2008-06

Optimal jammer placement to interdict wireless network services

Shankar, Arun

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

OPTIMAL JAMMER PLACEMENT TO INTERDICT WIRELESS NETWORK SERVICES

by

Arun Shankar

June 2008

Thesis Advisors:	David Alderson Hong Zhou
Second Reader:	W. Matthew Carlyle

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE *(Leave blank)*	2. REPORT DATE June 2008	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Optimal Jammer Placement to Interdict Wireless Network Services	5. FUNDING NUMBERS
6. AUTHOR(S) Arun Shankar	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

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

13. ABSTRACT (maximum 200 words)

The demand for wireless networks continues to grow as the need for portable, low-cost telecommunications systems increases around the world. Wireless networks are particularly complex because their topologies can change in response to operational requirements or environmental conditions and also because wireless networks are susceptible to electromagnetic interference. In this thesis, we consider the challenges associated with the operation and jamming of so-called "wireless mesh networks." In a wireless mesh network, the communication devices (denoted here as a *nodes*) are uniform in their ability to send and receive transmissions. We formulate and solve two related optimization problems for wireless mesh networks. First, we solve the problem of the network *operator*, namely: In order to maximize the utility of delivered network traffic, how should one set the power transmission levels for each node, and along what sequence of transmission links should the traffic flow? The second problem we consider involves an intelligent adversary, the *attacker*, who wants to place jamming devices among a finite number of locations to disrupt the operator's traffic in the worst possible way. We formulate and solve mathematical programs to obtain the optimal operation and jamming of these networks. We develop a computational decision-support tool that affords the rapid reconfiguration and analysis of various deployment scenarios.

14. SUBJECT TERMS Wireless Networks, Network Interdiction, Nonlinear Programming, Simultaneous Routing and Resource Allocation, Wireless Network Jammer locations, Jammer Placement	15. NUMBER OF PAGES 59
	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

OPTIMAL JAMMER PLACEMENT TO INTERDICT WIRELESS NETWORK SERVICES

Arun Shankar
Captain, United States Marine Corps
M.S., Hawaii Pacific University, 2006
B.A., University of Texas, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH
AND
MASTER OF SCIENCE IN APPLIED MATHEMATICS

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Author: Arun Shankar

Approved by: David Alderson
Thesis Co-Advisor

Hong Zhou
Thesis Co-Advisor

W. Matthew Carlyle
Second Reader

James Eagle
Chairman, Department of Operations Research

Clyde Scandrett
Chairman, Department of Applied Mathematics

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The demand for wireless networks continues to grow as the need for portable, low-cost telecommunications systems increases around the world. Wireless networks are particularly complex because their topologies can change in response to operational requirements or environmental conditions and also because wireless networks are susceptible to electromagnetic interference. In this thesis, we consider the challenges associated with the operation and jamming of so-called "wireless mesh networks." In a wireless mesh network, the communication devices (denoted here as a *nodes*) are uniform in their ability to send and receive transmissions. We formulate and solve two related optimization problems for wireless mesh networks. First, we solve the problem of the network *operator*, namely: In order to maximize the utility of delivered network traffic, how should one set the power transmission levels for each node, and along what sequence of transmission links should the traffic flow? The second problem we consider involves an intelligent adversary, the *attacker,* who wants to place jamming devices among a finite number of locations to disrupt the operator's traffic in the worst possible way. We formulate and solve mathematical programs to obtain the optimal operation and jamming of these networks. We develop a computational decision-support tool that affords the rapid reconfiguration and analysis of various deployment scenarios.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. WIRELESS NETWORKS....1
B. RESEARCH PROBLEM STATEMENT....3
C. LITERATURE REVIEW OF PREVIOUS WORK....4
D. STRUCTURE OF THESIS AND CHAPTER OUTLINE....5

II. MODEL FORMULATION....7
A. SIMULTANEOUS ROUTING AND RESOURCE ALLOCATION....8
1. Rate-Power Capacity Curve....8
2. SRRA Problem....9
B. THE ATTACKER'S PROBLEM....12
C. SOLUTION APPROACH....14
D. DECISION SUPPORT TOOL....14

