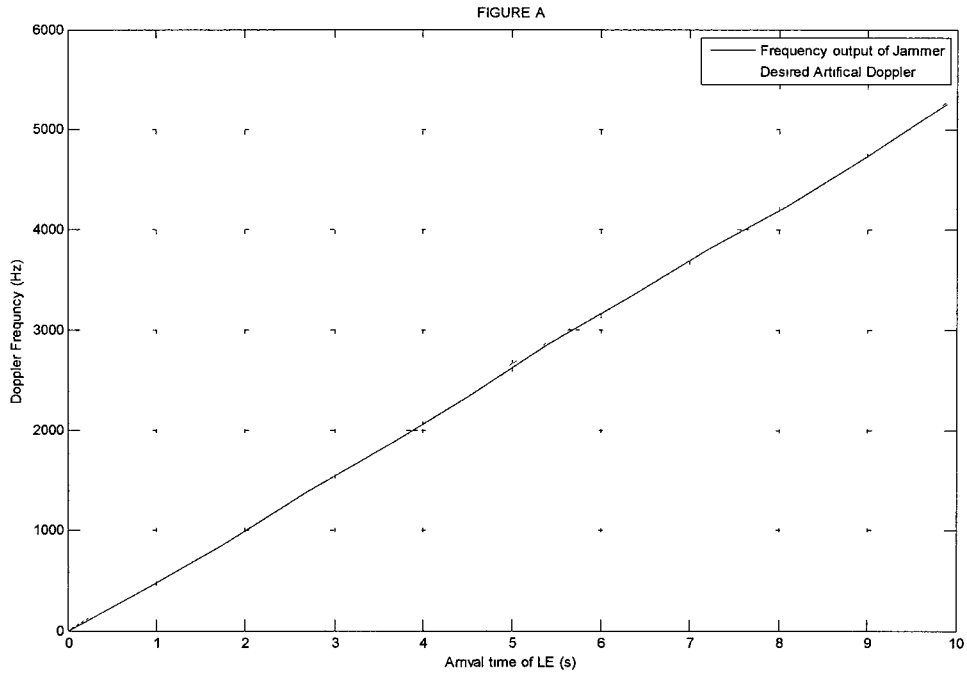


Figure D.1 a & b: Frequency and time output from jammer applying profile 4 against surveillance radar with 10 dB SNR, data decimation by 2



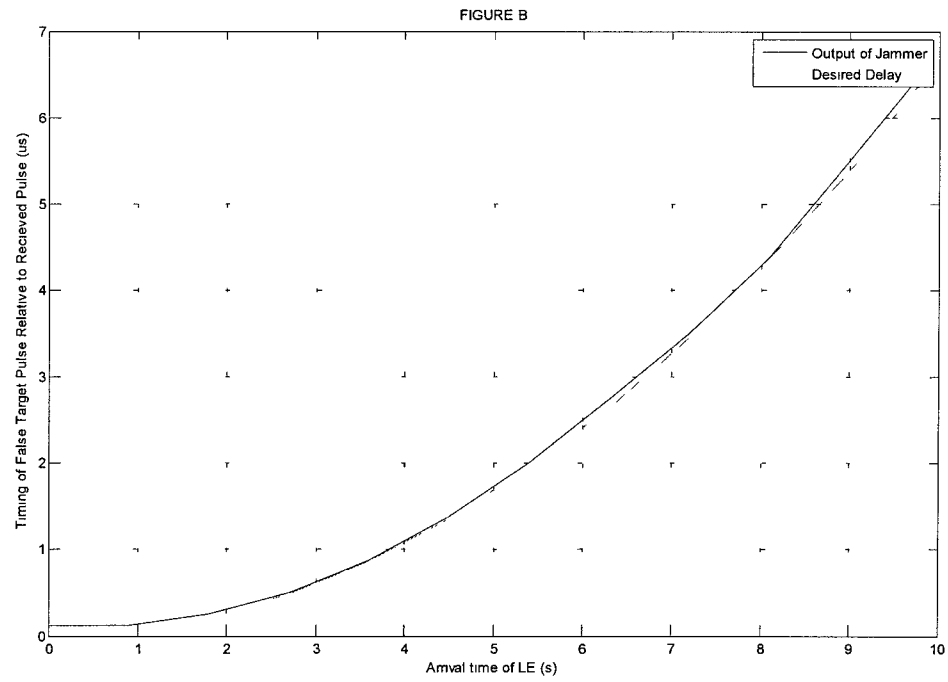


Figure D.2 a & b: Frequency and time output from jammer applying profile 4 against surveillance radar with 10 dB SNR, data decimation by 4

References

[1] M.I. Skolnik, *Introduction to Radar Systems*, 3rd edition, McGraw-Hill, 2001, pp. 115, 12, 30-94, 190, 278

