NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RISK OF USING PAST TO PREDICT FUTURE: A CASE STUDY OF JAMMING RCIEDS

by

Jeffrey A. Dayton

June 2009

Thesis Advisor:	Kyle Y. Lin
Second Reader:	Michael A. Herrera

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2009	Master's Thesis

4. TITLE AND SUBTITLE Risk of Using Past to Predict Future: A Case Study of Jamming RCIEDs	5. FUNDING NUMBERS
6. AUTHOR(S) Dayton, Jeffrey A.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

12a. DISTRIBUTION/AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

The radio controlled improvised explosive device (RCIED) is one of the deadliest threats to military personnel supporting the global war on terrorism, and due to its success is expected to play a major role as a weapon of choice in future insurgencies. To mitigate the risk of a RCIED attack, electronic jamming devices are utilized to interrupt the communications between a remote control and the RCIED trigger. We consider two approaches to determine the optimal jamming strategy for the coalition force. First, we formulate a mixed integer program to find the optimal jamming strategy based on recent attack data of RCIEDs. Second, we formulate a two-person zero-sum game to determine the optimal mixed strategy for jamming. With a simulation study, we found that with the first approach the coalition force tends to be overly optimistic in predicting the outcome, and is likely to underperform. In addition, the first approach allows the possibility for smart insurgents to deploy RCIEDs to purposely mislead the coalition force on what they plan to do in the future. The second game-theoretic approach provides a robust jamming strategy no matter how Red chooses to deploy their RCIEDs.

14. SUBJECT TERMS Game Theory, Zero-Sum Game, Radio Controlled Improvised Explosive Device Loadset, RCIED Loadset, Active Jamming Loadset, Optimizing Active Jamming Loadset	15. NUMBER OF PAGES 95
	16. PRICE CODE

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

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RISK OF USING PAST TO PREDICT FUTURE: A CASE STUDY OF JAMMING RCIEDS

Jeffrey A. Dayton
Major, United States Army
B.S., Rochester Institute of Technology, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
June 2009

Author: Jeffrey A. Dayton

Approved by: Kyle Y. Lin
Thesis Advisor

Michael A. Herrera
Second Reader

Robert F. Dell
Chairman, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The radio controlled improvised explosive device (RCIED) is one of the deadliest threats to military personnel supporting the global war on terrorism and due to its success is expected to play a major role as a weapon of choice in future insurgencies. To mitigate the risk of a RCIED attack, electronic jamming devices are utilized to interrupt the communications between a remote control and the RCIED trigger. We consider two approaches to determine the optimal jamming strategy for the coalition force. First, we formulate a mixed integer program to find the optimal jamming strategy based on recent attack data of RCIEDs. Second, we formulate a two-person zero-sum game to determine the optimal mixed strategy for jamming. With a simulation study, we found that with the first approach the coalition force tends to be overly optimistic in predicting the outcome, and is likely to underperform. In addition, the first approach allows the possibility for smart insurgents to deploy RCIEDs to purposely mislead the coalition force on what they plan to do in the future. The second game-theoretic approach provides a robust jamming strategy no matter how Red chooses to deploy their RCIEDs.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. RELATED WORK....3
B. THESIS ORGANIZATION....3

II. BACKGROUND ON RCIED AND JAMMING TECHNOLOGY....5
A. RCIED....5
B. JAMMING TECHNOLOGY....7
1. Jammers and CREW....7
2. Active and Reactive Jamming....8

III. METHODOLOGY....11
A. THE GAME-THEORETIC MODEL....11
1. Formulation of Zero-Sum Game for Blue....13
2. Formulation of Zero-sum Game for Red....14
B. OPTIMIZATION BASED ON RECENT ATTACK DATA....15
C. MODEL IMPLEMENTATION....18

IV. NUMERICAL EXPERIMENTS....23
A. THE MAIN EXAMPLE....23
1. Damage....24
2. Trigger Power....25
3. Frequency Bands....25
4. Jammer Power....25
B. DESIGN OF EXPERIMENT....26
C. RESULTS AND ANALYSIS....27
1. Heightened Expectation....27
2. Under Performance....31
D. DISCUSSION....36

V. CONCLUSIONS AND RECOMMENDATIONS....37
A. KEY FINDINGS....37
B. RECOMMENDATIONS FOR FUTURE RESEARCH....38

APPENDIX A: IED OVERVIEW....39
A. GAME THEORY....39
B. BEHIND THE IED....39
1. Components of an IED....39
2. Current Employment Techniques....41
3. IED Classifications....42
4. Current Threat....44
5. Insurgency and Counter-insurgency....45
C. HISTORY OF THE IED....46
1. Current Effect of the IED....46
2. Origin of the Acronym IED....47
3. IEDs Throughout History....49

APPENDIX B: OVERVIEW ON JAMMING TECHNOLOGY 51
A. GROUND JAMMING SYSTEMS 51
B. ELECTROMAGNETIC SPECTRUM MANAGEMENT 54
APPENDIX C: JAMMING PRINCIPLES AND DEFINITIONS 57
A. BASIC EW COMPONENTS AND PRINCIPLES 57
1. Antenna 57
2. Distance 57
3. Power 58
4. Duty Cycle and Time Sharing 60
5. Power Sharing 62
B. SIMPLIFICATION OF DATA REQUIREMENTS 63
APPENDIX D: DATA AND GRAPHS 67
A. DATA PLOTS 67
B. PLOTS OF MEANS AND CONFIDENCE INTERVALS 69
C. COMBINED PLOTS OF MEANS AND CONFIDENCE INTERVALS 71
LIST OF REFERENCES 73
INITIAL DISTRIBUTION LIST 77

LIST OF FIGURES

Figure 1. A soldier holds a RCIED using a cell phone as the triggering device.....7
Figure 2. RCIED Data.....12
Figure 3. Payoff matrix, Blue Strategy, Red Strategy, and Value of Game.....19
Figure 4. Sample solution from optimization of recent attack data model. 20
Figure 5. The model data.....24
Figure 6. Build of Red's observed strategy of recent attacks.....27
Figure 7. All observation values at 30 Watts for heightened expectation (less damage is better).....28
Figure 8. Data plot for heightened expectation over full range of power for 40 observations with 100 replications.....29
Figure 9. Expected damage and actual damage with confidence intervals.....31
Figure 10. All observation values at 30 Watts for under performance (less is better).....32
Figure 11. Data plot for under performance over full range of power for 40 observations with 100 replications.....33
Figure 12. Resulting and expected damage based on 10, 20, 40, 80, and 160 observations. 35
Figure 13. Components of an IED [From (Australian Government, Department of Defense)].....41
Figure 14. The Evolving Threat of IEDs by Trigger [From (Atkinson 15)].....43
Figure 15. Common Radio Controlled IED Triggers.....44
Figure 16. IED Incidents in Iraq [From (U.S. House of Representatives 43)].....46
Figure 17. IED Incidents in Afghanistan [From (U.S. House of Representatives 44)].....47
Figure 18. The jamming scenario [After (D. L. Adamy, EW102: A Second Course in Electronic Warefare 137)].....58
Figure 19. Two duty cycles of a single transmission [After (Electronic Warfare Division 2-5)].....61
Figure 20. Sample jamming scenario of a single transmission over two duty cycles.....61
Figure 21. Sample scenario of time share jamming of two transmissions over two duty cycles 62
Figure 22. Jamming of two signals with different power requirements.....63
Figure 23. Jamming of three signals with two signal power sharing.....63

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CREW	Counter RCIED Electronic Warfare
CWIED	Command Wire Improvised Explosive Device
EOD	Explosive Ordnance Disposal
FCC	Federal Communications Commission
GAMS	General Algebraic Modeling System
ICE	IED Countermeasures Equipment
IED	Improvised Explosive Device
IRA	Irish Republican Army
JIEDDO	Joint IED Defeat Organization
JIN	Joint IED Neutralizer
LRCT	Long Range Cordless Telephone
MOASS	Mother of All Spreadsheets
NIRF	Neutralizing IED with Radio Frequency
RCIED	Radio Controlled Improvised Explosive Device
UXO	Unexploded Ordnance
VBIED	Vehicle-borne IEDs
VOIED	Victim-Operated Improvised Explosive Device

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The improvised explosive device (IED) is the deadliest threat to military personnel supporting the global war on terrorism. From October 7, 2001 there have been over 2,373 deaths due to IEDs and the use of the IED has grown to unmatched numbers in use against military forces and has been termed the insurgent's "Weapon of Choice." One prominent form of the IED is the radio controlled IED (RCIED), which is detonated remotely via radio signals. Insurgent forces utilize common commercially available radio controlled devices such as garage door openers, cordless telephones, and cellular phones to remotely detonate these deadly roadside bombs. To prevent RCIED attacks, coalition forces use recent attack data to design the loadset for their electronic jamming devices. Does using recent attack data furnish coalition forces with the best strategy to exploit the disruption of the highly adaptive insurgents' future RCIED operations?

In this thesis, we develop a two-person zero-sum game for the combat between RCIEDs and electronic jammers. The model parameters include the RCIEDs available, their respective signal power, frequency used, and damage function. The problem facing the jammer is how to allocate a given jamming power among frequency channels in order to minimize the expected damage incurred by RCIED attacks. The model is implemented in an Excel interface, with the solution algorithm written in GAMS and solved using CPLEX.

Using a test example with 15 RCIEDs covering 21 frequency channels, the model produces the optimal RCIED mixture for the insurgents. Based on this optimal mixture, we simulate RCIED attacks that are observed by the coalition forces, who then design the optimal loadset based on those observations. We found that when using past to predict future, the coalition force tends to be overly optimistic in predicting the outcome. The coalition force is also likely to underperform, and the performance gap depends highly on the size of collected data. Furthermore, if the jamming loadset is determined based on the RCIED attack data, it is possible for smart insurgents to deploy RCIEDs to purposely mislead the coalition force about what they plan to do in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

An adventure in learning such as this is a test of patience, understanding, application, and unending dedication that, although completed alone, I have had the assistance and support of many people. To my wife, Zaida, you are my rock and my inspiration. To my children; Jacob, Zaida, and Jonah, you may not understand this, but you are the center of my universe. Dr. Kyle Lin, thank you for being more than an advisor in letting me take the lead and allowing mistakes to further the learning. Whenever we hit a dead-end, you always had a positive suggestion on how to reroute and continue forward. Thank you, CDR Michael Herrera, for your constant positive support and never allowing for me to lose sight of the goal. Dr. Gordon Bradley, thank you for opening my eyes to the layers involved in the world of IEDs. Dr. W.M. Carlyle, much appreciate for assisting with complicated coding questions, providing recommendations on difficult algorithms, and for just answering some of my silly questions. Much appreciation to LCDR Chris Taylor for taking the time and explaining some of basics of electrical engineering principles so I could go into complex areas with my eyes open. Many heartfelt thanks to the multitude of professionals at the Naval Postgraduate School who have provided me with the tools to embark a thesis such as this with little fear. Lastly, I would like to dedicate this work to all the fine Americans that have dedicated themselves to the service of this great nation. If this work even remotely assists in preserving one life, it will have been worth every ounce of effort placed into the completion.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Improvised explosive devices (IED) may have been an old tactic revived by insurgents, and may grow into a prominent tactic for insurgents and terrorist worldwide to threaten forces (Wilson 1). The U.S. counter-IED strategy now follows three distinct paths: defeat the device, attack the network, and train the force (Atkinson 21). Prior to exploring the creation of this game theoretic model, many concepts must be explained or explored to formulate and understand the background of this horrific weapon.

The improvised explosive device is the deadliest threat to military personnel supporting the global war on terrorism. From October 7, 2001 there have been over 2,373 deaths due to IEDs (Defense Manpower Data Center). The use of the IED has grown to unmatched numbers in use against military forces and has been termed the insurgent's "Weapon of Choice." (Australian Government, Department of Defense) Due to the continued success of this strategic weapon, this type of weapon is expected to both continue in employment, and grow in application by insurgencies. Examples are seen worldwide.

One prominent form of the IED is the Radio Controlled IED (RCIED), which is detonated remotely via radio signals. Insurgent forces utilize common commercially available radio controlled devices such as garage door openers, cordless telephones, and cellular phones to remotely detonate these deadly roadside bombs. To prevent RCIED attacks, coalition forces use electronic jammers to jam the communications between the wireless trigger and the bomb itself. Due to power limitations, however, usually the electronic jammer cannot jam all frequency bands. One common way to decide which frequency bands to jam is to use recent attack data to determine which bands the insurgents are more likely to use. The focal point of this thesis is finding an answer to the question, "Does using recent attack data furnish coalition forces with the best strategy to exploit the disruption of the highly adaptive insurgents' future RCIED operations?"

When taking a given amount of available power how do we apply this power to our electronic jamming systems in order to minimize the threat? This thesis considers two approaches. The first approach is to look at the recent attack data on RCIED triggers usage and design the optimal loadset by assuming what will happen in the future is similar to what has happened in the past. The second approach is to apply a game-theoretic model by assuming the insurgents actively choose their RCIED triggers in order to inflict the maximal damage.

When these two approaches are used, does the attack data and the game theoretic solutions provide the same or completely different solutions? If the solutions are different, what drives the quality of the solution? In addition, what is the relationship between the two solutions?

In this thesis, we develop a two-person zero-sum game for the combat between Red, who attacks with RCIEDs and Blue, who defends with electronic jammers. The model parameters include the RCIEDs available, their respective signal power, frequency used, and damage function. Red chooses one RCIED in order to incur the maximal expected damage. The problem facing Blue is how to allocate a given jamming power among frequency channels in order to minimize the expected damage incurred by RCIED attacks. The model is implemented in an Excel interface, with the solution algorithm written in GAMS and solved using CPLEX.

To compare the two approaches, we conduct a numerical experiment with 15 RCIEDs covering 21 frequency channels. We first use linear programming to compute the optimal mixed strategy for both players and the value of the game. Next, we simulate Red's optimal mixed strategy to generate a sequence of RCIED choices for Blue to observe. After observing the percentage of each RCIED used by Red, Blue then formulates a mixed integer program to compute the optimal jamming strategy based on observed data. Finally, we compare Blue's performance in these two approaches.

We found that when using past to predict future, the Blue tends to be overly optimistic in predicting the outcome. Blue is also likely to underperform, and the performance gap depends highly on the number of observations used to collect the data.

Furthermore, if the jamming loadset is determined based on observations of the RCIED attack data, it is possible for Red to smartly deploy RCIEDs to purposely mislead the coalition force about what they plan to do in the future. This causes Blue to suffer much more damage than they expected.

A. RELATED WORK

Martin and Nickerson (2008) developed the methodology to create an optimal jammer strategy using a zero-sum game technique as described in their joint thesis entitled, "A Game Theoretic Approach to IED Jamming Strategy". This thesis provided insight into the application of game theory in providing an optimal strategy of active jamming load sets. Lin and Shen (2008) wrote "A Game-Theoretic Model for Jamming Radio Controlled Improvised Explosive Devices" with the application "Jammer Decision-Aid Tool V1." This tool uses similar methodology as Martin and Nickerson's earlier work while implementing and executing the model solely through Microsoft Excel. The goal of this research is to expand upon the Jammer Decision-Aid Tool to incorporate active jamming techniques modeled to emulate current Counter RCIED Electronic Warfare (CREW) systems jamming capabilities and limitations. In particular, this thesis extends the earlier work by allowing each RCIED trigger to operate with a different power, and allowing the jammer to allocate different power levels to frequency bands.

B. THESIS ORGANIZATION

The rest of this thesis is organized as follows. Chapter II provides background on RCIEDs and various jamming technologies. Chapter III introduces the methodology, in particular, a mathematical model we developed to analyze the jamming problem. Chapter IV presents the numerical experiments designed to provide insights into the risk of using past to predict future when jamming RCIEDs. Lastly, Chapter V concludes the thesis and points out possible future research directions.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND ON RCIED AND JAMMING TECHNOLOGY

This chapter provides an overview of the RCIED and the basic definitions related to jamming systems. Section A reviews the basic definition of an RCIED as it is encountered on today's battlefield. Section B discusses the basic principles behind the effort aimed at countering the RCIED. From this background, the foundation of a model is built and discussed through the following chapters

A. RCIED

An improvised explosive device (IED) is defined as a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals or explosives and designed to destroy, incapacitate, harass, or distract (Department of Defense 256). Essentially, an IED can incorporate military ordnance or parts of ordnance used with improvised components in a non-standard fashion or build with entirely non-military pieces.

Almost any type of material can be found in the creation of an IED. It is fundamentally a "homemade" device with the purpose of causing death, injury, or destruction. IEDs are created in varying configurations, containers, functions, delivery methods, triggers, initiators, and explosive types. What makes IEDs unique is that the bomb maker improvises with fairly common items that are readily available to build the device (Improvised Explosive Devices (IEDs)/Booby Traps).

The RCIED is a type of IED defined by the trigger. The trigger of an RCIED is a radio transmitter and receiver link. A few examples are car alarms, wireless door bells, cell phones, pagers and walkie-talkies. The initial threat from RCIEDs came from low frequency and low powered devices such as garage door openers, radio controlled toys, RC units from car alarms, and wireless doorbells. Cellular, satellite and long range cordless telephones (LRCT) are currently some of the most used initiators for these devices (D'Alessio).

The device is constructed so that the receiver is connected to an electrical firing circuit. The transmitted signal causes the receiver to initiate the IED. Usually the receiver triggers the initiator, but it may also be used to remotely arm the device to be initiated by other means. The adaptation of using radio control devices has enabled the insurgent freedom of movement with standoff ability that is not limited by a wire. The absence of a wire gives the insurgent autonomy while maintaining the control of initiating the IED (CTF-7 CALL Representative 5).