III. ANALYZING A SAMPLE NETWORK....17
A. VALIDATING THE MODEL....17
B. ANALYSIS ON A LARGER NETWORK....19
C. HEURISTICS FOR JAMMER PLACEMENT....21
1. Node Density....21
2. Source and Destination Nodes....23
3. Network Cut....25
D. ENUMERATING ALL POSSIBLE SOLUTIONS....27
1. Most and Least Effective Jammer Locations....27
2. Secured Source and Destination Nodes....32
E. SUMMARY AND DISCUSSION....35

IV. SUMMARY AND CONCLUSIONS....37

LIST OF REFERENCES....39

INITIAL DISTRIBUTION LIST....41

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Sample Network for Validation 17
Figure 2. Sample Network from Xiao et al. (2004) 20
Figure 3. Jammer locations according to node density 21
Figure 4. Jammer locations near sources and destinations 23
Figure 5. Jammer locations (network cut) 25
Figure 6. Ten most effective jammer locations 27
Figure 7. Best operator response to different jammer placement 29
Figure 8. Ten least effective jammer locations 30
Figure 9. The effect of placing one jammer 31
Figure 10. 30 most effective jammer locations not near source and destination nodes 32
Figure 11. 15 most effective jammer locations not near source and destination nodes 33
Figure 12. Results of the most effective jammer location sets not near source and destination nodes 34
Figure 13. Results of the most effective jammer location sets not near source and destination nodes 35
Figure 14. Results of the most effective jammer location sets among different heuristics 36

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Utility values for placement of a single jammer 18
Table 2. Utility values for placement of two jammers 19
Table 3. Utility values for placement of one jammer (node density) 22
Table 4. Utility values for placement of two jammers (node density) 22
Table 5. Utility values for placement of one jammer (supply and destination) 24
Table 6. Utility values for placement of two jammers (supply and destination) 24
Table 7. Utility values for placement of one jammer (network cut) 26
Table 8. Utility values for placement of two jammers (network cut) 26
Table 9. Utility value for placement of four jammers (network cut) 26
Table 10. Utility values for most effective jammer locations 28
Table 11. Utility values for most effective pairs of jammer locations 28

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank the Operations Research Department and Applied Mathematics Department for giving me the opportunity to receive such a thorough, rewarding graduate education from the Naval Postgraduate School. I would particularly like to thank my thesis advisor, Professor Alderson, for never giving up on me and holding me accountable. His close guidance and mentorship set an example that I hope to pass along to my subordinates some day.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Wireless networks provide an effective means for information exchange in situations where fixed (i.e., wired) communication links are not possible or are not desirable. The portability of these networks allows information systems professionals the ability to design flexible communications networks that fit the needs of both mobile and stationary users without the cost or constraints of wires. As demand for these networks continues to grow, so do the challenges underlying their design and security.

In this thesis, we consider the challenges associated with the operation and jamming of so-called "wireless mesh networks." A wireless mesh network is a network in which each communication device (denoted here as a *node*) can serve as both a wireless transmitter and a wireless receiver. We assume that all nodes in the network are homogenous in terms of their transmission and receiving capabilities. Moreover, nodes in the network can serve as either the source of a communication message, the destination for a message, or as an intermediate transmission point. Source nodes typically correspond to the location of an end-user (also called a *station*) or the location of remote sensing device (also called a *sensor*). Destination nodes may include end-users or computer servers acting as data aggregation points. Nodes can play interchangeable roles, in the sense that the same node may be the source of one communication message, the destination for a different communication message, and an intermediate transmission point for a third message. We use the term *link* to refer to the bi-directional communication between two nodes.

We formulate and solve two related optimization problems for wireless mesh networks. First, we solve the problem of the network *operator*, namely: In order to maximize the utility of delivered network traffic, how should one set the power transmission levels for each node, and along what sequence of transmission links should the traffic flow? This problem is a nonlinear convex optimization problem, and it can be solved by a variety of methods. The second problem we consider involves an intelligent adversary, the *attacker*, who wants to place jamming devices among a finite number of locations to disrupt the operator's traffic in the worst possible way. Specifically, we

restrict attention to enumeration over a finite set of pre-selected jammer locations to obtain the most disruptive combination. In both cases, we measure network performance in terms of the volume of traffic delivered to source and destination nodes.