[2] G.W. Stimson, *Introduction to Airborne Radar*, 2nd edition, SciTech Publishing, 1998, pp. 450-455, 199-233, 151, 163-176, 135-150, 442, 469-472

[3] B.R. Mahafza, *Radar Systems Analysis and Design Using MATLAB*, 2nd edition, Chapman & Hall/CRC, 2005, pp. 40-42, 56-63, 207-218, 381-389

[4] D.C. Schleher, *Electronic Warfare in the Information Age*, Artech House, 1999, pp. 1-24, 201-256, 293-331, 333-345

[5] S. Vakin, L. Shustov, R. Dunwell, *Fundamentals of Electronic Warfare*, Arctech House, 2001, p. xiii-xvii

[6] D.C. Schleher, *Introduction to Electronic Warfare*, Artech House, 1986, pp. 29-31, 45-56

[7] W. Richard Stevens, Stephen A. Rago, *Advanced Programming in the UNIX Environment*, 2nd edition, Addison-Wesley, 2005, p173-176

[8] J.G. Proakis, D.G. Manolakis, *Digital Signal Processing Principles, Algorithms, and Applications*, 4th edition, Pearson Prentice Hall, 2007, p750-779

[9] N.A.W Center, *Electronic Warfare and Radar Systems Engineering Handbook*, Point Mugu, CA: Electronic Warfare Division, 1999.

[10] L. Neng-Jing, Z. Yi-Ting, "A Survey of Radar ECM and ECCM", *Aerospace and Electronic Systems, IEEE Transactions on* , vol.31, no.3, pp.1110-1120, July 1995

[11] C.M. Kwak, "Application of DRFM in ECM for Pulse Type Radar", *Infrared, Millimeter, and Terahertz Waves, 2009*. IRMMW-THz 2009. *34th International conference on*, pp. 1-2, September 2009

[12] P. Kalata, T. Chmielewski, "Range Gate Pull Off (RGPO): Detection, Observability and α-β Target Tracking", *System Theory, 1997., Proceedings of the Twenty-Ninth Southeastern Symposium on* , pp.505-508, March 1997

[13] D. Adamy, "Jamming Technique – Cover Jamming", *Journal of Electronic Defense*, August 1996, pp. 66-67,

[14] D. Adamy, "Deceptive Jamming Techniques – Range Gate Pull-Off", *Journal of Electronic Defense*, November 1996, pp. 66-63

[15] D. Adamy, "Deceptive Jamming Techiques Used Against Monopulse Radars", *Journal of Electronic Defense*, Febuary 1997, pp. 52-61

[16] F. Neri, "Anti-Monopulse Jamming Techniques", *Microwave and Optoelectronics Conference.2001.IMOC 2001. Proceedings of the 2001 SBMO/IEEE MTT-S International*, vol. 2, pp. 45-50, 2001

[17] W. Zongbo, G. Meiguo, L. Yunjie, J. Haiqing, "Design and Application of DRFM System Based on Digital Channelized Receiver", *Radar, 2008 International Conference on,* pp. 375-378, September 2008

[18] J. Changyong, G.Meiguo, W. Zongbo, F. Xionqjun, "Design of High Speed DRFM System", *Computer Science and Information Engineering, 2009 WRI World Congress on* , vol.3, pp.582-586, 2009

[19] S. Guoying, L. Yunjie, G. Meiguo, "An Improved DRFM System Based on Digital Channelized Receiver", *Image and Signal Processing, 2009. CISP '09. 2nd International Congress on* , pp.1-5, October 2009

[20] J. Lange, "Digital Electronic Attack Technique Host: DRFM Capability Specification", Defence Research and Development Canada Technical Memorandum 2008-189, September 2008

[21] J. Lange, "Digital Electronic Attack Technique Host: Final Report", Defence Research and Development Canada Technical Memorandum 2009-176, February 2010

[22] J. Lange, "Radio Frequency Countermeasures", Defence Research and Development Canada Technical Memorandum 2006-261, 2006

[23] D. Kutman, "Solutions for Radar Pulse Deinterleaving", Master's Thesis, Carleton University, 2011

[24] D-TA Systems Inc., "DTA- 2300D: Systems Manual", Rev B, December 2010

[25] D-TA Systems Inc., "DTA-2210 Software Development Kit Manual", Rev C, November 2010

[26] D-TA Systems Inc., "Sensor Processing for Demanding Applications", Equipment Manual, May 2011

[27] Texas Instruments DAC5687 Datasheet, Rev E, September 2006. Retrieved from Web site: http://focus.ti.com/docs/prod/folders/print/dac5687.html#technicaldocuments

[28] Linear Technology LTC 2208 Datasheet. Retrieved from Web site: http://www.linear.com/product/LTC2208