There is a distinct future of IEDs forecasted in asymmetric warfare. Commenting on the future of IEDs, Lieutenant General Thomas Metz, USA, Director, JIEDDO commented:

> I am often asked if the IED threat can be removed from the battlefield, and my answer is, 'No.' In its most fundamental form, the IED is a lethal ambush, and men have been ambushing their enemies for thousands of years. (U.S. House of Representatives 41)

RCIEDs account for the largest proportion of casualties in today's modern asymmetric warfare environments. A successful counter strategy is the combination of acute threat analysis with technological devices (Kestrel, a Lightweight, Software-Configurable Jamming System to be Exhibited at IDEX 2009). Due to their demonstrated success in Iraq and Afghanistan, it is acknowledged that the use of IEDs on the battlefield is a definite threat to current and future force protection (U.S. House of Representatives 48).

Facing a numerically, militarily, or industrially superior opponent, the use of IEDs by inferior forces is not a surprise. From an enemy perspective of being outnumbered, outgunned, or ill-equipped; the use of IEDs is logical. The enemy can negate their opponents' combat advantages with devices that are highly effective, readily available, and fairly inexpensive. These enticing qualities of munitions provide the asymmetric enemy the capability to efficiently strike without fear of substantial loss.

Eliminating IEDs as a weapon of strategic influence depends on defeating the networks that buy, build, and place the bombs (Atkinson 28). In order to defeat this network, service members need the autonomy to traverse the battle space freely to pursue

and engage these networks. This is the importance of the jammer as one form of protection to ensure freedom of movement. Figure 1 shows one definitive success of a jamming system as an EOD expert holds a cell phone IED triggering device that malfunctioned. (U.S. House of Representatives 16) This is one case where there is no question that a jammer successfully performed its mission.

Figure 1. A soldier holds a RCIED using a cell phone as the triggering device

Further in-depth information on the background of IEDs is located in Appendix A for the inquisitive reader. Appendix A contains information on the components of an IED, the distinct classifications of an IED, and the current IED threat. This appendix also contains a breadth of information on IEDs through history, the first occurrences of the term IED, and how the insurgents employ IEDs.

B. JAMMING TECHNOLOGY

1. Jammers and CREW

RCIED jammer systems are electronics-based radio frequency communication systems. Jammers transmit from low to high power, up to 500 Watts. They are one form of electronic warfare countermeasure that usually operates in frequency ranges from 20 to

300 megahertz. RCIED jammers either blocks the radio signal of a transmitter to receiver or causes an intended RCIED to prematurely detonate. Both cases involve the jammer transmitting radio signals. The blocking of the signal involves the jammer to over-ride the original signal and effectively blocking it through interference. The latter goal involves the intended remote detonation at an intended safe distance (U.S. House of Representatives 16). An important note is that when a jammer is effective, often service members will not even know that they were in danger of a potential IED blast.

RCIED jammers are members of the Counter Radio Controlled Improvised Explosive Device Electronic Warfare (CREW) systems. Two of these CREW systems include the IED Countermeasures Equipment (ICE) and the Warlock. Both of these devices use counter radio frequencies to block the signals of the radio control explosives triggers (Wilson 4). Two other members of the CREW family that transmit at high frequencies to counter the electronics in RCIEDs are the Joint IED Neutralizer (JIN) and the Neutralizing Improvised Explosive Devices with Radio Frequency (NIRF) (Wilson 4).

2. Active and Reactive Jamming

Each jammer uses a different concept of jamming to block the radio signal of the RCIED. The two types of jamming used to block the radio signal are referred to as active and reactive. With active jamming, a jammer emits electromagnetic waves continuously across a spectrum of preset frequencies to interrupt the RCIED triggering signal (Atkinson 25).

With reactive jamming, a jammer scans the selected segments of the electromagnetic spectrum in search of a threat frequency. Once a threat frequency is detected, the jammer then transmits on that frequency to interrupt the radio trigger for as long as the threat frequency is present (Atkinson 25). Effectively, the reactive jammer could be thought of as a scan and jam device. It becomes more flexible as it is not constrained by the prescribed list of constant channels to block and can effectively monitor more potential threats. The cost of this flexibility is that the device cannot

always jam all threat encountered if in a densely populated electromagnetic environment and with reactive jamming, a jammer listens and acts, it is possible that it is too late to act after hearing something. Active jamming does not have these problems.

With respect to the lessons learned and derivations discussed in Chapter III, we begin the creation of a model that generates the optimal minimal damage given an amount of power to apply to an active jamming system. The jamming modules in the model are combined to create an RCIED jamming system or package. The strategies from this point forward are with respect to a module or set of modules working hand in hand to successfully jam a RCIED threat.

Interested readers can refer to Appendix B for supplementary information on electronic jammers and the electromagnetic spectrum. Appendix C explores electronic warfare principles and advanced concepts.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

This chapter introduces the mathematical models designed to assess the risk of using the past to predict the future in jamming RCIEDs. Section A discusses a two-person zero-sum game, where Red chooses an RCIED trigger and Blue chooses an active jamming strategy. Section B discusses an optimization model, where Blue determines its optimal jamming strategy based on the percentage each trigger is used by Red. Section C explains how these two models are implemented in an Excel interface, with optimization written in GAMS and solved using CPLEX.

A. THE GAME-THEORETIC MODEL

In this section, we develop a two-person zero-sum game for the combat between Red, who attacks with RCIEDs, and Blue, who uses electronic jammers to interfere with RCIED detonation signals. Suppose there are *n* RCIED triggers available, and together they use *m* frequency channels. Let $a_{i,j} = 1$ if trigger *i* uses channels *j*, for $i = 1,...,n$ and $j = 1,..,m$. Each trigger uses at least one channel, and it is possible that a trigger uses multiple channels. For instance, a quad-band cell phone can use any of its four channels to transmit a detonation signal. Figure 2 shows an example with *n* = 15 and *m* = 21, where the matrix $[a_{i,j}]$ is shown on the right-hand side.

Total Power available = 30.00

	Name	Damage	Power	Frequency Bands in Spectrum 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	Key Fob	1	0.75	1																				
2	Garage Opener	1	0.5		1																			
3	RC Toy 1	1	1			1																		
4	Wireless Doorbell	1	1				1																	
5	RC Toy 2	1	1					1																
6	Walkie-Talkie 1	1.1	1.75						1															
7	Walkie-Talkie 2	1.2	2							1	1													
8	LRCT Handset 1	1.2	2									1	1											
9	LRCT Base 1	1.2	2.5										1	1										
10	LRCT Handset 2	1.2	2.2											1	1									
11	LRCT Base 2	1.3	2.7													1	1	1						
12	Cell Phone 1	1.4	2.8															1	1					
13	Cell Phone 2	1.4	2.9																1	1				
14	Cell Phone 3	1.5	3																	1	1	1	1	
15	Cell Phone 4	1.4	2.9																				1	1

Figure 2. RCIED Data

Besides the matrix $[a_{i,j}]$, the model has two parameters for each trigger, as shown on the left-hand side in Figure 2. An RCIED detonated by trigger *i* delivers a damage d_i and requires a jamming signal with power at least w_i to jam each channel it uses. The damage scale d_i is relative, while w_i is measured in Watts.

In this two-person zero-sum game, Red has *n* pure strategies, each corresponding to a RCIED trigger. A pure strategy by Blue is an allocation of jamming power among *m* channels as long as the total does not exceed the total power available, denoted by *t*. Although this definition results in an infinite number of pure strategies, we can trim them down by the following arguments. First, each of Blue's pure strategy is defined by the set of triggers it jams. If two pure strategies jam the same set of triggers, they should be regarded as the same pure strategy even if they have a different power allocation. This observation ensures that the total number of Blue's pure strategies is at most 2^n, where *n* is the number of triggers.

Second, for each of these 2^n potential pure strategies, we can eliminate those that are infeasible; that is, those pure strategies that require more than a total power *t*. Third, we can remove dominated pure strategies. For instance, if it is feasible to jam triggers {1,2,4,5}, then any pure strategy that jams only a subset of {1,2,4,5} is dominated. Let *s* denote the number of Blue's pure strategies after applying these three steps. The value *s* depends on the total jamming power available *t*. When *t* is small, there are few pure

strategies because most of them are infeasible. When *t* is large, there are also few pure strategies because most of them are dominated. The value of *s* tends to be at its largest possible value when *t* is about half of the total power required to jam all *n* triggers.

At this point, we have converted the two-person zero-sum game between Red and Blue into a standard form, where Red has *n* pure strategies, and Blue has *s* pure strategies. If Red uses pure strategy *i*, $i = 1,..,n$, and Blue uses pure strategy *k*, $k = 1,..,s$, then the payoff to Red is $b_{i,k} = 0$ if trigger *i* is jammed by Blue's pure strategy *k*, and $b_{i,k} = d_i$ otherwise.

1. Formulation of Zero-Sum Game for Blue

Let $(B_1,...,B_s)$ denote a mixed strategy for Blue, where $\sum_k B_k = 1$. The decision variable B_k, $k = 1,...,s$, denotes the probability Blue uses pure strategy *k*. In order to minimize the expected damage incurred by RCIEDs, Blue can formulate a linear program to determine its optimal mixed strategy as follows.

Sets & Indices:

i index number for RCIED triggers

k index number for pure strategies

Data:

$b_{i,k}$ damage incurred if Red uses RCIED *i* by Blue uses pure strategy *k*

Decision Variables:

B_k percentage use of pure strategy *k*

V value of game

Formulation:

Objective:

$$\min V \tag{1}$$

subject to

$$\sum_k b_{i,k} B_k \le V \quad \forall i \tag{2}$$

$$\sum_k B_k = 1 \tag{3}$$

where

$$B_k \ge 0$$

The maximum damage that Blue can receive is the variable, *V*, provided that Blue follows their optimal mixed strategy, $(B_1,...,B_s)$. Therefore, *V* must be greater than or equal to the sum of the expected value produced by using the mixed strategy B_k against each Red pure strategy *i*. This rule must hold against all *i* of Red's pure strategies and is shown formally in Equation (2). The percentage utilization of pure strategy *k*, denoted by B_k, is a real number greater than or equal to zero. Equation (3) ensures that the total usage adds up to one.

2. Formulation of Zero-sum Game for Red

We can also compute the optimal mixed strategy for Red by a linear program. Let $(R_1,...,R_n)$ denote a mixed strategy for Red, where $\sum_i R_i = 1$. The decision variable R_i denotes the probability that Red uses RCIED trigger *i*, $i = 1,..,n$. Red can formulate the following linear problem to find his optimal mixed strategy and the maximum damage value.

Decision Variables:

R_i percentage use of RCIED *i*

V value of game

Formulation:

Objective:

$$\max V \tag{4}$$

subject to

$$\sum_i b_{i,k} R_i \geq V \quad \forall k \tag{5}$$

$$\sum_i R_i = 1 \tag{6}$$

where

$$R_i \geq 0$$

The maximum damage that Red can deliver is the variable, *V*, provided that Red follows their optimal mixed strategy, $(R_1, ..., R_n)$. Therefore *V* must be less than or equal to the sum of the expected value produced by using the mixed strategy R_i against each Blue pure strategy *k*. This rule must hold against all *k* of Blue's pure strategies and is shown formally in Equation (5). The percentage utilization of RCIED *i*, denoted by R_i, is a real number greater than or equal to zero. Equation (6) ensures that the total usage adds up to one.

B. OPTIMIZATION BASED ON RECENT ATTACK DATA

In classical decision theory, one is often tempted to forecast what will happen by a probability distribution and then derives the optimal strategy against that forecast. With this approach, Blue would observe over a period of time and count the number of each RCIED trigger use. Then, Blue develops an optimal jamming strategy against those observations. In other words, Blue uses recent attack data to forecast what will happen in the future. This section presents a model that allows Blue to determine the optimal strategy with this approach.

In addition to the model parameters in Section A, Blue uses recent attack data to estimate q_i, the probability that a RCIED trigger will be chosen by Red. Although Blue can simply enumerate all pure strategies found in Section III.A, compare their performances, and select the best one, we below introduce a mixed integer program that solves the optimization problem more efficiently.

To formulate the mixed integer program, we introduce three sets of decision variables. The first decision variable is the power applied to jam channel *j*, denoted by W_j. The constraint $\sum_j W_j \le t$ ensures that the jammer can allocate at most *t* Watts across all channels. The second decision variable, denoted by Z_i, indicates whether RCIED trigger *i* is jammed. Let $Z_i = 1$ if trigger *i* is jammed, and $Z_i = 0$ otherwise. The last set of decision variables is a binary $n \times m$ matrix, denoted by $[X_{i,j}]$, that tracks if frequency channel *j* is jammed for RCIED trigger *i*, $i = 1,..,n$, $j = 1,...,m$. Let $X_{i,j} = 1$ if RCIED *i* is successfully jammed on frequency channel *j*, and $X_{i,j} = 0$ otherwise. We present the formulation below, and then provide some explanations.

Sets & Indices:

i index number for RCIED triggers

j index number for frequency bands

Data:

$a_{i,j}$ $a_{i,j} = 1$ if RCIED *i* uses frequency band *j*, or $a_{i,j} = 0$ otherwise

d_i damage incurred by RCIED trigger *i*

w_i power required to jam RCIED trigger *i*

q_i percentage of RCIEDs that use trigger *i*

t total power available to jammer

Decision Variables:

Z_i $Z_i = 1$ if RCIED trigger *i* is jammed, or $Z_i = 0$ otherwise

$X_{i,j}$ $X_{i,j} = 1$ if frequency band *j* is jammed for RCIED trigger *i*, or $X_{i,j} = 0$ otherwise

W_j power assigned to jam frequency band *j*

Formulation:

Objective:

$$\min \sum_i q_i d_i (1 - Z_i) \tag{7}$$

subject to:

$$\sum_j W_j \le t \tag{8}$$

$$Z_i \le \min_{j \in S_i} X_{i,j} \quad \text{where} \quad S_i \equiv \{ j : a_{i,j} = 1 \} \qquad \forall i \tag{9}$$

$$a_{i,j} X_{i,j} w_i \le W_j \qquad \forall i \; ; \; \forall j \tag{10}$$

where:

$X_{i,j} = 0$ or 1

$Z_i = 0$ or 1

$W_j \ge 0$

Blue's objective is to minimize the expected damage caused by all RCIEDs, as shown in Equation (7). If Red uses trigger *i*, then the damage, d_i, is multiplied by zero if the RCIED is jammed or one if the RCIED is not jammed, which is taken into account by the $(1 - Z_i)$ term. The objective function is the expected damage because trigger *i* is used with probability q_i.

Three constraints support this objective function. The first constraint is the total power constraint, as shown in Equation (8), which requires the sum of all the power applied to jam each channel *j*, W_j, must not exceed the total power available to the jammer, *t*.

The second constraint is a partitioned constraint that ensures that all required channels of a trigger are jammed in order for the device to be considered successfully jammed, as shown in Equation (9). For RCIED trigger i, S_i denotes the set of channels

trigger *i* uses. For trigger *i* to be jammed $(Z_i = 1)$, $X_{i,j}$ needs to be 1 for all *j* in S_i. In Equation (9), if an instance of the observed $X_{i,j}$ is zero, then trigger *i* is not successfully jammed and therefore Z_i is also zero.

The last constraint determines if the power supplied to jam channel *j* is sufficient to successfully jam trigger *i*'s transmission on channel *j*, as shown in Equation (10). If either $a_{i,j} = 0$ or $X_{i,j} = 0$, then Equation (10) is trivially true. If both $a_{i,j} = 1$ and $X_{i,j} = 1$, then the allocated power to channel *j* needs to meet the required power to jam trigger *i*, therefore the inequality.

C. MODEL IMPLEMENTATION

This model uses Microsoft Office Excel 2007 as the primary user interface. Excel is utilized to input, store, and manage the simple data set and the output data. Data preparation, calculations, files importing, file exporting, and many other minor functions are performed in the Microsoft Visual Basic running in the background of Excel. The visual basic code calls upon the General Algebraic Modeling System (GAMS 23.0) to solve the linear and mixed integer programs. GAMS, in turn, invokes CPLEX (ILOG CPLEX 11) as the primary solver.

The data is input by the operator in Excel and appears in the form of Figure 2, the RCIED Data as seen in Section III.A. Contained with the RCIED data is the total power available to the electronic jamming system. Another important data parameter that is supplied by the operator is the number of observations used in determining the recent attack data.

Once all data and parameters are set, the first significant calculation is to determine the number of pure strategies, *s*, available to Blue. A list of all possible strategies is built. The feasibility of each strategy is determined based on the power requirements of the RCIED trigger, w_i, and the total power available, *t*. Starting with the feasible strategy with the largest cardinality and working to the smallest cardinality, we

enumerated through each of the feasible strategies and eliminate the dominated strategies. The remaining dominant feasible strategies are the set of Blue's pure strategies for the designated power level, *s*.

After determining Blue's pure strategies, the next action performed by Excel is the calculation of the payoff matrix made up of the elements $b_{i,k}$. The payoff matrix is always of dimension $n \times s$. Figure 3 contains an example of the payoff matrix.

		Blue % Use of Pure Strategy													
		2.5%	2.5%	4.2%	15.8%	7.1%	2.0%	9.8%	9.2%	0.6%	19.1%	2.5%	2.2%	8.9%	13.5%
		Payoff													
Red % Strat Use		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2.4%										1	1	1	1	1
2	2.4%						1	1	1	1			1	1	1
3	3.6%	1	1	1	1	1				1					1
4	3.6%				1	1			1	1					1
5	3.6%		1	1		1		1	1						1
6	5.4%							1.1	1.1	1.1				1.1	1.1
7	11.9%	1.2		1.2	1.2	1.2								1.2	
8	5.9%	1.2		1.2	1.2							1.2			1.2
9	7.9%		1.2	1.2	1.2							1.2			1.2
10	6.9%		1.2	1.2	1.2							1.2			1.2
11	14.6%	1.3	1.3			1.3			1.3	1.3		1.3	1.3	1.3	
12	1.7%	1.4	1.4			1.4			1.4	1.4			1.4	1.4	
13	6.8%						1.4		1.4	1.4	1.4		1.4		
14	15.8%						1.5	1.5			1.5				
15	7.6%						1.4	1.4			1.4		1.4		

Value of Zero-Sum Game = 0.46 (Less is better)

Total Power Available = 30.00

Figure 3. Payoff matrix, Blue Strategy, Red Strategy, and Value of Game.