Wireless networks play an important role in the United States (US) military. For example, the US Marine Corps depends heavily on wireless network technology in Distributed Operations (DO). The DO concept provides squad-size units the telecommunications technology that they need to communicate critical information with higher units. Wireless networks also play a considerable role in Humanitarian Assistance and Disaster Relief (HA/DR) operations. These operations usually occur in areas where telecommunications infrastructure is sparse (as in developing countries) or has been destroyed (as in the aftermath of an earthquake or hurricane), making wireless mesh networks increasingly important.

We develop an interdiction model that determines the effect of jammers on the utility of a wireless network with optimized routing and resource allocation. We analyze the effects of this model on a sample network. We found that the most effective placement of a jammer is near source and destination nodes or critical transshipment nodes. Placing single jammers at other locations provides little or no effect on the network. We use Microsoft Excel, Visual Basic for Applications (VBA) and the General Algebraic Modeling System (GAMS) (GAMS Development Corporation, 2008) to implement this model in a user-friendly fashion.

The tools developed in this thesis will provide commanders with a better understanding of wireless mesh network capability, vulnerability, and operation. Moreover, this thesis is the first step in the development of a self-contained decision support tool suitable for development in live exercises and real-world operations.

I. INTRODUCTION

A. WIRELESS NETWORKS

Wireless networks provide an effective means for information exchange in situations where fixed (i.e., wired) communication links are not possible or are not desirable. The portability of these networks allows information systems professionals the ability to design flexible communications networks that fit the needs of both mobile and stationary users without the cost or constraints of wires. As demand for these networks continues to grow, so do the challenges underlying their design and security.

There are many wireless communication technologies in common use today. These include mobile phone technologies (personal cellular phones, SMS text messaging), computer "wi-fi" technologies (wireless hotspots, wireless local area networks), technologies for satellite communication (GPS, Iridium satellite phones), and radar technologies for long-range sensing. In this thesis, we will focus on a particular network technology used in so-called "wireless mesh networks."

Wireless networks are increasingly popular anywhere that physical links are not available or possible. Examples include developing countries and rapidly changing environments. It is increasingly common to observe countries deploying national telecommunication systems built exclusively from wireless technologies (Hayden, 2006).

Wireless networks also play a vital role in the United States (US) military. The need for commanders to deploy communications networks rapidly is more important than ever before. Military functional areas including logistics, intelligence, and warfighting all depend on wireless networks for critical information exchange. For example, the US Marine Corps depends heavily on wireless network technology in Distributed Operations (DO). The DO concept provides squad-size units the telecommunications technology that they need to communicate critical information with higher units. Members of DO units carry multiple wireless technologies including GPS systems, handheld radios, and various other event-driven sensors. These devices provide small unit leaders with the information that they need to make split-second decisions in crucial situations.

Wireless networks also play a considerable role in Humanitarian Assistance and Disaster Relief (HA/DR) operations. These operations usually occur in areas where telecommunications infrastructure is sparse (as in developing countries) or has been destroyed (as in the aftermath of an earthquake or hurricane). The success of HA/DR operations hinges on the ability to pass information quickly and efficiently. The portability of wireless networks caters to that need.

Wireless networks are important not only for point-to-point communication but also for the remote sensing of environmental conditions. The ability to mass produce small, wireless sensing devices inexpensively means that it is now cost effective to deploy large quantities of "disposable" sensors that operate for only a limited period but are never retrieved. These "sensor nets" are increasingly employed to monitor weather, seismic activity, agricultural conditions, national infrastructure systems, and potential terrorist behavior. They can greatly enhance the situational awareness (SA) available to any system operator or commander.

Wireless networks have numerous advantages over wired networks. They are easy to deploy because they do not require the installation of wires. This reduces the amount of infrastructure and manpower needed. This also allows for simple reconfiguration should the need arise to change network connectivity patterns. In addition, wireless networks do not require large, central coordination for new components to join or be removed from the network. Consequently, these networks provide increased flexibility and mobility at, arguably, a lower overall cost.

Wireless networks also have disadvantages over wired networks. Most importantly, wireless networks are susceptible to electromagnetic interference. This interference can be caused by any number of sources, including magnets, overhead power lines, and even other users in the network. The interference is nonlinear in nature, so it is difficult to predict, detect, and mitigate. Also, the operational complexity of wireless networks can be higher than wired networks. For example, the range and interference associated with a transmitter determine the possible routes in the network as well as the flow transmitted over them (Johansson, 2003). This brings about challenges for efficient routing of data because the capacity of each link may be different and changing

independently over time. While software protocols exist to manage these tradeoffs, the parameters of these protocols may be difficult to tune, thus in practice it may be more difficult to optimize traffic flow in a wireless network than in a wired network.

Because wireless transmissions are subject to interference either from the environment or from other signals, wireless communications are vulnerable to *jamming*. Wireless jammers are some of the oldest threats to network security. These devices aim to restrict or destroy a wireless communications signal between two or more nodes. Wireless jammers provide a nonlethal weapon to combatants at war. Both the US military and its foes have used them in the past. Restricting the flow of electronic information on a battlefield can significantly influence the outcome of an engagement. The ability to detect and/or employ wireless jammers can provide considerable benefits to a commander and affect the likelihood of mission success.

B. RESEARCH PROBLEM STATEMENT

In this thesis, we consider the challenges associated with the operation and jamming of so-called "wireless mesh networks." A wireless mesh network is a network in which each communication device (denoted here as a *node*) can serve as both a wireless transmitter and a wireless receiver. We assume that all nodes in the network are uniform in terms of their transmission and receiving capabilities. Moreover, nodes in the network can serve as either the source of a communication message, the destination for a message, or as an intermediate transmission point. Source nodes typically correspond to the location of an end-user (also called a *station*) or the location of remote sensing device (also called a *sensor*). Destination nodes may include end-users or computer servers acting as data aggregation points. Nodes can play interchangeable roles, in the sense that the same node may be the source of one communication message, the destination for a different communication message, and an intermediate transmission point for a third message. We use the term *link* to refer to the bi-directional communication between two nodes.

We formulate and solve two related optimization problems for wireless mesh networks. First, we solve the problem of the network *operator*, namely: In order to maximize the utility of delivered network traffic, how should one set the power

transmission levels for each node, and along what sequence of transmission links should the traffic flow? This problem is a nonlinear convex optimization problem, and it can be solved by a variety of methods. The second problem we consider involves an intelligent adversary (the *attacker*) who wants to place jamming devices (among a finite number of locations) to disrupt the operator's traffic in the worst possible way. Specifically, we restrict attention to enumeration over a finite set of pre-selected jammer locations to obtain the most disruptive combination. In both cases, we measure network performance in terms of the utility achieved of traffic delivered to destination nodes.

To our knowledge, this is the first attempt to formulate and solve a bi-level model of wireless operation and jamming using optimization. In the current operational environment, decisions about where to place jammer locations is heuristic or ad hoc (Joint Doctrine for Electronic Warfare, 2000). Our objective is to provide a quantitative means to assess the optimal attack and defense of wireless mesh networks. Building on the work of Brown et al. (2006), we develop both the mathematical model and the computational tools needed to solve them. Specifically, we design the user interface for this model in Microsoft Excel, and create the solution methods in General Algebraic Modeling System (GAMS) (GAMS Development Corporation, 2008) and Visual Basic for Applications (VBA). VBA provides the user interface and establishes a connection between Excel and GAMS. The Mixed Integer Nonlinear Optimization Solver (MINOS) (Stanford Business Software, 2008) in GAMS solves the mixed integer nonlinear program. We analyze several numerical examples to validate the solution approach.

These tools will provide commanders with a better understanding of wireless mesh network capability, vulnerability, and operation. Moreover, this thesis is the first step in the development of a self-contained decision support tool suitable for development in live exercises and real-world operations.