The payoff matrix, data vectors, and scalar data are all prepared in comma separated value and text files and exported from Excel. Excel calls GAMS to solve the two-person zero-sum games from Blue and Red perspective. The value of the game, Blue's mixed strategy, and Red's mixed strategy are then imported back into Excel. Examples of these strategies and the game value are also displayed in Figure 3. The optimal mixed strategy for Red, R_i, are displayed vertically to the left. The optimal mixed strategy for Blue, B_k, is displayed horizontally across the top.

Next, the data of recent attack observations of RCIED use are generated. Based on the number of observations set by the operator, random numbers are applied to the distribution set by Red's optimal mixed strategy, R_i. The observed attack strategy, q_i, is the final proportional distribution of these observations.

As before, Excel exports the recent attack strategy. GAMS is invoked to solve for the optimal solution based on this strategy. Finally, the optimal jamming strategy based on recent attack data are imported back into Excel.

Optimal Loadset	Percentage observed by Blue	Damage	Power
0	0.0%	1	0.75
0	0.0%	1	0.5
1	5.0%	1	1
0	0.0%	1	1
0	2.5%	1	1
1	2.5%	1.1	1.75
1	17.5%	1.2	2
1	10.0%	1.2	2
1	5.0%	1.2	2.5
1	12.5%	1.2	2.2
1	12.5%	1.3	2.7
0	2.5%	1.4	2.8
0	7.5%	1.4	2.9
0	12.5%	1.5	3
1	10.0%	1.4	2.9

[Xi,j]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1
14	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Exp[Damage] = 0.35

Figure 4. Sample solution from optimization of recent attack data model.

The key data that are imported into Excel are the optimal pure jamming strategy for Blue and the expected damage value. In Figure 4, Blue's pure strategy resulting from the solution of the optimization model are in the column labeled, "Optimal Loadset." The matrix labeled, "$[X_{i,j}]$," is the map of frequency bands for each RCIED trigger, where one indicates a successful jamming while zero indicates otherwise.

Knowing the optimal mixed strategy for Red and given a pure strategy for Blue, an expected damage is calculated using the equation $(1-Z_i)\Box R_i \Box d_i$. This is the expected damage if Red is actually using an optimal mixed strategy but Blue is countering a strategy based on recent attack data.

Now, if the process of generating an attack strategy for Red and solving are performed repeatedly, we expect different results due to the nature of random numbers. The operator can enter the number of replications of this procedure.

Also, the operator can enter a range of jammer power to see how the performance varies. Chapter IV presents some numerical experiments. Additionally, if the operator wants to perform analysis on a range of jammer power, or on different sizes of attack data, the operator would also supply the starting and ending power levels, the step size for the power level, and the number of replications per power level.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NUMERICAL EXPERIMENTS

This chapter presents numerical experiments based on the model in Chapter III to answer our research question: What is the risk of using past to predict future in using jammers to deter RCIED attacks? Section A presents the main example for numerical experiments. The results of the experiments are observed in Section B and followed by a discussion in Section C.

A. THE MAIN EXAMPLE

This section presents our main example. We use open source information to estimate data we believe are representative in real world. The frequencies for each device are in their correct relative order in the electromagnetic spectrum and the correct sets of frequency ranges a particular device would operate (Marshall, How the Radio Spectrum Works) (Marshall, Tyson and Layton, How Cell Phones Work). The actual RCIED triggers in the data set were selected as the most common, and were presented in Figure 3, Chapter I. These common triggers are just an extract from the large population of possible radio frequency transmitters and receivers. The data was selected as a fair representation from the possible realm while providing a fair spectrum of the varying complexity of power and radio spectrum requirements.

For the ease of explanation, Figure 5 contains the parameters used for the model. This provides a reference throughout this discussion. These presented parameters are referenced throughout the remainder of this section. Below we further explain how we choose these numbers.

Total Power available = 30.00

				Frequency Bands in Spectrum																			
	Name	Damage	Power	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	Key Fob	1	0.75	1																				
2	Garage Opener	1	0.5		1																			
3	RC Toy 1	1	1			1																		
4	Wireless Doorbell	1	1				1																	
5	RC Toy 2	1	1					1																
6	Walkie-Talkie 1	1.1	1.75						1															
7	Walkie-Talkie 2	1.2	2							1	1													
8	LRCT Handset 1	1.2	2									1	1											
9	LRCT Base 1	1.2	2.5										1	1										
10	LRCT Handset 2	1.2	2.2											1	1									
11	LRCT Base 2	1.3	2.7													1	1	1						
12	Cell Phone 1	1.4	2.8															1	1					
13	Cell Phone 2	1.4	2.9																1	1				
14	Cell Phone 3	1.5	3																	1	1	1	1	
15	Cell Phone 4	1.4	2.9																				1	1

Figure 5. The model data.

1. Damage

The damage value of each RCIED trigger is a comparative numeric value placed on each RCIED trigger where the higher the number, the more dangerous the device. This damage value is based on the research and implications from the information presented in Section I and Appendices A, B, and C. There is no known formal presentation of a specific RCIED trigger related to the size, expected explosive potential, or amount of damage caused by an IED. Further exploration is required to link certain triggers and certain explosives to certain terrorist groups or geographic regions.

Further, reasoning through the problem says that using a garage door opener with limited short range would be detrimental in detonating a very powerful IED where the triggerman would be dangerously close. Likewise, it would make little sense to place a short-range radio controlled device as the trigger of a precision improvised explosive or a complex improvised explosive that has taken many dangerous man-hours to create and emplace. The maximum value for the damage of the data set is 1.5 and the minimum value is 1.0. This places the RCIEDs data in same order of magnitude relative value to each other. If further research provides no correlation between the IED trigger and the relative damage caused by the IED, we use a value of 1 for the damage of all RCIED triggers. However, in this model we allow a damage-RCIED dependency to account for this possibility.

2. Trigger Power

The trigger power refers to the jamming power required to jam the trigger. The power required to jam a RCIED trigger is derived through much research, observation, and calculation. Appendix C reviews some of the basic components in the research required to determine these values. In this thesis, we estimate the trigger power by surveying the product specifications.

3. Frequency Bands

The frequency bands for each device are located in the matrix located to the right of the list of RCIED devices in Figure 5. Our example includes 6 single-band devices and 9 multiband devices, including 7 dual-band devices, 1 tri-band device, and 1 quad-band device.

RCIED triggers 7 through 15 are all multiband devices. A common Motorola Talkabout radio may operate on a range of channels, but the range is typically in one band of the spectrum and this is another example of a single-band device in our data. RCIED 7 would be a dual-band walkie-talkie, also referred to as handheld two-way radio. This is usually the type radio the police and firemen use and these radios operate on two distinct sets of frequency bands. Another example of multiband devices is the cell phone, such as RCIED triggers 12-15. For example, the company LG produces cell phones that operate on dual-, tri-, and quad-bands, of which dual- and quad-band cells phones are the norm.

4. Jammer Power

The jamming power refers to the total power the jammer has available. If the jammer power is less than 0.5 Watts, then the jammer cannot even jam the Garage Door Opener—the trigger that requires the least power to jam. In other words, the problem is trivial unless the jammer power is at least 0.5 Watts.

What is the total power required to successfully jam all the devices in our example? This power can be determined in two steps. In the first step, we look at each frequency band and determine the power that is required to jam all devices on that

frequency band, in other words, the largest power among those triggers that use that band. An example is Cell Phones 1 and 2 operating in band 16. If 2.8 Watts were applied to this band only Cell Phone 1 is jammed as Cell Phone 2 requires 2.9 Watts. Consequently, it requires 2.9 Watts to jam band 16 entirely. In the second step, we add these power numbers across all frequency bands, which results in 45.2 Watts in our example.

If the jammer power is 45.2 Watts or more, then the problem also becomes trivial because the jammer can jam all triggers. In Section B, we use 30 Watts as the jammer power and make observations at this fixed total power value. In Section C, we vary this jammer power to observe how it affects the jammer performance.

B. DESIGN OF EXPERIMENT

Upon completion of the data entry, the first step is to compute the optimal mixed strategy for both Blue and Red, as discussed in Section III.A. The value of the zero-sum game—denoted by *V* throughout this chapter—will be used as benchmark in order to assess the optimization approach when Blue uses recent attack data to design his jamming loadset.

To determine the effectiveness of the optimization approach based on recent attack data, we use Monte Carlo simulation to generate RCIED attack data. For example, we can generate 40 RCIED incidents based on Red's optimal mixed strategy, as shown in Figure 6. After the final tally, the counts are each divided by the total number of observations—in this case 40—as shown in column three in Figure 6. If Blue believes that Red will choose RCIED triggers using these percentages, then Blue can use the mixed-integer program—detailed in Section III.B—to find the optimal pure strategy. The expected damage computed with this approach—denoted by *H* throughout this chapter—represents the damage that Blue believes based on the optimization approach.

The actual damage, however, is not equal to *H*, because column 1 and column 3 are usually not the same in Figure 6. To compute the actual damage for a pure strategy, we can simply compute the expected damage for that pure strategy against Red's optimal mixed strategy. This actual damage will be denoted by *U* throughout this chapter.

	Red's optimal mixed strategy	Counts over 40 attacks	Percentage observed by Blue
1	2.4%	0	0.0%
2	2.4%	0	0.0%
3	3.6%	2	5.0%
4	3.6%	0	0.0%
5	3.6%	1	2.5%
6	5.4%	1	2.5%
7	11.9%	7	17.5%
8	5.9%	4	10.0%
9	7.9%	2	5.0%
10	6.9%	5	12.5%
11	14.6%	5	12.5%
12	1.7%	1	2.5%
13	6.8%	3	7.5%
14	15.8%	5	12.5%
15	7.6%	4	10.0%

Figure 6. Build of Red's observed strategy of recent attacks.

For a specific jammer power, the value of the game (*V*) does not change regardless of the number of recent attack data observed. The process of assigning random numbers to determine the recent attack data that Blue perceives as Red's strategy is simulated multiple times. Each time we simulate recent attack data, and compute the expected damage Blue perceives (*H*) as Blue computes his optimal loadset based on the attack data. Additionally, we determine the damage value if Red is actually using his optimal mixed strategy (*U*).

C. RESULTS AND ANALYSIS

The main purpose of this section is to compare *V*, *H*, and *U* defined in Section B. In Section 1, we compare *H* with *V* and discuss Blue's heightened expectation. In Section 2, we compare *U* with *V* and discuss Blue's under performance.

1. Heightened Expectation

Further continuing our example, we have a jammer with 30 Watts of power available and the data remains unchanged for our 15 RCIED triggers. What happens

when we allow Blue different numbers of observations in which to build their recent attack data file? How influential is the depth of the recent attack file on Blue's responding strategy?

Blue is allowed 10, 20, 40, 80, and 160 observations in which to formulate the recent attack RCIED trigger usage for Red. This becomes what Blue thinks Red's strategy is through Blue's observations. Figure 7 compares some basic values found for trials all at 30 Watts for our data set based on allowing Blue these five different levels of observation, listed in the first column.

Comparison of Observation at 30 Watts-Heightened Expectation					
Number of Observations	Number of Replications	Value of Game [V]	Heightened Expectation Damage Value [H]	Ratio of Difference of Expectation from Value [(H-V)/V]	Ratio of Standard Error of H to H [(SE_H/H)]
10	6400	0.463	0.085	-81.588%	1.100%
20	1600	0.463	0.185	-59.967%	0.925%
40	400	0.463	0.271	-41.545%	0.969%
80	100	0.463	0.328	-29.044%	1.093%
160	25	0.463	0.378	-18.299%	1.521%

Figure 7. All observation values at 30 Watts for heightened expectation (less damage is better)

The damage value that Blue expects (*H*) as a result of their observation is highly dependent upon the number of observations. Additionally, the deviation between the value Blue expects and the game-theoretic value are reversely proportional.

If we first look at the row of results based on 10 observations at 30 Watts of power. If the attack data based on these 10 observations is generated and solved over 6,400 replications, we find that Blue would expect a damage value of 0.085, the 4th column of Figure 7. The 5th column shows that if we compare this expected damage to the game theoretic value we find that there is an 81.588% difference in the solution. The -81.588% demonstrates that the damage value, where less is better, is lower than the value of the game. Simply put, based on 10 observations, this example results in an 81% over inflation of the expected damage from the game theoretic solution.

The last column of Figure 7 is the ratio of the standard error of the expected damage to the expected damage. The largest gap encountered for these values is 1.521%. Using a goal of 1% for the standard error ration as an acceptable range to evaluate the expected damage calculation allows the simple conclusion that the quality of the approximation for the enemy solution increases as the number of observations increases. This is seen by the requirements for more replications for smaller numbers on observations to achieve a quality result. Also, this is observed by the percent difference of the expected damage and the value of the game. This gap, or percentage difference, decreases as the number of observations increase.

Next, we vary the jammer power over a range from 0 Watts to 46 Watts. After assigning a step size of 0.5 Watts and allow Blue 40 observations to predict Red's strategy, the resulting plot in Figure 8 is achieved by using 100 replications for each power step.

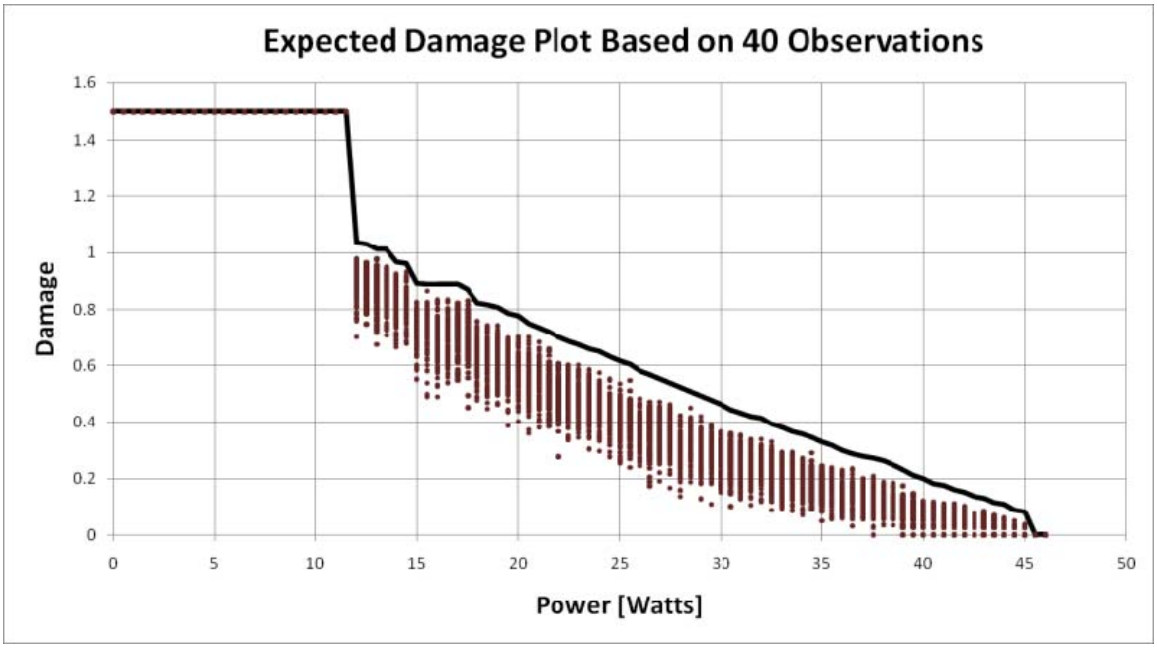


Figure 8. Data plot for heightened expectation over full range of power for 40 observations with 100 replications

Some very insightful observations are made from this plot of data in Figure 8. Each dark red dot represents the expected damage by Blue based on the results of the perceived Red strategy—in this case based on 40 observations. The solid black line is the game-theoretic solution. From this data plot, it appears that Blue can do at a minimum the same as the game-theoretic value and in most cases better. This plot will mislead Blue into the expectation of performing better through the use of recent attack data than through the game-theoretic approach. Additional data plots for 10, 20, 80, and 160 observations are available in Appendix D.

The next insight to observing what the game value and the expected value are predicting across the range of power values. Note, in Figure 8 and the remainder of the plots and graphs of this thesis, the expected damage between 0 Watts and 12 Watts is a straight horizontal line located at 1.5 damage. To understand this, first note that at 0 Watts, we expect no reduction in damage and the strategy for Red that produces the most damage is cell phone 3, RCIED trigger 14 (Refer to Figure 5). The minimum power for Blue to start jamming a known RCIED trigger is 0.5 Watts. We do not see any movement in the damage function until 12 Watts, because cell phone 3 is a quad band device requiring 1.5 Watts of power per band to negate the 1.5 damage it produces. So, until the jammer has 12 Watts of power, it cannot jam cell phone 3 and because it produces the most damage becomes Red's pure strategy.

The maximum power required to jam all devices is 45.2 Watts. For the maximum power, the damage converges to zero. Additionally, with this data, the values between 12 Watts and 45.2 Watts become very interesting as there are pairs of mixed strategies for both players produced by the game theoretic model and through Blue's observations over multiple replications of the model based on recent attack data determine varying values of damage.

From the 100 replications presented in Figure 8, we can determine the expected damage value and the 95% confidence intervals for the power range. Using the data plotted in Figure 8, the expected damage for Blue based on history is the dark red solid line in Figure 9. The dark red dashed lines are the upper and lower 95% confidence interval.

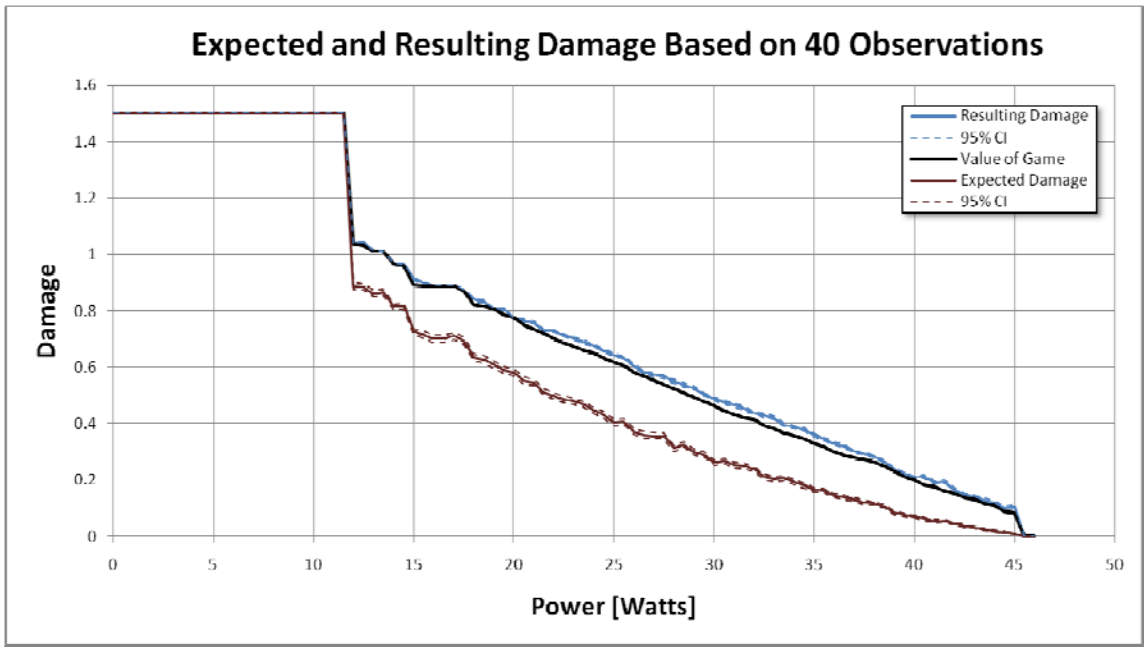


Figure 9. Expected damage and actual damage with confidence intervals

2. Under Performance

This section explores the resulting damage based on the pure strategy Blue, determined through the solution of the model based on past attack data. The blue line in the above figure represents this resulting damage.

The solution of the model for the given recent attack representation of the strategy Blue perceives Red is using produces the damage value Blue expects to receive and produces a pure strategy for Blue. If we compute the resulting damage through the use of this pure strategy by Blue against the optimal mixed strategy by Red we find another damage value. This damage value demonstrates Blue's actual damage received based on using the past to predict the future. In most cases, this damage is more than expected and Blue underperforms.

Figure 10 is similar to Figure 8, except it compares the underperformance (U) experienced by Blue by basing their strategy on the recent attack observations of Red's use of RCIED triggers. These comparisons are all made for 30 Watts of power and show the effect of the 10, 20, 40, 80, and 160 observations used to determine the past. The underperformance shows similar trends to the heightened expectation.

Comparison of Observation at 30 Watts-Under Performance					
Number of Observations	Number of Replications	Value of Game [V]	Under Performance Damage Value [U]	Ratio of Difference of Performance from Value (U-V) / V	Ratio of Standard Error of U to U [(SE_U / U)]
10	6400	0.463	0.592	27.895%	0.151%
20	1600	0.463	0.518	12.011%	0.226%
40	400	0.463	0.489	5.699%	0.287%
80	100	0.463	0.477	3.051%	0.380%
160	25	0.463	0.470	1.538%	0.461%

Figure 10. All observation values at 30 Watts for under performance (less is better)

The value of the game (*V*) remains deterministic, independent of the number of observations. The damage value that Blue incurs, under performance of the Blue pure strategy (*U*), based on recent attack data is highly dependent upon the number of observations. Additionally, the gap between the value Blue expects and the game-theoretic value are reversely proportional to the number of observations. As we would expect, 10 observations produces a poor estimate of the past and likewise produces the largest gap between *U* and *V*.

Column 5 shows that if we compare this expected underperforming damage value to the game theoretic value, we find that there is a 27.985% difference gap. The percentages here are all positive, meaning that the actual damage is higher than the value of the game. Simply put, based on 10 observations this example results in a 28% under performance from the game theoretic solution.

Observing the standard error values for the calculation of the underperformance encountered by Blue, results in the largest gap encountered for these values, that of 0.461%. Using a goal of 1% for the standard error ration as an acceptable range to evaluate the expected damage calculation, allows the simple conclusion that the quality of the approximation for the enemy solution increases as the number of observations increases.

Again, we observe the total power available to a jammer over a range from 0 Watts to 46 Watts. Performing 100 replications for each power step, a step size of 0.5 Watts, and Blue making 40 observations, to predict Red's strategy results in the plot in Figure 11.

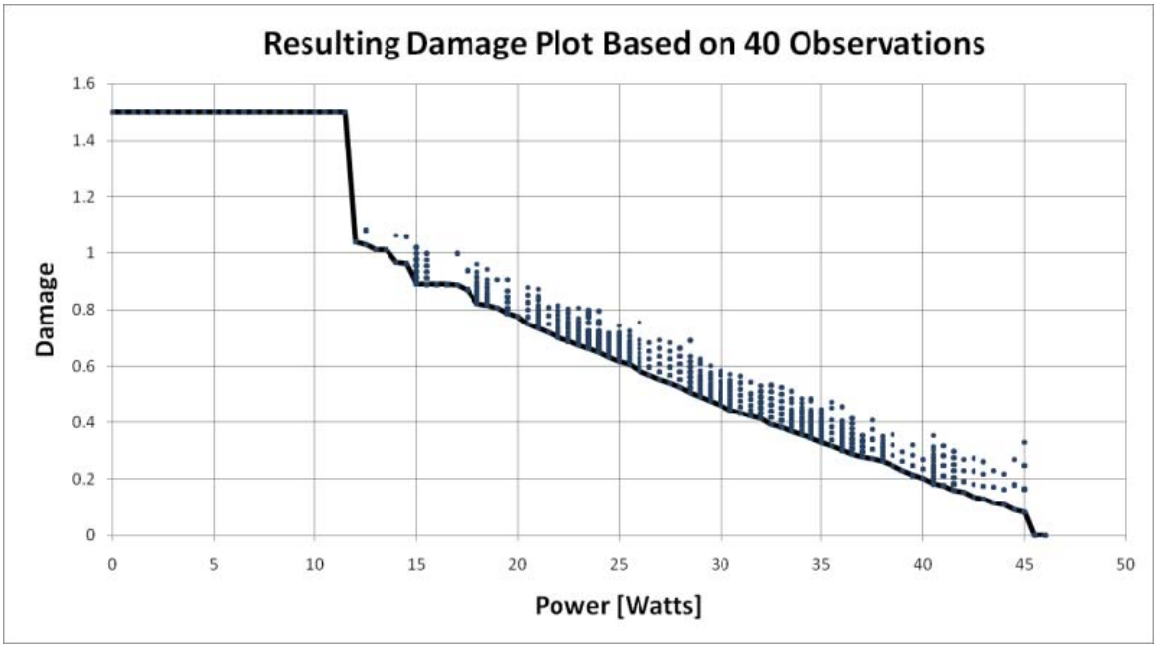


Figure 11. Data plot for under performance over full range of power for 40 observations with 100 replications

From this data plot in Figure 11, Blue underperforms compared to the game value and the value they expected to incur based on Red's observed strategy. This should be eye opening for Blue as the best they can do is the game-theoretic value and in most cases they perform worse. This plot introduces Blue to the mistake of using past to predict future. The value you expect to achieve is not the value you will get from a devious and intelligent enemy. Additional data plots for 10, 20, 80, and 160 observations are available in Appendix D.

From the 100 replications presented in Figure 11, we can determine the expected underperformance value and the 95% confidence intervals for the entire power range.

Using the data plotted in Figure 11, the expected damage for Blue based on history is the blue solid line in Figure 9. The blue dashed lines are the upper and lower 95% confidence interval.

Based on 100 repetitions of generating the recent attack data, we can also compare the number of observations, namely 10, 20, 40, 80, and 160 observations and observe the values of damage expected and resulting compared to the damage value found through the game theoretic model. Figure 12 displays the each observation level. The black line represent the game value, the red lines the expecting damage value and the blue line the actual damage Blue incurs. This series of charts show trend of damage over full range of power that re-enforces the observations made through the analysis of the gaps at 30 Watts.

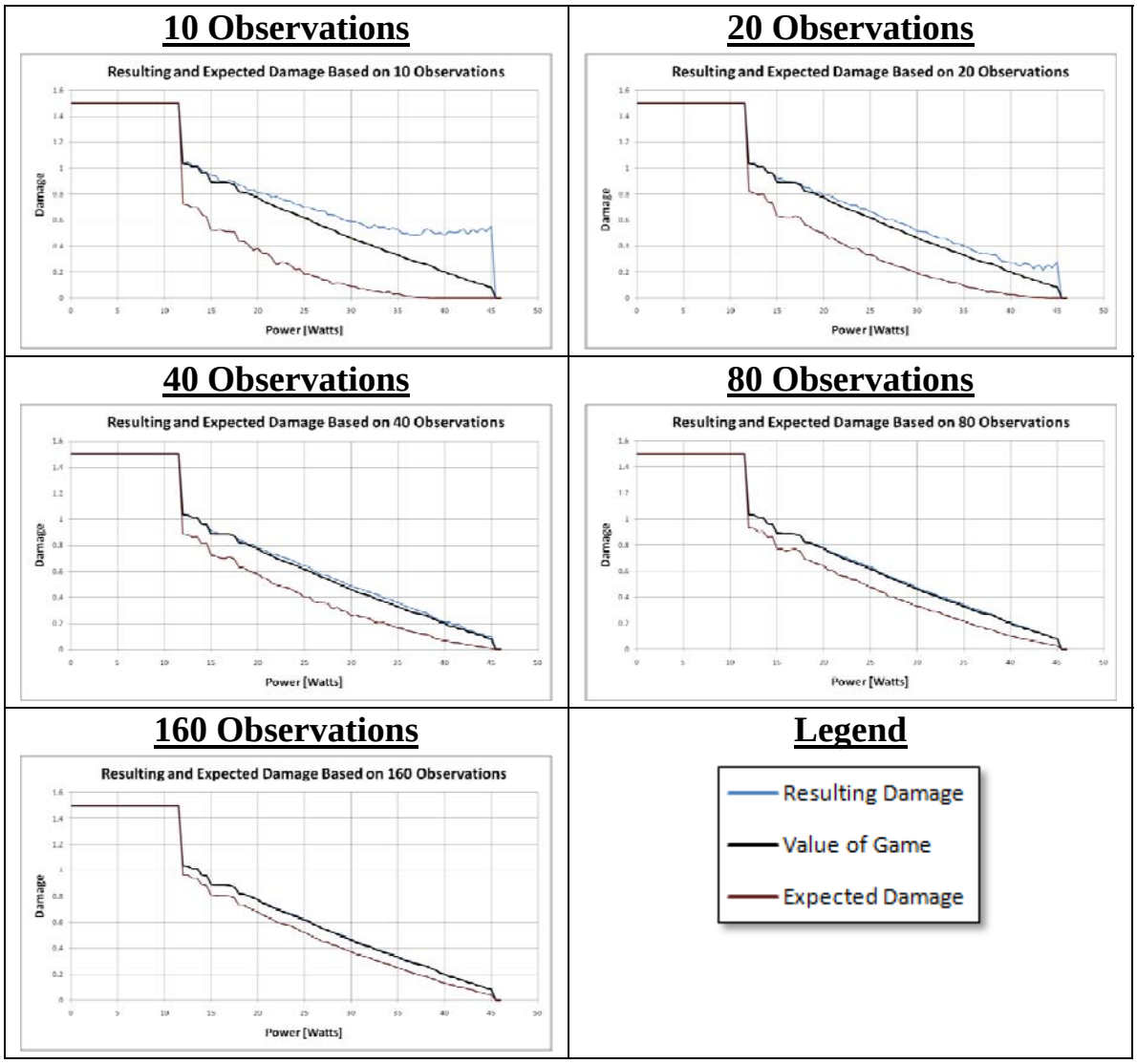


Figure 12. Resulting and expected damage based on 10, 20, 40, 80, and 160 observations.

From Figure 12, as the number observations increase, the gap between both the resulting and expected damage and the value of the game increases over the non-trivial range of power. As the number of observations increases, Blue is more likely to observe a better approximation of Red's strategy. With a more accurate observation of Red's strategy, the use of recent attack data provides a better quality solution as is seen by the reduction in the gaps with the increase in observations.

D. DISCUSSION

When using past to predict future, Blue tends to be overly optimistic in predicting the outcome and the result is a heightened expectation. In addition, Blue is likely to underperform. The performance gaps depend highly on the number of observations used to collect recent attack data, where the more observations, the less the gap.

Further, we have stated that Red is an intelligent enemy. What would happen if Red did not follow their optimal mixed strategy for a couple of months? This counter-intelligence could result in the devastating effects for Blue if Blue designs jamming loadset based on recent attack data. Say that Red has a surplus of garage door openers and decides to use only garage door openers for the next two months, although, garage door openers have a limited range and the insurgents would have to use small sized IEDs they continue with this plan. If Blue uses attack data based on the last month, their pure strategy is to jam the garage door openers. As no other trigger is used during the time period the recent attack data is observed, Blue is susceptible to any other RCIED trigger than a garage door opener. As Red is intelligent, for the third month they deploy quad band cell phones attached to very large IEDs that devastate Blue.

This is an extreme and very unlikely example, but this points out another concern and shortfall on determining an optimal jamming loadset based on recent attack data. The lack of observance highly effects the selection to jamming each RCIED.

The robust solution provided by the game theoretic solution will provide the balanced solution based on enemy and friendly capability rather than observation and perception. Additionally, using the optimal mixed strategy provides Blue a guarantee that the maximum damage that they will incur is the value of the game. If Red deviates from the optimal mixed strategy, Blue will encounter an even better result by incurring less damage. Blue's use of the optimal mixed strategy defeats Red's efforts of subversion and misdirection.

V. CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the conclusions in section A. Additionally, addressed in Section B are recommendations into areas of further research and development.

A. KEY FINDINGS

In this thesis, we developed a mathematical model for the combat between RCIEDs and electronic jammers. Red chooses a RCIED to attack, while Blue designs a jamming loadset to minimize the expected damage. We applied a game-theoretic approach to derive the value of the game, and then use simulation to estimate Blue's performance if Blue chooses the jamming loadset based on observation of Red's recent attack data.

The numerical experiments showed that when using the past to predict the future, Blue tends to be overly optimistic in its predictions of jammer effectiveness. More precisely, the minimal damage Blue is led to believe based on recent RCIED attack data will be higher than the actual damage if Red uses the optimal mixed strategy. The heightened amount of over estimation is highly dependent upon the recent RCIED attack data.

In addition, Blue's optimal strategy based on recent RCIED attack data tends to underperform. That is, the optimal pure strategy perceived by Blue based on recent attack data will always underperform compared to the optimal mixed strategies determined through the game-theoretic approach. The difference between the underperformance and the value of the game also depends highly upon the quality of the data provided to approximate Red's strategy.

Another risk of using past to predict future is the possibility that Red can purposely mislead Blue. For example, Red can solely use garage door openers for a period of time. If Blue adopts a jamming loadset specifically designed to counter garage door openers, then Red can shift to the heavy use of cell phones where Blue is now more susceptible.

To reduce these aforementioned risks, Blue should adopt the optimal mixed strategy produced by the game theoretic approach. Blue's optimal mixed strategy is randomized, which makes it difficult for Red to predict and manipulate. Blue's optimal mixed strategy is also robust, in a sense that if Red deviates from his optimal strategy by using a suboptimal strategy, Blue performs even better than expected.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

This thesis creates a model that becomes the foundation for additional research to follow. The two main recommended areas to grow from this research are in further modeling and data collection.

On modeling, the next two steps to grow from this model naturally are first to extend the model to incorporate reactive jamming. For reactive jamming it becomes important to consider the operational environment and take into account the radio traffic in the background. Blue's optimal jamming strategy in a sparsely populated desert can be very different from a densely populated urban area.

Another research direction on modeling is to incorporate multiple jamming modules. If separate modules with their respective frequency ranges, power specifications, and whether it is active jamming or reactive jamming, then how does Blue use them optimally to minimize RCIED attack risk? Does the conclusion in this thesis carry over to this case?

On data collection, much work needs to be done. In this thesis, we used mock up data to run our numerical experiments. To use the methods proposed in this thesis in the theater, one needs to survey all RCIED triggers available in each geographical area. The compilation of all trigger technical specification—such as power usage, frequency, and damage—to feed into our model can be a daunting task itself.

A couple of ideas on further modeling and data collection are just the surface of this intoxicating and in-depth problem. As this problem is researched further, the pioneer need not fear the fall, rather live for the adventure of discovery.

APPENDIX A: IED OVERVIEW

The intent of this appendix is to overview concepts in depth; define what an IED is, how it is employed, organizations formed to combat this device, and the future implications.