C. LITERATURE REVIEW OF PREVIOUS WORK

Considerable research exists involving the optimization of wired telecommunications networks having fixed communication links (see Resende and Paradalos, 2006 and references therein). More recent research has expanded that concept to optimize simultaneously both the routing of flow (network layer) and allocation of

resources (physical layer) throughout the network. This thesis draws primarily on the work of Xiao et al. (2004), who present a model for optimal simultaneous routing and resource allocation (SRRA) in a wireless network. They use a fictional network to analyze the benefits of the formulation. They present a variety of design problems having differing (and competing) objectives, including minimum power, minimax link utilization, and maximum utility. Their results demonstrate that simultaneously optimizing routing and resources achieves a higher utility than using uniform resource output.

In follow-on work, Johansson et al. (2004) develop a similar formulation and additionally consider optimizing transmission scheduling for wireless networks. They find that throughput optimization leads to activating the shortest links with nonzero flows and assigning zero flows to the rest of the links. This type of wireless network is not realistic in practice, because we expect that nodes communicate at nonzero levels. As a result, they modified their formulation to consider a concept of "fairness" by attempting to balance throughput and total utility.

Rosati et al. (2006) document the importance of these SRRA problems. They argue that satellite bandwidth resources will continue to decrease as wireless technology progresses. Since a true SRRA model would require coordination among all nodes in a network, it is actually an impractical solution for extremely large networks with no central control (i.e., the entire Internet) (Rosati, 2006). But network managers of individual, decentralized networks can still benefit from the SRRA problem to optimize their share of a larger architecture.

None of the existing research in SRRA problems explores network interdiction. Specifically, they do not consider an attacker's goal of interdicting arc(s) that would cause the worst damage to the network.

D. STRUCTURE OF THESIS AND CHAPTER OUTLINE

The remainder of this thesis is arranged as follows. In Chapter II, we introduce the nonlinear formulation first presented by Xiao et al. (2004). We then extend this formulation to develop a model of wireless transmission and to consider jammer

interference. In Chapter III, we use this model to analyze various scenarios of jammer quantities and locations. In Chapter IV, we summarize the contributions of this thesis and offer suggestions for further research.

II. MODEL FORMULATION

Two nodes in a wireless network communicate through the transmission of electromagnetic signals. The strength and clarity of these signals are a factor of gain, noise, distance, and power (Xiao, 2004). *Gain* defines a receiving node's ability to accept and interpret a signal based on its distance from the transmitter and directional orientation. *Noise* is electromagnetic interference in the signal caused by any variety of outside factors. Magnets, power lines, radio jammer locations, and other communication nodes are typical elements known to cause noise. *Distance* is the physical space between two communication nodes. *Power* is the strength of the signal from the transmitting device. A higher amount of power can overcome noise interference (Stahlberg, 2000).

Jamming occurs when an external signal travels to a receiving antenna at the same frequency as a transmitter. The jammer adds noise to the receiver's signal, causing the signal to lose its clarity. Noise caused by multiple jammers is additive in that the cumulative effect is the sum of individual interference. Enough noise can result in the complete loss of the signal by the receiver. Qualitatively, a successful jammer is one where the jamming power equals the signal power at the receiver (Stahlberg, 2000).

The strength of a wireless signal (and its interference) is inversely proportional to the square of its distance. Thus, a jammer at twice the distance would have to operate at four times the power to achieve the same results (Stahlberg, 2000).

A jamming attack is difficult to overcome. Unlike other security breaches, such as denial of service (DoS) attacks or conventional computer viruses, jammers interfere with architecture at the physical level (Xu, 2005). A software alteration cannot alleviate the effects of a jammer. Instead, the network designers must make a physical change. Nodes must be moved out of the path of the jammer, or flows must be rerouted through nodes that are not affected by the jammer. In smaller, mobile units such as light infantry platoons or reconnaissance teams, relocating nodes may be the most simple and appropriate solution. However, larger headquarters elements and command posts that are less mobile will find the latter solution most appropriate.

Many types of jammers exist. A constant jammer emits a continuous signal on one or more frequencies (Xu, 2005). A network's ability to overcome this type of jammer's interference depends on the number of frequencies over which it broadcasts, the location of the jammer, and the amount of power emitted from the jammer and from the transmitting nodes (Stahlberg, 2000). Other variations of jammers provide intermittent broadcasts of signal interference. A time interval, frequency spectrum, or set of reactionary events can trigger the jammer to broadcast interference. In this thesis, we will analyze the effects of a continuous, omni-directional jammer interfering equally on all frequencies.