A. GAME THEORY

Game theory is defined as the study of how players should rationally play games. Each player is forced to choose a strategy they think will provide the best outcome. Although each player makes choices, they must keep in mind the choices of the other player. These sequence of choices force each player to develop a strategy based on the outcome of their choice with respect to their opponent's choice. Each would like the game to end in a desired outcome which gives as large (or small) a payoff as possible. Game theory further defines rules and principles to ensure an optimal strategy (Straffin 3). An in depth explanation of the game theory approach is found in Chapter III.

As IEDs are built with a specific target in mind out of non-traditional materials and as they become more complex they become very hard to detect and defend against. IEDs cover a broad spectrum, to say the least, because by definition they can take on almost any shape or form. With almost infinite possibilities in configuring an IED, there are three distinct categories, each designed for a specific tactical purpose; the package type IED, vehicle-borne IEDs (VBIED), and the suicide bomber (Improvised Explosive Devices (IEDs)/Booby Traps). Commonality is also found among the components of an IED.

B. BEHIND THE IED

1. Components of an IED

All IEDs share four major components; the power source, the trigger or switch, the detonator and the main charge (Australian Government, Department of Defense 1). The following are explanations of each component:

• Power Source: Typically a battery or anything that can provide energy to power the IED.

• Trigger/Switch: The mechanism that initiates the IED. This mechanism can be a simple switch, a timer, a pressure plate, a command wire, or a radio controlled device. The six main triggers/switches are pressure plates, cell phones, command wire, low-power radio-controlled, high-power radio-controlled and passive infrared (Atkinson 4).

• Detonator: The small explosive charge, usually a blasting cap, that initiates the main charge after receiving input from the initiator and power from the power source.

• Main Charge: Homemade explosive or military ordnance, such as artillery rounds, initiated in an unconventional manner (Australian Government, Department of Defense).

Figure 13 demonstrates the common configuration and components of an IED. The insets contain examples of the power source, trigger/switch, detonator, and the main charge. Note the main charge can be engineered from unexploded ordnance (UXO) or a recovered mine (Improvised Explosive Devices (IEDs)/Booby Traps).

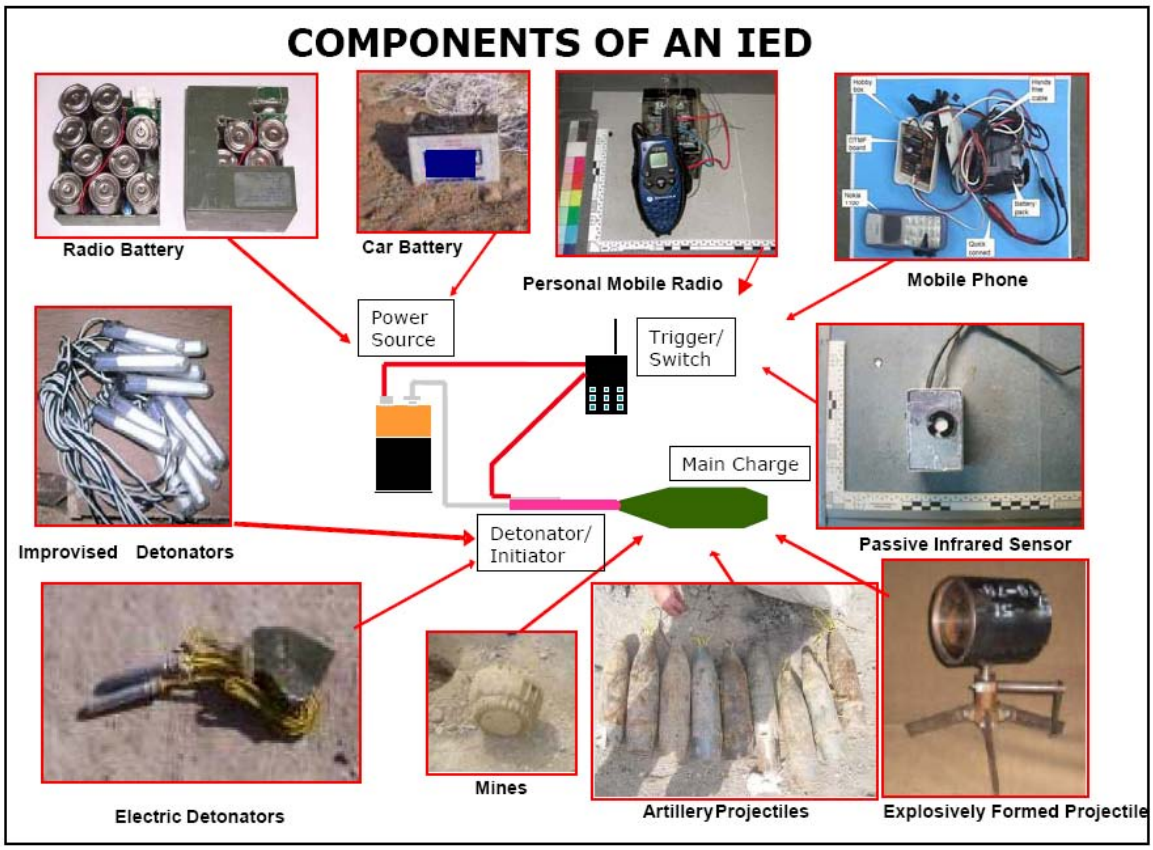


Figure 13. Components of an IED [From (Australian Government, Department of Defense)]

2. Current Employment Techniques

Having defined what an IED is and what the basic components are, the next step is to introduce some of the common tactics and techniques of employment. This section will primarily focus on the package type IED emplaced to disrupt ground forces. These techniques are some of the more common and the list is not inclusive because as the IED has infinite configurations of components, it also has just as many techniques of emplacement.

IEDs are often found along main supply routes, alternate supply routes, and unimproved roads in the medians, above ground and buried below ground (CTF-7 CALL Representative 2). These devices are hidden behind guard rails, in roadside trash, and

even the carcasses of dead animals (D'Alessio). IEDs are disguised to look like any object, limited only by the imagination and capabilities of the bomb maker (CTF-7 CALL Representative 4).

3. IED Classifications

There are two classifications of IED types; by delivery mechanism or by type of trigger/switch. The more direct classification of the two is by delivery mechanism. An incomplete list of IEDs classified by delivery mechanism are package, vehicle-borne (VBIED), boat-borne, animal-borne, house-borne and suicide bombers. Classification by delivery mechanism leads to tactics and techniques to prevent and deter. Likewise, classification by switch/trigger looks at the same IED dilemma from a different viewpoint.

Anything that is capable of closing a power loop or making an electrical connection can be utilized as a switch/trigger. Through the leverage of the vast and expanding consumer electronics market, insurgents are able to initiate IEDs that are simple, inexpensive, and catastrophic (Atkinson 4). The following are explanations of IEDs classified by trigger/switch:

• Command Wire Improvised Explosive Device (CWIED) - An IED using a wire connected to the trigger, detonator, or battery to allow the insurgent to control the instant of initiation. The wire effectively becomes the switch.

• Radio Controlled Improvised Explosive Device (RCIED): The trigger is a radio transmitter and receiver link. A few examples are car alarms, wireless door bells, cell phones, pagers and walkie-talkies.

• Victim-Operated Improvised Explosive Device (VOIED): These are designed to function upon contact with a victim; also known as booby traps. Some examples of VOIEDs are tripwires, pressure plates, and tilt rods. Note that one controversy is whether or not victim operated devices are, or are not, “booby traps.”

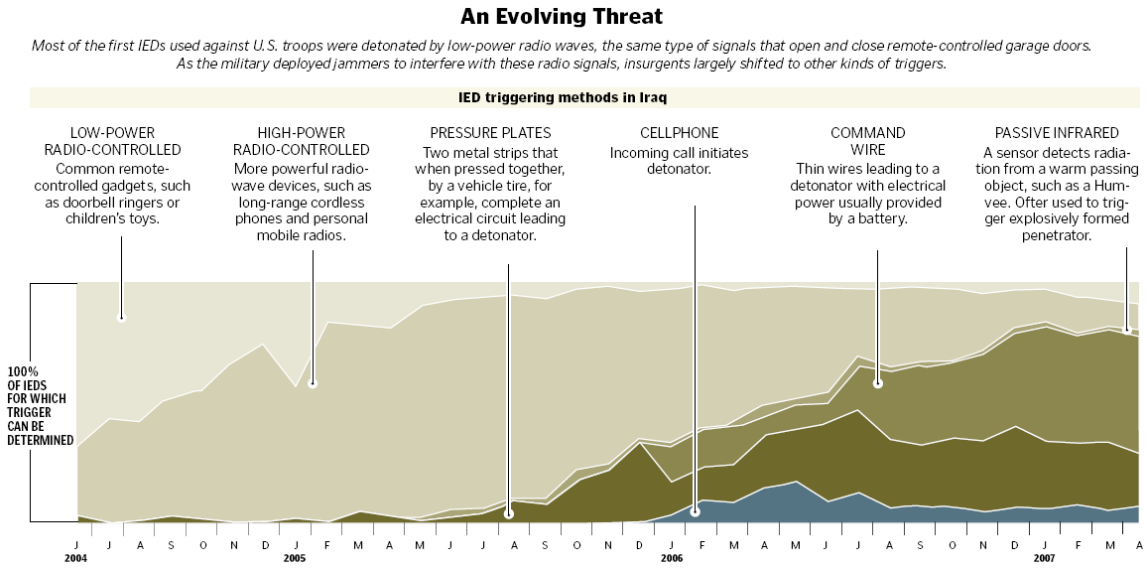


Figure 14. The Evolving Threat of IEDs by Trigger [From (Atkinson 15)]

The classification of IED by switch/trigger for the six most common triggers observed from June 2004 to April 2007 is found in Figure 14. Note the changing techniques over time. The higher technology cell phones emerge as well as the simplest technology of the command wire. This is an example of where the insurgents adapt by the IED trigger changing over time.

A few examples of possible RCIED triggers/switches are found in Figure 15 (CTF-7 CALL Representative 5) (Miles 10-63). These radio controlled devices are each labeled: A – RC Unit From Car Alarm, B – Wireless Doorbell, C – Garage Door Opener, D – LRCT Base Station, E – LRCT, F – Cell Phone, G – Walkie-Talkie, H – Radio Controlled Toy, and I – Cordless Telephone.

Figure 15. Common Radio Controlled IED Triggers

4. Current Threat

Current use of IEDs have been compared to the use of Artillery as they become a combat multiplier for the insurgent. But, IEDs do not manufacture themselves. It takes an IED cell to support an IED attack. These network structures defy identification in Iraq, Afghanistan, and the other insurgencies throughout the world (Meigs). What are the expected components of these networks?

A typical IED cell is suspected to contain five to ten people and the organization is described as fluid and decentralized. The main roles including a financier that provides the funds, bomb maker that makes the IED, emplacer that installs or places the IED, triggerman that initiates the IED, spotter who assists the triggerman in locating the target, and often a cameraman to record video footage of the incident. Videos of exploding U.S. vehicles and dead Americans are distributed via the Internet to win new supporters (Wilson 2). In 2007, there where an estimated 169 cells in Iraq alone (Atkinson 14).

As expected, the task is not only to defend against the IED. A parallel task is to eliminate the network. Attacking or neutralizing the shadowy network is just as important as defending against the IED, but it involves a separate set of complex issues and challenges that are outside the scope of this research (Atkinson 3). But, these are all intricacies of an insurgency that we have yet to define.

5. Insurgency and Counter-insurgency

The doctrinal definition of insurgency "is an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict. Stated another way, an insurgency is an organized, protracted, politico-military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control." (U.S. Army/Marine Corps 2).

Doctrinally from FM 5-34, counterinsurgency is defined as "military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat an insurgency." (U.S. Army/Marine Corps 2)

Throughout history, insurgents have commonly utilized terrorist and guerilla tactics. This leads to no surprise that the IED has become a common and preferred weapon of current insurgencies (U.S. Army/Marine Corps 18). The prowess of the U.S. Armed Forces in combat operations will logically lead insurgents opposed to the U.S. to asymmetric approaches instead of challenging the U.S. Forces in direct engagements. An insurgency needs to adapt to succeed against a force superior in resources and technology (U.S. Army/Marine Corps 3-4). The adaptive asymmetric weapon of today is the IED.

C. HISTORY OF THE IED

1. Current Effect of the IED

The IED is the deadliest threat to military personnel supporting Operation Enduring Freedom in Afghanistan and Operation Iraqi Freedom in Iraq (U.S. House of Representatives 15). In support of the global war on terrorism, from October 7, 2001 to May 2, 2009, there have been 209 deaths due to IEDs of the total of 452 deaths (~46.2%) in support of Operation Enduring Freedom and 2,164 deaths due to IEDs of the 3,430 deaths in support of Operation Iraqi Freedom (~63.1%) (Defense Manpower Data Center). The use of the IED has grown to unmatched numbers in use against military forces and has been termed the insurgent's "Weapon of Choice." (Australian Government, Department of Defense) Figure 16 shows the number of IED incidents in Iraq from the onset of the war. From this chart the growth of their use increase from 2003 to 2007 where in mid-2007 there were in excess of 2,500 IED incidents in a month.

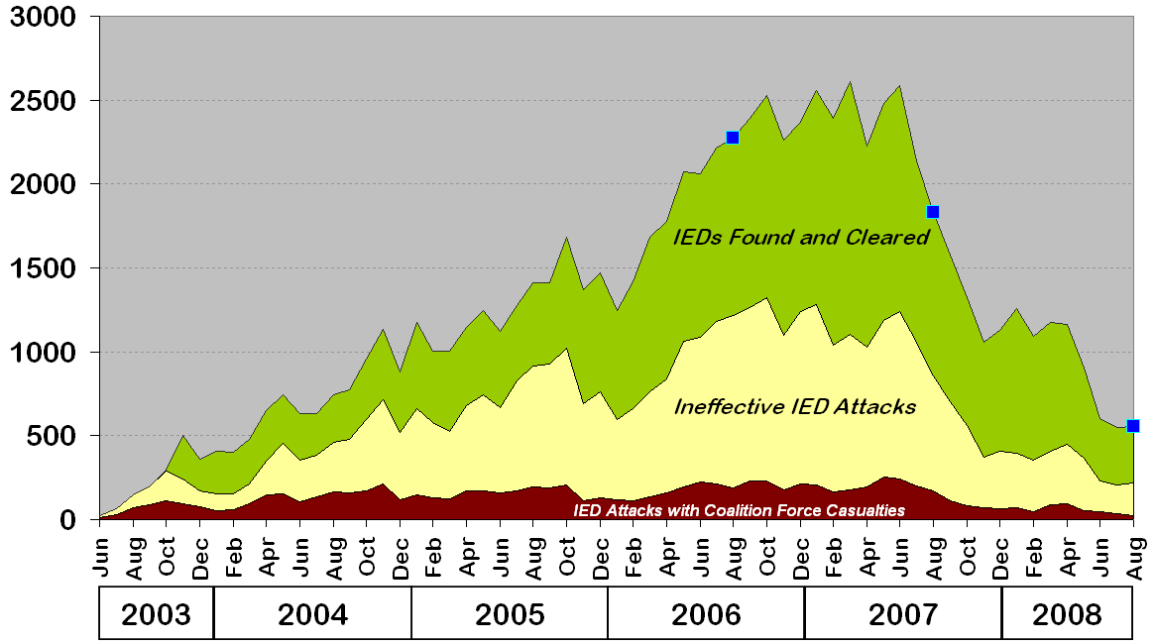


Figure 16. IED Incidents in Iraq [From (U.S. House of Representatives 43)]

Similar to Figure 16, Figure 17 shows the number of IED incidents, but it shows the monthly trend for Afghanistan from 2005 to 2008. The interesting conclusion drawn from looking at both figures is that although the magnitudes of the number of IEDs are on

different scales for incidents per month, as the IED incidents were showing a decreasing trend mid-2007 through 2008 in Iraq, the number of IED incidents are overall is increasing in Afghanistan through the same time period.

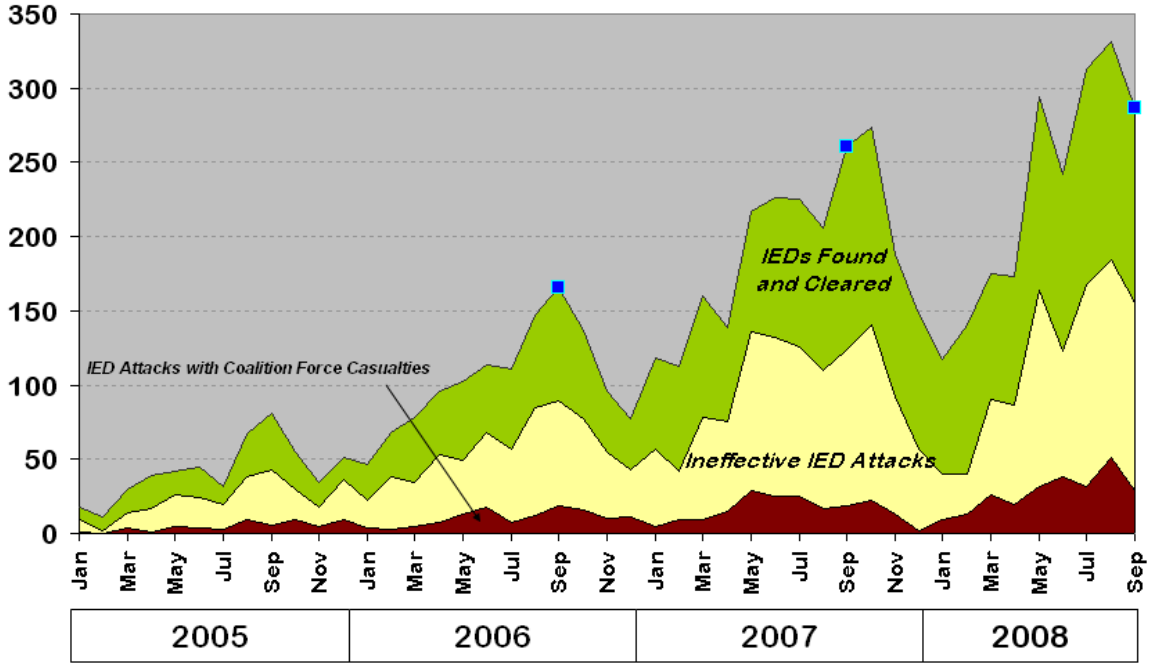


Figure 17. IED Incidents in Afghanistan [From (U.S. House of Representatives 44)]

On the other hand, before drawing too many parallels to the increase in one area and a decrease in another, we must compare the magnitude. In Iraq, the numbers decrease from 2,500 per month in August 2007 to level of 500 per month in August 2008. In Afghanistan, the comparative increase in August 2007 is approximately 215 IED incidents per month to approximately 325 per month in August 2008. Many conclusions can be drawn from these comparative numbers and trends, but one is certain in that the insurgents have found a tactically effective weapon and continues to explore its use while exploring our weaknesses.

2. Origin of the Acronym IED

The term Improvised Explosive Device and the acronym IED have become common household phrases through their use in the media. But, where did the term originate? Although the IED is primarily related to the current conflicts in Iraq and Afghanistan, the exact use of the term IED is brought to fruition early in Operation Iraqi

Freedom. On 21 March 2003, troops crossed into Iraq beginning Operation Iraqi Freedom. On 1 May 2003, President George W. Bush declared, "major combat operations in Iraq have ended." (Associated Press; USA TODAY Research and Wire Reports) But, we would soon learn that the loss of U.S. troops would drastically increase as the war does continue against an insurgency rather than a traditional combat force.

In Baghdad on Memorial Day, 26 May 2003, while conducting an escort mission of large logistics trucks, PFC Jeremiah D. Smith was killed when his vehicle was hit by the blast of unexploded ordnance. In May 2003, the term IED was not used but this soldier is most likely the first combat loss to an IED in OIF (Associated Press; USA TODAY Research and Wire Reports). The next combat loss occurred on 28 June 2003 with the loss of SGT Timothy M. Conneway. SGT Conneway died of wounds suffered on 26 June 2003 when his vehicle was hit by an explosive device in Baghdad (Associated Press; USA TODAY Research and Wire Reports). This would be the second casualty to an explosive device in one month and within two months of the Presidents declaration to the conclusion of the major combat operations.

A little less than a month later, on 21 July 2003, again in Baghdad, a convoy is hit by what is released as an "improvised explosive device." This is the first official statement where the term IED is used as the official cause. Unfortunately, this device was the cause of death for Cpl. Mark A. Bibby (Associated Press; USA TODAY Research and Wire Reports).

Through the remainder 2003, IEDs continued to grow in number and one common thread among them was their use of adapted military explosives, primarily artillery shells. The direct conflict with Iraqi troops was over, but the insurgency had obtained a major cache of ordnance to create IEDs from this surplus of ordnance where these pilfered explosives appeared in the growing number of IEDs. One of the main supply routes from Kuwait to Baghdad, Route Tampa, was one of the most common locations for IEDs in 2003. On 29 July 2003, three artillery shells wired to a washing machine timer were discovered west of Taji, just eight days after the loss of Cpl. Bibby. Soon, other initiators would be discovered to include egg timers and rudimentary remote control devices of children's toys, wireless door bells, and car key fobs (Atkinson 8).

The enemy's grasp of the potential of these devices was growing and their tactics were evolving. The frequency of the IEDs used continues throughout 2003 where at least 77 U.S. casualties were caused by IEDs and the U.S. lost the most, 20, in December (Associated Press; USA TODAY Research and Wire Reports). A new weapon of the insurgency in Iraq is born; silent, demoralizing, and extremely effective.

3. IEDs Throughout History

Are IEDs a new tactical concept? No, IEDs have been used throughout recent history; just the term of improvised explosive device is new. The meanings and differences in names to describe the different types of explosive devices have differed though time and caused confusion through historical cases and their employment today.

The EOD community has used the term IED since the early 1960's to describe these types of explosive devices. Further, although the term IED was not used, there is evidence of their tactical use dating back to 1943. Belarusian Guerrillas used command-detonated and delay-fused IEDs to derail thousands of German trains in World War II. Other examples can be found of the now termed IED use in Vietnam, Northern Ireland, Afghanistan (against USSR in 1979), Lebanon, and Chechnya. Improvised techniques in employment of explosive devices can be traced back through the American Civil War, World War I, Korean War, and the earliest document use of an IED, by today's definition, being 1581 during the siege of Psk'ow (Jones 11-15).

Throughout the world, IED attacks are not a new occurrence. For over nine years the Hezbollah, an Islamic Shia political and paramilitary organization, used IED tactics in Israel and southern Lebanon. The Hezbollah, literally meaning party of God, is viewed as one organization responsible for passing IED techniques through Iran to Iraq. Chechen Rebels utilized IED for over seven years in their struggles in Chechnya and Russia. Today, the Taliban and Al Qaeda forces have at least seven years experience of their employment in Afghanistan (Keesee 4).

The Irish Republican Army (IRA) has over 35 years of tactical experience in utilizing IEDs throughout Northern Ireland. During this time British troops encountered

more than 7,000 IEDs. In comparison, what the British forces encountered over a 35 year span is less than current troops in Iraq and Afghanistan encounter in just nine months (Atkinson 4).

IEDs with Radio-Controlled triggers account for only 10% of all the IEDs encountered. RCIEDs, on the other hand, account for the majority of U.S. casualties due to IEDs. Through the employment of over 30,000 jammers, U.S. service members have begun to greatly reduce the capabilities and success rate of the RCIED (Atkinson 5).

APPENDIX B: OVERVIEW ON JAMMING TECHNOLOGY

A. GROUND JAMMING SYSTEMS

This next section is an overview on information gathered about different ground jamming systems. These systems, by name, include the following:

Warlock: The Warlock Force Protection System consists of three versions, Blue, Green, and Red, manufactured by EDO Corporation and ITT Electronic Systems. The Warlock was originally designed to defeat proximity fused indirect fire munitions and has a second capability of jamming enemy communication devices. The Warlock systems have gone through software and hardware revisions to improve the frequency ranges and capabilities (SPG Media Group Limited).

Warlock Green: The Warlock Green is a member of the CREW family derived from the Shortstop counter artillery system through the use of changed computer components and an adapted antenna. The final product was a vehicle mounted jammer capable of defeating sophisticated threat systems. The name, Warlock Green, was inspired by the wife of an engineer from Fort Monmouth who collected miniature kitchen witches. The final production was performed by EDO Corporation and shipped out of Thousand Oaks, California, as early as March 2003 (Atkinson 7-25).

Warlock Red: The Warlock Red is a member of the CREW family of jammers designed by EDO Corporation to counter specific low power threats (SPG Media Group Limited). It is a low cost vehicle mounted jammer that emerged on the battlefield in the summer of 2004 (Atkinson 7-25).

Warlock Blue: The Warlock Blue or Little Blue is a half watt portable jammer the size of a walkie-talkie designed for dismounted troops to carry. The first models emerged from production in factories in California and Maryland in July 2005. This jammer was designed to conquer a low power radio frequency threat (Atkinson 19-25).

Chameleon: The Chameleon is a programmable jammer designed to adapt to the ever changing insurgent threat. It engages the full spectrum of RCIED triggers from garage door openers to cellular phones. Initial testing was performed in part by the Johns

Hopkins University Applied Physics Laboratory in the summer of 2005. The Chameleon was purchased by the Marines and put into action in November 2005 (Atkinson 26).

Channel/Acorn: The top-secret Navy program in counter-RC technology began after October 1983 when a truck packed with explosives killed 241 U.S. service members in Beirut. The resulting technology became known as the Channel series. The Channel series provided vessels protection against radio controlled bomb threats in foreign ports. Prior to 2002, the Channel series was considered obsolete and taken out of service. Navy specialists in Indian Head, Maryland, began reconfiguring the specifications of the Channel series jammers to conquer the growing threat caused by a device called the Spider Mod 1 in Afghanistan. This jamming device became known as the Acorn and was fielded in Afghanistan in November 2002 (Atkinson 6).

Duke/Duke 2: The Duke jammer is often referred to as a big box with a big antenna. This big box is a powerful and complex reactive jammer intended to phase out the Warlock series by covering the entire radio spectrum. This initiative, began in December 2004, would further simplify military logistics through the use of a common jammer. The Duke was designed by Army engineers at Fort Monmouth, produced by the Syracuse Research Corporation, and fielded November 2005. The Duke 2 is an improved version of the Duke jammer that was fielded in the summer of 2006 (Atkinson 16-28).

Citadel: The Citadel is a jammer used by explosive ordnance disposal (EOD) teams to create a protective area around technicians defusing a bomb. This portable jammer worked well to provide protection for a few yards but failed to provide the standoff distance required to protect a patrol and is not capable of vehicle mounting (Atkinson 6).

Shortstop: The Shortstop was designed in 1990 by Army engineers at Fort Monmouth, New Jersey and manufactured by the Whittaker Corporation. This mobile jammer is the size of a footlocker and originally intended to confound the proximity fuses in incoming artillery and mortar shells. (SPG Media Group Limited) The Shortstop prematurely detonates incoming rounds by causing them to register the approaching ground far prior to their impact (Atkinson 7).

Cottonwood/Ironwood: The Cottonwood jammer is a vehicle mounted CREW system in the Navy inventory. The Navy removed the Cottonwood from the Suburban in which they were mount and installed them in armored vehicles. In this role the Cottonwood is often referred to as the Ironwood (Atkinson 10-25).

MMBJ: The Mobile Multi Band Jammer is a vehicle mounted CREW system popular with the Special Forces community for defeating simple low powered radio devices (Atkinson 15-25).

ICE/MICE: A jammer, similar in capability to the SSVJ, called the IED Counter Electronic device (ICE) is a vehicle mounted member of the CREW family. (Atkinson 15-25) The ICE, favored by the Marines, is designed to jam radio trigged devices used by insurgents to initiate vehicle-borne or hidden explosives. (D'Alessio) The later modifications of the ICE are referred to as the MICE systems (Atkinson 15-18).

SSVJ: The Army's Rapid Equipping Force initiated through an organization in Las Cruces, New Mexico, to build prototype Self-Screening Vehicle Jammers (SSVJ). These jammers would go into full production. The SSVJ is a vehicle mounted member of the CREW family of jammers used in support of Operation Iraqi Freedom and Operation Enduring Freedom after March 2003 (Atkinson 25).

Jukebox: The Jukebox is a member of the CREW family of jammers used in support of Operation Iraqi Freedom and Operation Enduring Freedom after March 2003 (Atkinson 25).

Symphony: The Symphony is a member of the CREW family of jammers used in support of Operation Iraqi Freedom and Operation Enduring Freedom after March 2003 (Atkinson 25).

Spiral: The Spiral 2.1 is a CREW jamming system produced by the EDO Corporation. The Navy has begun research and development on Spirals 3.1, 3.2 and 3.3; projected to become the next generation of CREW systems supporting Iraq and Afghanistan (Atkinson 27-28).

Guardian: The Guardian is a backpack jammer also known as the Quick Reaction Dismounted (QRD). The Guardian replaced Little Blue, the Warlock Blue (Atkinson 28).

JIN: The Joint IED Neutralizer (JIN) is a member of the CREW family that counters RCIEDs through high frequency transmissions (Wilson 4).

NIRF: The Neutralizing Improvised Explosive Devices with Radio Frequency (NIRF) is a member of the CREW family that counters RCIEDs through high frequency transmissions (Wilson 4).

B. ELECTROMAGNETIC SPECTRUM MANAGEMENT

The electromagnetic spectrum has grown in importance as a battle space for service members to monitor (Atkinson 16). From the onset of the Iraqi conflict, much of the communications infrastructure was destroyed. At least two results are seen from this; the number of cellular telephones is preferred as there are very few traditional land lines left, and the number of other radio devices that are foreign to the U.S. such as the long range cordless telephone (LRCT) are in use. To complicate management further, the electromagnetic spectrum management varies by country and regulatory guidance is potentially different for each country. Normally, an organization such as the Federal Communications Commission (FCC) would monitor and regulate the electromagnetic spectrum, but there is no such organization in Iraq or Afghanistan (Atkinson 13). The spectrum is unregulated.

With no organization, such as the FCC, the electromagnetic spectrum in both Iraq and Afghanistan remains unchallenged and open to unlimited and uncontested usage. Through the use of a spectrum analyzer, the enemy can monitor the capabilities of a jamming system and make strategic decisions on changing RCIED triggers to different frequencies or increasing power. Then the enemy has countered the countermeasure (Atkinson 16).

In early 2006, the U.S. had created in Baghdad a document known as the “Mother of All Spreadsheets” or MOASS. The MOASS was a complete collection of radio frequencies that insurgents used to trigger roadside bombs. With this document, Army intelligence analysts and Navy electrical engineer matched the enemy’s known RCIEDs with the then 14 variants of jammers in use by coalition forces (Atkinson 25).

The updated MOASS in Baghdad was shared with the National Security Agency. Army and Navy electronic warfare officers in New Jersey and Maryland, respectively, further analyzed the MOASS and made recommendations to update the loadsets of all the jamming systems. These updated loadsets where then sent back to Baghdad to disseminate throughout the battle space to reprogram all of the jammers. This process took weeks and concurrently the MOASS in Baghdad had new frequencies and devices added (Atkinson 25). This circular process is continual.

The painstaking process of updating loadsets seems to be paying off. The move to the integration of both active and reactive jammers and the continual reprogramming of these jammers has glimmers of success. From mid-2006 and throughout 2007 and 2008, the use of RCIEDs in Iraq continues to decline (Atkinson 26).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: JAMMING PRINCIPLES AND DEFINITIONS

A. BASIC EW COMPONENTS AND PRINCIPLES

1. Antenna

The two main types of antenna used in electronic warfare are of the type that cover a 360-degree azimuth or that cover a smaller angular area (Adamy, Introduction to Electronic Warefare Modeling and Simulation 105-106). A vehicle mounted or man-pack antenna is typically the ladder, an omnidirectional "whip" antenna. This type of antenna is assumed as used in this study of radio frequency jammers. The omnidirectional antenna is one type of isotropic antenna. Isotropic antennas radiate equally in all directions (Miller 559-560). Omnidirectional antennas are used in the tactical ground environment as the radio waves are transmitted from the vertically polarized mast of the antenna in a 360 degree circle on the horizontal plane and angular in the vertical plane (Adamy, Introduction to Electronic Warefare Modeling and Simulation 109).

2. Distance

Distance is first introduced through the principle of propagation. Propagation, or wave propagation is the movement of radio signals from the transmitter to the receiver through the earth's atmosphere (Miller 5). The propagation of the radio wave is an initial introduction of distance as a main factor of radio wave properties. The free-space propagation model, Equation (11), demonstrates that the direct loss is a ratio of the distance as the wave radiates out in a circular motion by the length of the transmitted radio wave.

The free-space propagation model (Adamy, EW102: A Second Course in Electronic Warefare 114) is:

$$L = \frac{(4\pi)^2 d^2}{\lambda^2} \tag{11}$$

where: $L \equiv$ direct loss ratio {unitless}

$d \equiv$ distance {meters}

$\lambda \equiv$ length of transmission wavelength {meters}

This model will focus on line-of-sight models along the earth's surface with the transmitter's and receiver all operating on relatively the same altitude. Additionally, the free space propagation model is based off of the geometry of the radio waves and there are no significant contributions from the atmospheres or rain (D. L. Adamy, EW102: A Second Course in Electronic Warefare 113). The basic jamming scenario is displayed in Figure 18.

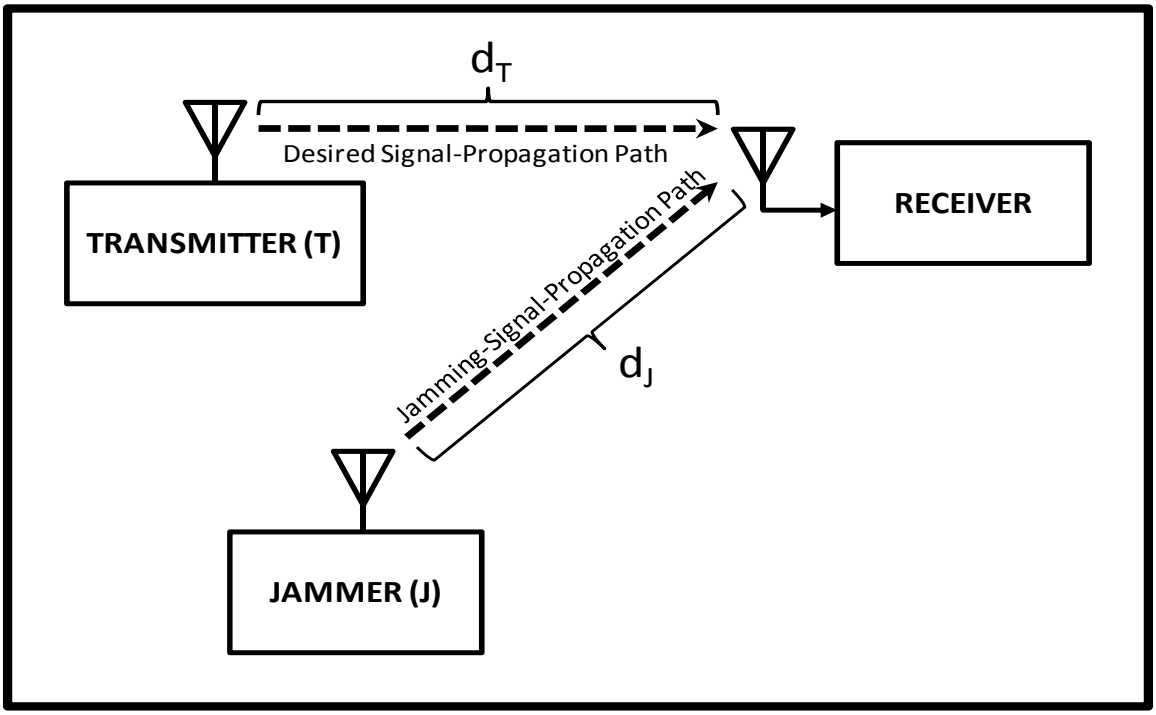


Figure 18. The jamming scenario [After (D. L. Adamy, EW102: A Second Course in Electronic Warefare 137)]

3. Power

The signal-to-noise ratio or jammer-to-signal ratio (JSR) assist in determining how much power is enough to jam a signal. SNR is defined as the relative measure of desired signal power to noise, or in this case jammer, power (Miller 11-12). In determining the JSR we must know specification of the jammer and characteristics of the receiver targeted to jam.