A. SIMULTANEOUS ROUTING AND RESOURCE ALLOCATION

As noted previously, the SRRA model optimizes the routing and resource allocation (transmission power) within a wireless network. In order to formulate this model, we first derive and define the capacity formula of the arcs within the network. This formula will provide the basis for the capacity constraint in the operator's problem.

1. Rate-Power Capacity Curve

We adopt the rate-power curve established by Neely et al. (2005), which is an extension of the Shannon Capacity formula (see also Cover and Thomas, 1991, pp. 249-250). The rate-power curve assumes unit bandwidth for each link and considers noise interference by other transmitters as well as interference from outside sources such as wireless jammers. The capacity from transmitter *i* to receiver *j* is

$$\phi_{ij} = \log\left(1 + \frac{g_{ij}P_{ij}}{n_j + g_{ik}\sum_{k\neq j}P_{ik} + \sum_{l\neq i} g_{lj}\sum_{k} P_{lk}}\right) \qquad (1)\,.$$

Here, P_{ij} is the power assigned by node *i on* arc $(i, j) \in A$. The gain g_{ij} represents the receiving node's ability to accept a signal based on its distance from the transmitting node. Receiving nodes $j \in N$ are subject to Additive White Gaussian Noises (AWGNs) n_j. We add one to the fraction within the log function to ensure that the value of the

capacity is never negative. The second term in the denominator $g_{ik}\sum_{k\neq j}P_{ik}$ represents noise caused by other transmissions from node *i* (self interference). The third term in the denominator $\sum_{l\neq i}g_{lj}\sum_{k}P_{lk}$ corresponds to the noise caused by other transmissions to node *j*. We normally measure the power P_{ij} and noise n_j in watts and the capacity ϕ_{ij} in bits per second (Cover and Thomas, 1991). The gain g_{ij} is a dimensionless constant used to scale the power of the transmitter.

The gain g_{ij} is a function of the square of the distance between the nodes (Stahlberg, 2000). Following the convention in Xiao et al. (2004), we assume that $m=\min(d_{ij})$ and $g_{ij}=\frac{m^2}{d_{ij}^{\,2}}$. The minimum length provides a factor to scale the gain in relation to the rest of the network. We assume that concurrent transmissions from node *i* are broadcast along different frequencies so there is no self-interference (frequency division multiple access). The resulting equation is

$$\phi_{ij}=\log\left(1+\frac{\left(\frac{m^2}{d_{ij}^2}\right)P_{ij}}{n_j+\sum_{l}\left(\frac{m^2}{d_{lj}}\right)P_{lj}}\right) \qquad (2)$$

which simplifies to

$$\phi_{ij}=\log\left(1+\frac{\frac{P_{ij}}{d_{ij}^{\,2}}}{\frac{n_j}{m^2}+\sum_{l}\frac{P_{lj}}{d_{lj}^{\,2}}}\right) \qquad (3)\,.$$

2. SRRA Problem

We consider a wireless networking problem in which the capacity of an individual broadcast channel (i.e., the capacity of a link in the network) follows from the power (i.e., the resource) assigned to it. We define data traffic on the network in terms of its destination, and thus we introduce a different traffic commodity for each destination. The challenge is to determine simultaneously the optimal capacity of each broadcast channel

as well as the optimal route for all network traffic. Following the problem statement by Xiao et al. (2004), we present mathematical program SRRA.

The "log-utility" function imposes particular value on the traffic flowing through the network. For each source-destination pair, anything less than unit flow results in a negative contribution to system performance, with a zero flow yielding infinitely negative utility. Flows above the unit level yield a positive contribution to system performance with decreasing marginal utilities. Overall, this utility function creates incentive for fair and balanced flow among source-destination pairs with severe penalties for flow below the unit level.