There are two important specifications in this use of the JSR. First, this is not radar jamming, rather the scope of this research is for radio frequency or communications jamming. With radar jamming the distance is factored to the fourth power as the signal path is to the target and back. In radio communications jamming the signal only propagates in one direction and the distance factor is squared. This propagation loss reduction by a square rather than a fourth power provides an increase in range for a decrease in power; therefore the modification to JSR. Second, jamming does not focus on the enemy transmitter and does have the goal of influencing the receiver.

The equation to determine JSR (D. L. Adamy, EW102: A Second Course in Electronic Warefare 138) is:

$$JSR = \frac{\left(\frac{P_J G_J}{(d_J)^2}\right)}{\left(\frac{P_T G_T}{(d_T)^2}\right)} \tag{12}$$

where: $P_J \equiv$ Power of the Jammer

$P_T \equiv$ Power of the Transmitter

$G_J \equiv$ Gain of receiver's antenna from the Jammer

$G_T \equiv$ Gain of receiver's antenna from the Transmitter

$d_J \equiv$ Distance from the receiver to the Jammer

$d_T \equiv$ Distance from the receiver to the Transmitter

As seen in Equation (12) above, the power is the effective radiated power of either the jammer or the transmitter that is attempted at being jammed is a product of the power and the gain of the antenna of the receiver. In tactical communications, the omnidirectional "whip" antenna is the norm and the receiver with a whip antenna has the same gain from both the jammer and the transmitter (Adamy, EW102: A Second Course

in Electronic Warefare 139). As both gains cancel each other out, the simplification of Equation (12) follows as Equation (13) and the signal-to-jammer ratio becomes the following:

$$JSR = \frac{\left(\frac{P_J}{(d_J)^2}\right)}{\left(\frac{P_T}{(d_T)^2}\right)} \tag{13}$$

4. Duty Cycle and Time Sharing

Radio frequencies are emitted in pulses with a rest time between pulses. The ratio of the pulse time to the pulse repetition time is known as the duty cycle (Miller 657). The equation for the duty cycle takes the form as displayed in Equation (14):

$$DC = \frac{PW}{PRT} \tag{14}$$

where: $DC \equiv$ Duty cycle {unitless}

$PW \equiv$ Pulse width {microseconds}

$PRT \equiv$ Pulse repetition time {microseconds}

Two duty cycles of a radio frequency transmission pulses are observed in Figure 19. The target of the jammer is to block the transmission over the pulse width. Figure 20 is the same sample radio frequency as in Figure 19 over two duty cycles with an appropriate jamming cycle overlaid. The jammer could jam constantly at the max power of the transmission signal, but this would produce much wasted jamming time. Instead, in the valleys between the jamming signals become free time, time available to possible jam another signal.

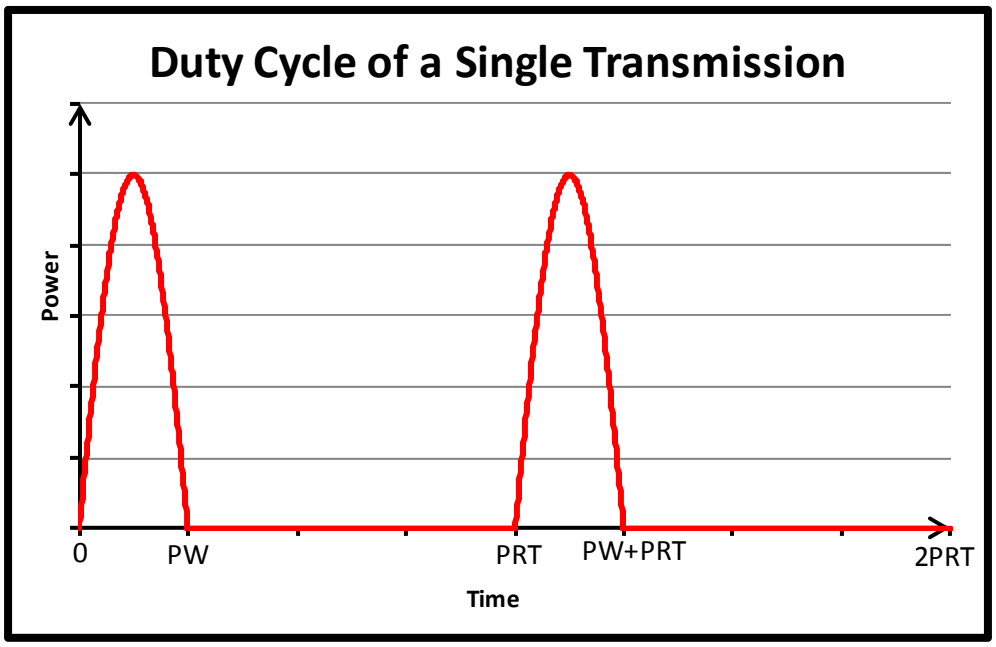


Figure 19. Two duty cycles of a single transmission [After (Electronic Warfare Division 2-5)]

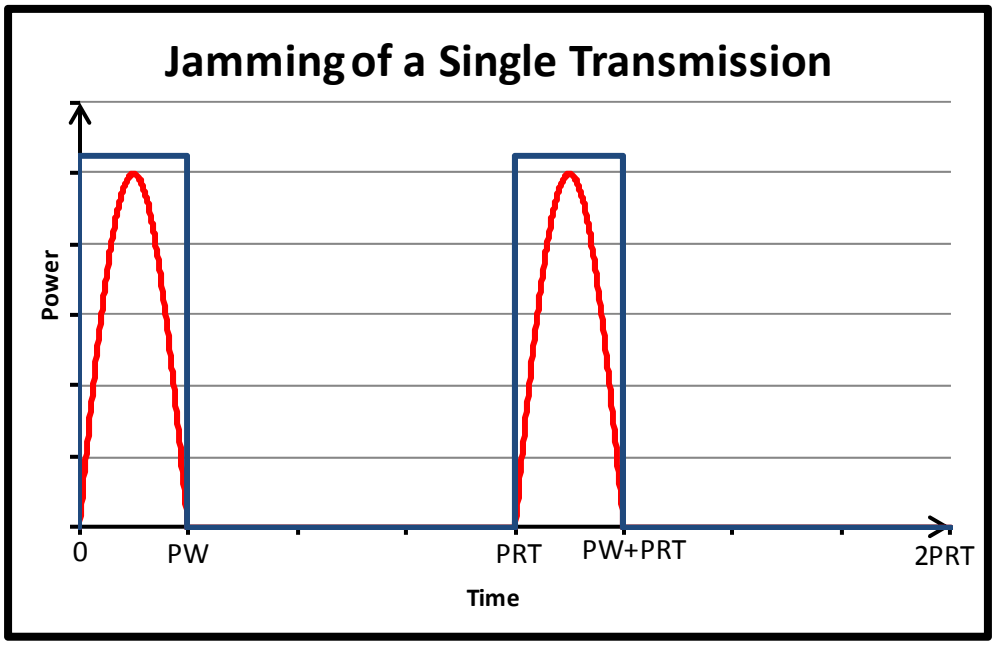


Figure 20. Sample jamming scenario of a single transmission over two duty cycles.

With the free time in the jammers duty cycle, time sharing becomes important concept in maximizing the efforts of the jammer. Through time-sharing, the jammer's frequency modulator is able to jam more than one frequency over the jamming cycle (Jeong and Ra 1-5). If another RCIED trigger is found with the same duty cycle, it may have its own power and time requirements. Figure 21 introduces a second independent signal and the time and power overlay pattern to also jam this signal.

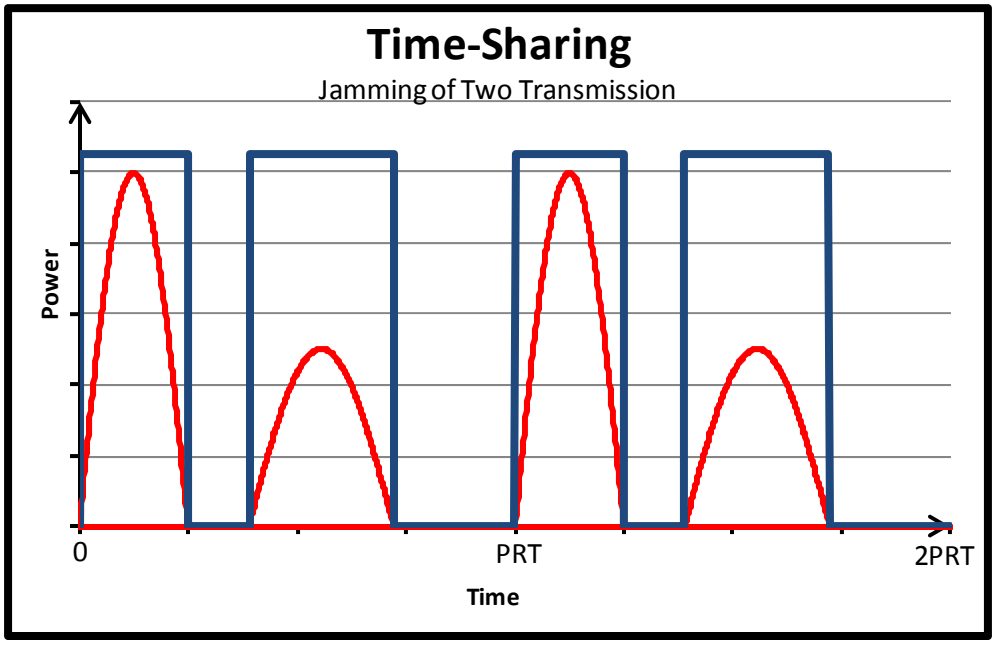


Figure 21. Sample scenario of time share jamming of two transmissions over two duty cycles

5. Power Sharing

Power sharing is where the power amplifier of the jammer is called upon to amplify two or more signals simultaneously (Royal Thai Naval Academy 268). Figure 21 demonstrates a jammer pattern for the jamming of two signals over two pulse repetitions. The same two independent signals are represented in Figure 22, but here the jammer is conserving power and only applying enough power to successfully jam each individual signal. The maximum power available is labeled. Signal 1 requires almost all of the available power over its pulse width. Signal 2 only requires half of the maximum power for the duration of its pulse width.

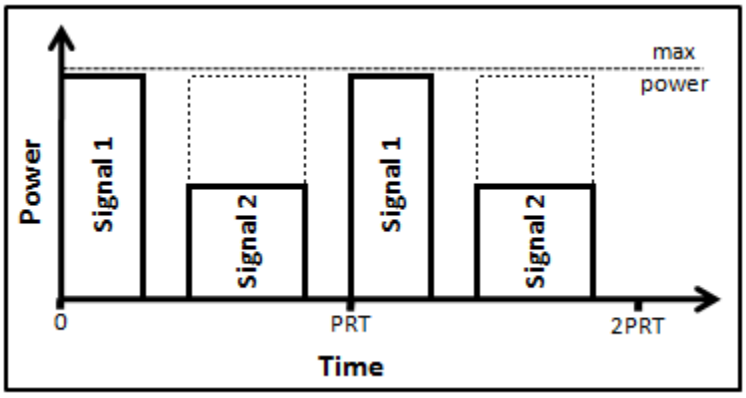


Figure 22. Jamming of two signals with different power requirements

Now, introducing a third signal that is desirable to jam and it has the same pulse width, pulse repetition time and power requirements as Signal 2 in Figure 22. The jammer has the power and time available. The result of adding this third radio frequency to jam is displayed in Figure 23. Signals 2 and 3 in this case are power sharing.

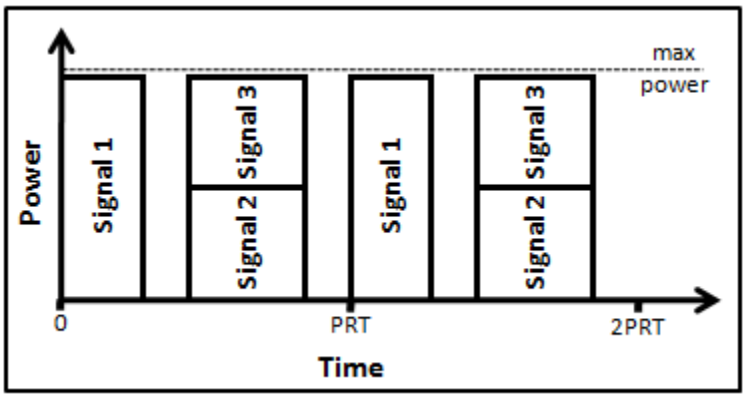


Figure 23. Jamming of three signals with two signal power sharing

Not only are Signals 2 and 3 power sharing in Figure 23, Signal 1 and the Signal 2-3 pair are time sharing. This displays a simple combined time sharing and power sharing jamming strategy for these three radio frequency signals.

B. SIMPLIFICATION OF DATA REQUIREMENTS

The current proposed data for each RCIED trigger is the expected distances for the transmitter receiver pair, the expected distance of the jammer to the trigger or

standoff distance, the power of the transmitter, the power the jammer applied to jamming the particular frequency, and the jammer to signal ratio required for the RCIED trigger's receiver. Through much study of each individual RCIED trigger receiver pair most of these required values are measured. For the scope of this thesis and the modeling, we can reason through the reduction of data requirements.

In determining the ability of the jamming system to successfully jam and RCIED trigger with respect to power and distance, Equation (15) must be satisfied.

$$JSR_T \leq \frac{\left(\frac{P_J}{(d_J)^2}\right)}{\left(\frac{P_T}{(d_T)^2}\right)} \tag{15}$$

Breaking down Equation (15) into parts it is observed P_T is data found through the examination of the device. The d_J is a decision variable for the standoff distance of the jammer as a fixed number of meters for all jamming modules of the jamming system. P_J, or the power of the jammer, is a decision variable that is minimized to possibly conserve power to apply to other possible IED threats. This leave the distance of the transmitter to the receiver of the RCIED, d_T. The distance could be achieved using an appropriate discrete distribution.

When allowing d_T to become a random variable, say x, Equation (15) takes the form of Equation (16).

$$JSR_T \leq \frac{P_J}{P_T} \frac{x^2}{(d_J)^2} \tag{16}$$

Solving Equation (16) for x and changing the inequality to the viewpoint of the insurgent, the result is Equation (17).

$$x < \sqrt{JSR_T (d_J)^2 \frac{P_J}{P_T}} \tag{17}$$

Evaluating the random variable x, a unique discrete distribution defined by each individual transmitter, we would define an acceptable threshold of enemy success or $Pr\{X < x\}$. For each given resulting probability for each trigger, there is a resulting

power requirement for the jammer to successfully jam a signal within the given probability, or from the perspective of the insurgent to successfully trigger an RCIED.

The resulting P_J is with respect to each individual RCIED. The P_J variable becomes data for each individual RCIED trigger as the power, in Watts, to successfully jam a triggers signal with respect to the triggers jam to signal ratio, standoff distance of the jammer, and power of the radio transmission of the transmitter at an appropriate defined level of probability. (In the formulation of the models, Chapter III, P_J is the parameter w_i.)