Formulation 1: SRRA

Index Use

$i \in N$	node *(alias j, k)*
$q \in Q \subseteq N$	source node
$d \in D \subseteq N$	destination node
$r \in R \subseteq N$	transshipment node
$(i, j) \in A$	arc *(link)*

Calculated Data

d_{ij}	distance between node $i \in N$ and $j \in N$	[distance]
m	$\min(d_{ij})$	[distance]
ρ_i	total power available at node $i \in N$	[power]
n_j	signal noise at node $j \in N$	[noise]

Decision Variables

X_{ij}^{d}	flow along arc $(i, j) \in A$ that is destined for node $d \in D$ [flow]
S_i^d	traffic supply at node $i \in N$ that is destined for node $d \in D$ [flow]

P_{ij}	power assigned by node i to arc $(i, j) \in A$	
	[power]	
$STOT^d$	total traffic delivered to node $d \in D$	[flow]

Formulation

$$\max_{X,S,P} \quad \sum_{d} \sum_{i \neq d} \log_2 \left(S_i^d \right) \tag{D0}$$

$$s.t. \quad \sum_{k:(j,k) \in A} X_{jk}^d - \sum_{i:(i,j) \in A} X_{ij}^d = \left\{ \begin{matrix} S_q^d & j = q \\ 0 & o/w \\ -STOT^d & j = d \end{matrix} \right\} \forall j \in N \tag{D1}$$

$$-STOT^d = -\sum_{q \neq d} S_q^d \tag{D2}$$

$$\sum_{d} X_{ij}^d - \log \left(1 + \frac{\frac{P_{ij}}{d_{ij}^2}}{\frac{n_j}{m^2}} \right) \leq 0 \tag{D3}$$

$$\sum_{j:(i,j) \in A} P_{ij} \leq \rho_i \qquad \forall i \in N \tag{D4}$$

$$P_{ij} \geq 0 \qquad \forall (i, j) \in A \tag{D5}$$

$$X_{ij}^d \geq 0 \qquad \forall (i, j) \in A, \forall d \in D \tag{D6}$$

$$S_i^d \geq 0 \qquad i \neq d \tag{D7}$$

The objective represents the sum of the utilities for each delivered stream of traffic. The first constraint (D1) enforces balance of flow at each node for each commodity. The second constraint (D2) ensures balance of flow between the source and destination nodes. The third constraint (D3) defines the capacity of arc (*i,j*) and follows directly from (3). The second term in the denominator of (3) is absent because we assume that wireless jammer locations are not present in this formulation. Bandwidth allocation for each link is fixed (i.e., each link has unit bandwidth—there is no frequency division multiplexing, or FDMA) and the capacity of a link is a nonlinear function of the power

allocated to it. The fourth constraint (D4) indicates that each node has a limited amount of power to allocate among its broadcast channels. Finally, all variables are constrained to be nonnegative.

Xiao et al. (2004) solve this problem using a dual decomposition method. They separate the formulation into network routing and power allocation sub-problems and use a subgradient method with Lagrange multipliers to converge to an optimal solution. In this thesis, we use GAMS (GAMS Development Corporation, 2008) with the MINOS (Stanford Business Software, 2008) solver to obtain the solution. We guarantee an optimal solution because the formulation is convex.

B. THE ATTACKER'S PROBLEM

The previous formulation considered the task of the network operator (or autonomous network protocols) to assign resources to arcs and then route traffic in a manner that maximizes overall utility. Here we consider the challenge associated with an intelligent adversary who wants to disrupt this maximum flow in the worst possible manner. We assume that both the attacker and the defender have perfect information about the network, and that they share the same objective function. But the attacker wishes to minimize the defender's maximum utility.

In this problem, the attacker has a finite number of jamming devices that can be placed among a finite set of predetermined locations. Each jamming device interferes with wireless traffic by effectively increasing the "noise" seen by nearby receivers. The amount of interference seen by a receiver is a nonlinear function of the distance from the jammer placement to the receiver and the power of the jammer, all relative to the placement and strength of any other signals. We represent the decision problem of the "attacker" by introducing additional variables and constraints and presenting a mathematical program SRRA-Attack.