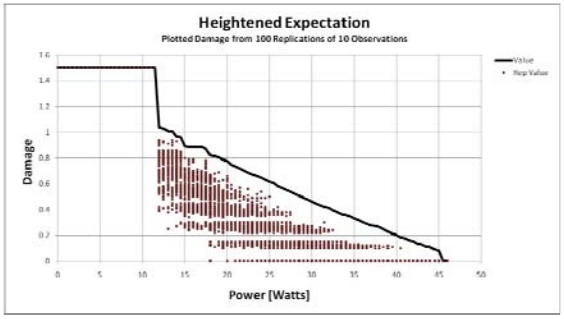
THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D: DATA AND GRAPHS

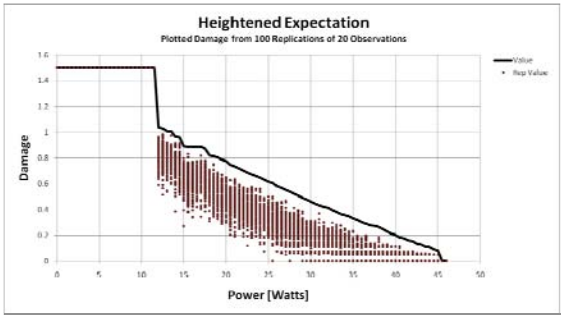
A. DATA PLOTS

100 Replications–Heightened Expectation Data Plots:

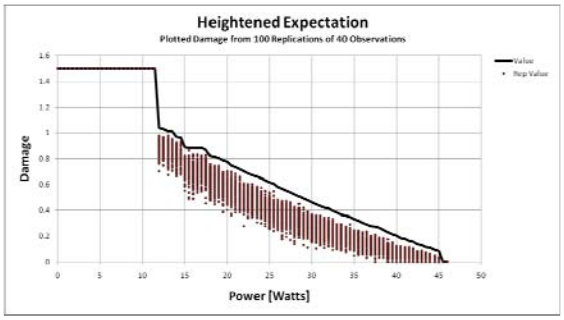
10 Observations



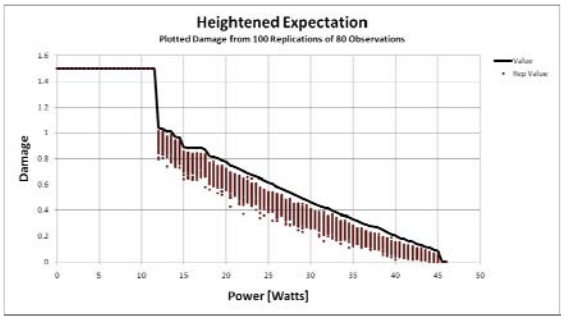
20 Observations



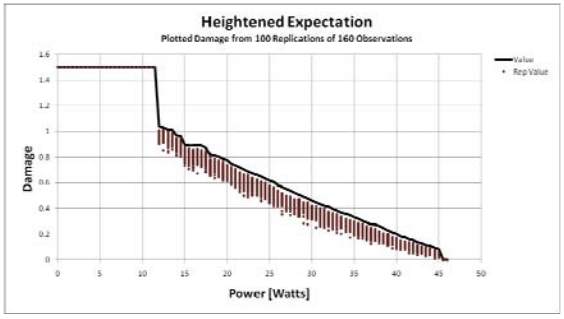
40 Observations



80 Observations

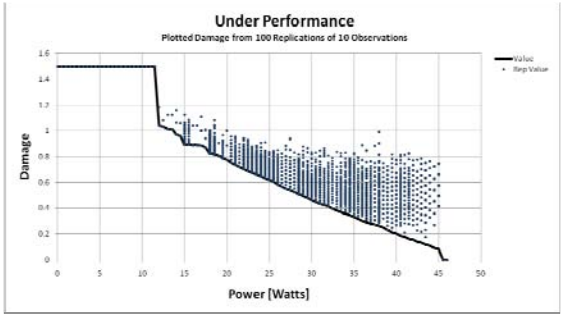


160 Observations

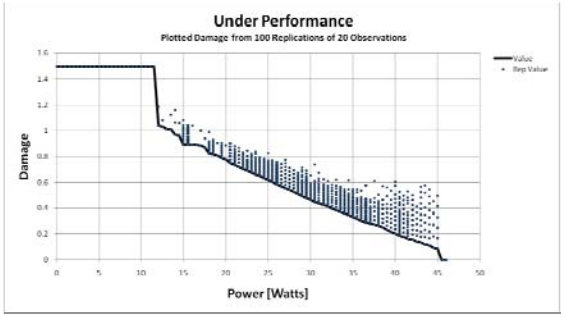


100 Replications–Under Performance Data Plots:

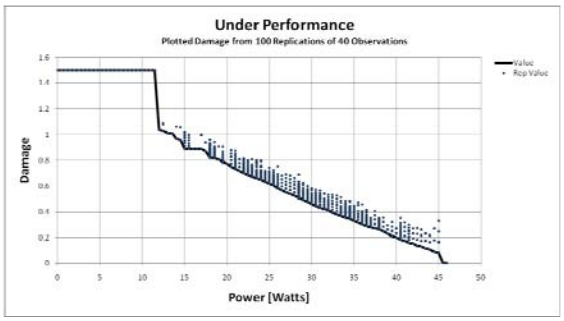
10 Observations



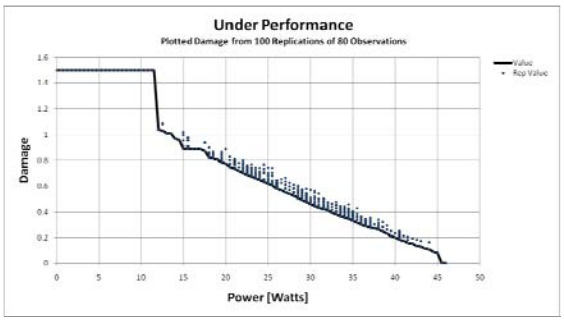
20 Observations



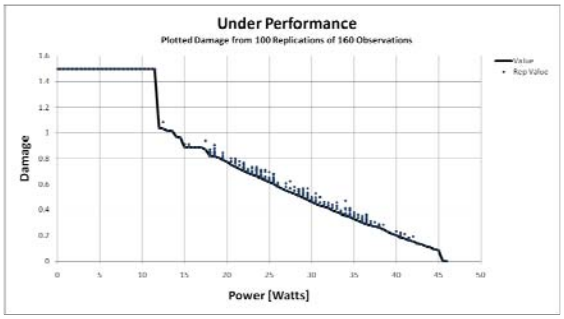
40 Observations



80 Observations



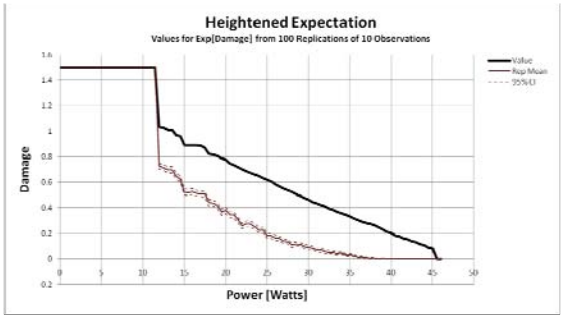
160 Observations



B. PLOTS OF MEANS AND CONFIDENCE INTERVALS

100 Replications–Expectation Mean and CI:

10 Observations



20 Observations

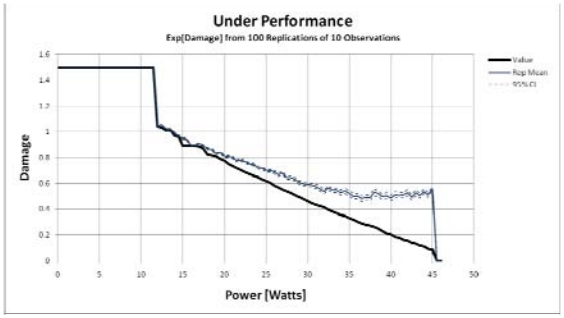
40 Observations

80 Observations

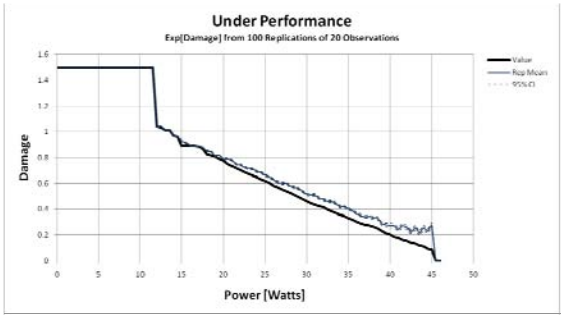
160 Observations

100 Replications – Under Expectation Mean and CI:

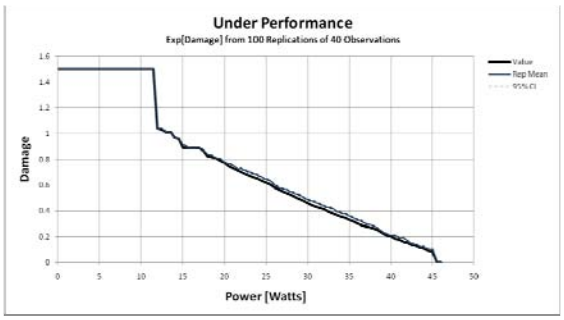
10 Observations



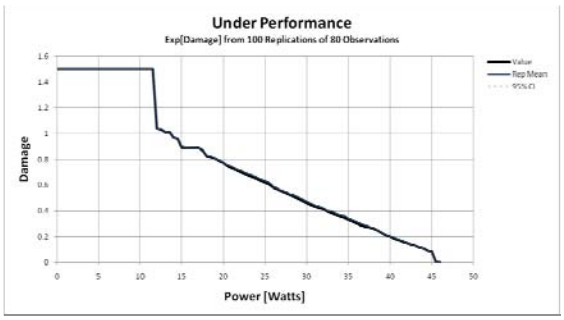
20 Observations



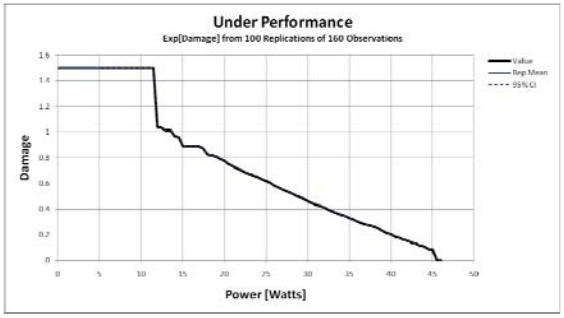
40 Observations



80 Observations



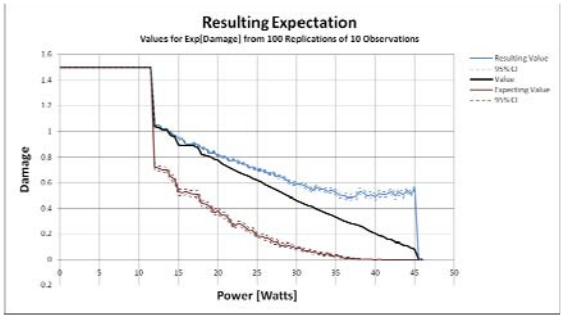
160 Observations



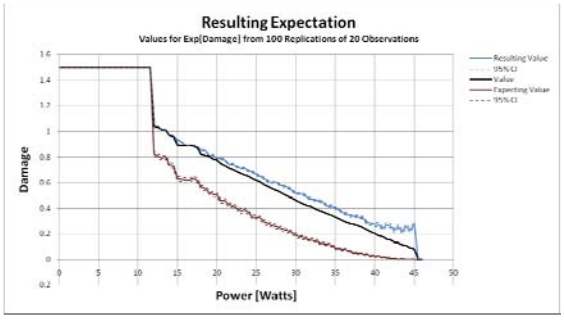
C. COMBINED PLOTS OF MEANS AND CONFIDENCE INTERVALS

100 Replications–Combined Expectation Means and CIs:

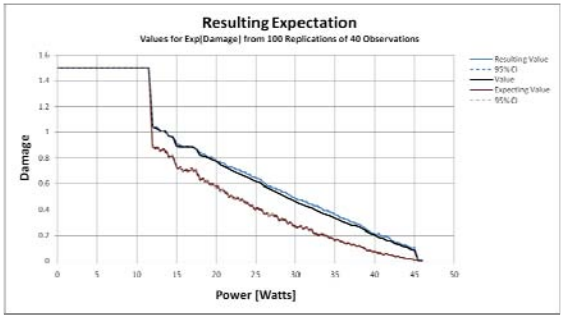
10 Observations



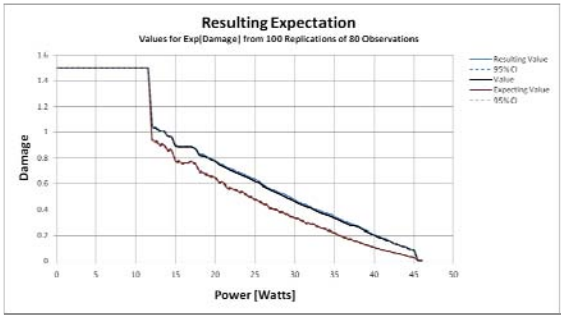
20 Observations



40 Observations



80 Observations



160 Observations

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adamy, David L. EW102: A Second Course in Electronic Warefare. Boston: Artech House, 2004.

———. Introduction to Electronic Warefare Modeling and Simulation. Boston: Artech House, 2003.

Associated Press; USA TODAY Research and Wire Reports. "U.S. Military Struggles to Adapt to War's Top Killer." USAToday.com. 21 February 2008 <http://www.usatoday.com/news/graphics/ied-deaths/flash.htm?tabNum=tab1>.

Atkinson, Rick. Left of Boom: The Struggle to Defeat Roadside Bombs. e-document. The Washington Post, 2007.

Australian Government, Department of Defense. "Improvised Explosive Device (IED) Fact Sheet." defence.gov.au. 16 January 2009 <http://www.defence.gov.au/publications/IED_fact_sheet.pdf>.

CTF-7 CALL Representative. CJFT-7 OIF Smart Card 4. Version 1.A. Baghdad: CTF-7/C3 Training Cell - CALL LNO, 2004.

D'Alessio, Stephen. "Marine Corps News." 7 August 2005. Marines schooled in new bomb protection. 21 February 2009 <http://192.156.19.109/marinelink/mcn2000.nsf/ad983156332a819185256cb600677af3/b89628064c45144e85257056003871f1?OpenDocument>.

Defense Manpower Data Center, Data Analysis and Programs Division. "DOD Personnel and Military Casualty Statistics, Defense Manpower Data Center." Casualty Summary by Reason, October 7, 2001 through January 31, 2009. 5 June 2009 <http://siadapp.dmdc.osd.mil/personnel/CASUALTY/gwot_reason.pdf>.

Department of Defense. Joint Publication 1-02; Department of Defense Dictionary of Military and Associated Terms. Department of Defense, 2009.

Electronic Warfare Division. Electronic Warfare and Radar Systems Engineering Handbook. Point Mugu: Electronic Warfare Division, 1997.

GAMS 23.0. "GAMS On-line Documentation." 14 February 2009. GAMS. 9 June 2009 <http://www.gams.com/docs/document.htm>.

ILOG CPLEX 11. "CPLEX 11 Solver Manual." 2007. GAMS. 9 June 2009 <http://www.gams.com/dd/docs/solvers/cplex.pdf>.

Improvised Explosive Devices (IEDs)/Booby Traps. 11 January 2005. GlobalSecurity.org. 21 February 2008 <http://www.globalsecurity.org/military/intro/ied.htm>.

Jeong, Unseob and Sung-Woong Ra. "Interference Rejection of a Feedback Noise Jamming Using a Switch-Matrix Tx/Rx Control." IEEE: Vehicular Technology Conference (2006): 1-5.

Jones, Ian. Malice Afterthrought: The History of Booby Traps from World War One to Vietnam. London: Greenhill Books, 2004.

Keesee, Robin L. "JIEDDO Cooperative Opportunities; International Acquisition Forum – XXII." 07May30-JIEDDO Coop Opportunities.ppt. Joint Improvised Explosice Device Defeat Organization, 30 May 2007.

Kestrel, a Lightweight, Software-Configurable Jamming System to be Exhibited at IDEX 2009. 20 February 2009. army-technology.com. 21 February 2009 <http://www.army-technology.com/contractors/jamming/enterprise/press3.html>.

Lin, Kyle Y. and Yu-Chu Shen. A Game-Theoretic Model for Jamming Radio Controlled Improvised Explosive Devices. Monterey: Naval Postgraduate School, 2008.

Marshall, Brian. How the Radio Spectrum Works. 30 January 2009 <http://electronics.howstuffworks.com/radio-spectrum1.htm>.

Marshall, Brian, Jeff Tyson and Julia Layton. How Cell Phones Work. 7 June 2009 <http://electronics.howstuffworks.com/cell-phone8.htm>.

Martin, Lanaya A. and Joshua L. Nickerson. A Game Theoretic Approach to IED Jamming Strategy. MS Thesis. Monterey: Naval Post Graduate School, 2008.

Meigs, Montgomery. "On the Offensive: The Battle Against IEDs." 2007 April 16. Army Times. 21 February 2009 <http://www.armytimes.com/community/opinion/marine_opinion_meigs_070416/>.

Miles, Kevin, FBI SABT of Las Angeles. "The Future of IEDs in the U.S." The Future of IEDs in the US.ppt. 19 February 2009.

Miller, Gary M. Modern Electronic Communication. 6th Edition. Columbus: Prentice Hall, 1999.

Royal Thai Naval Academy. Space & Electronic Warfare Lexicon Terms. Samut Prakan: Royal Thai Naval Academy, 2005.

SPG Media Group Limited. "New Fuze Solutions for new Mortar Systems." 6 September 2001. army-technology.com. 21 February 2009 <http://www.army-technology.com/contractors/ammunition/junghans/press1.html>.

———. "Off-the-Shelf Solutions for the Battlefield." 14 May 2008. army-technology.com. 21 February 2009 <http://www.army-technology.com/features/feature1918/>.

Straffin, Phillip D. Game Theory and Strategy. 6th Printing. Washington, DC: The Mathematical Association of America, 2006.

U.S. Army/Marine Corps. Counterinsurgency Field Manual. Chicago: University of Chicago Press, 2007.

U.S. House of Representatives. The Joint Improvised Explosive Device Defeat Organization: DOD's Fight Against IEDs Today and Tomorrow. Committee on Armed Services, Subcommittee on Oversight & Investigations. Washington, DC, 2008.

Wilson, Clay. "Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures." CRS Report for Congress 21 November 2007: 1-6.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Kyle Y. Lin
   Naval Postgraduate School
   Monterey, California

4. CDR Michael A. Herrera
   Naval Postgraduate School
   Monterey, California

5. MAJ Jeffrey A. Dayton
   TRAC WSMR FWD
   Fort Bliss, Texas

6. JIEDDO
   5000 Army Pentagon
   Washington, District of Columbia

7. Army Asymmetric Warfare Office
   400 Army Pentagon
   Washington, District of Columbia

8. Director, Operations Analysis Division
   Code C19, MCCDC
   Quantico, Virginia