Formulation 2: SRRA-Attack

New Index Use

$l \in L$ potential jammer location

New Data

d_{lj} distance from jammer location $l \in L$ to receiver $j \in N$

[distance]

New Decision Variables

Y^l binary indicator whether a jammer placed at location $l \in L$

$Y^i = 1$ if jammer is active at location $l \in L$, $Y^i = 0$ otherwise

[binary]

Formulation

$$\min_{Y} \left[\begin{array}{lll}
\max\limits_{X,S,P} & \sum\limits_{d} \sum\limits_{i \neq d} \log_2 \left(S_i^d \right) & \text{(A0)} \\
s.t. & \sum\limits_{k:(j,k) \in A} X_{jk}^d - \sum\limits_{i:(i,j) \in A} X_{ij}^d = \begin{cases} S_q^d & j = q \\ 0 & o/w \\ -STOT^d & j = d \end{cases} \forall j \in N & \text{(A1)} \\
& -STOT^d = -\sum\limits_{q \neq d} S_q^d & \text{(A2)} \\
& \sum\limits_{d} X_{ij}^d - \log \left(1 + \dfrac{\dfrac{P_{ij}}{d_{ij}^{\,2}}}{\dfrac{n_j}{m^2} + \sum\limits_{l} \dfrac{P_{lj}}{d_{lj}^{\,2}} (Y^l)} \right) \leq 0 & \text{(A3)} \\
& \sum\limits_{j:(i,j) \in A} P_{ij} \leq \rho_i \qquad \forall i \in N & \text{(A4)} \\
& P_{ij} \geq 0 \qquad \forall (i,j) \in A & \text{(A5)} \\
& X_{ij}^d \geq 0 \qquad \forall (i,j) \in A, \forall d \in D & \text{(A6)} \\
& S_i^d \geq 0 \qquad i \neq d & \text{(A7)} \\
& Y^l \in \{0,1\} & \text{(A8)}
\end{array} \right.$$

Binary attack variables Y^l affect the capacity of nearby arcs via constraint (A3). A jammer creates noise at a receiver by broadcasting at the same frequency, as discussed in (4).

C. SOLUTION APPROACH

One approach to solving the min-max attacker's formulation is to take the dual of the inner program so that the entire formulation becomes a minimization problem (Brown et al., 2006). Unfortunately, our formulation does not lend itself to this technique, due to the nonlinear nature of the objective function and capacity constraint. In addition, the use of linear approximations for these functions is not attractive because it either makes the arc transmission capacities unrealistic or makes the attack variables unrealistic for the underlying problem. The dual decomposition presented in Xiao et al. (2004) does not lend itself to this technique either.

Given a finite number of potential jammer placements and a finite number of available jammer locations, it is possible to enumerate all possible attack scenarios, evaluate the optimal objective under each scenario, and then identify the best one(s). This is computationally feasible for problems of modest size, but becomes intractable for large problems. In the next chapters, we do exactly this. Then for larger problems, we devise various heuristics for quickly finding "good" combinations of jammer placements without having to enumerate. Our heuristic strategies include: (1) choose locations that afford high interference values; (2) choose jammer locations based on proximity to node locations; and (3) consider set covering formulations that provide interference across the entire region. We analyze these heuristics and compare their performance to optimal jammer assignments.

D. DECISION SUPPORT TOOL

We develop a decision support tool using GAMS and Microsoft Excel. This tool requires the user to input the location of nodes and jammers in the network along with their effective ranges. It also requires the user to input the power of the jammers and the nodes. The user must input the noise associated with each receiving node in the network. He must also designate whether a given node is a source, destination, or both.

We then use VBA to calculate the required data and designate the proper sets for the SRRA-Attack formulation. We use VBA to pass the data into GAMS. The formulation exists in GAMS, so we use GAMS to calculate the solution and return the results to Microsoft Excel.

The use of Microsoft Excel and VBA make the tool quite simple to use. The user is only directly exposed to the input and the results. Minor modifications can allow a user to analyze several types of networks for many different scenarios.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ANALYZING A SAMPLE NETWORK

A. VALIDATING THE MODEL

We begin by validating our attacker's formulation against a network with six nodes and four potential jammer locations (Figure 1). The simplicity of this network will allow us to verify that the solutions provided by the model support our intuitions.

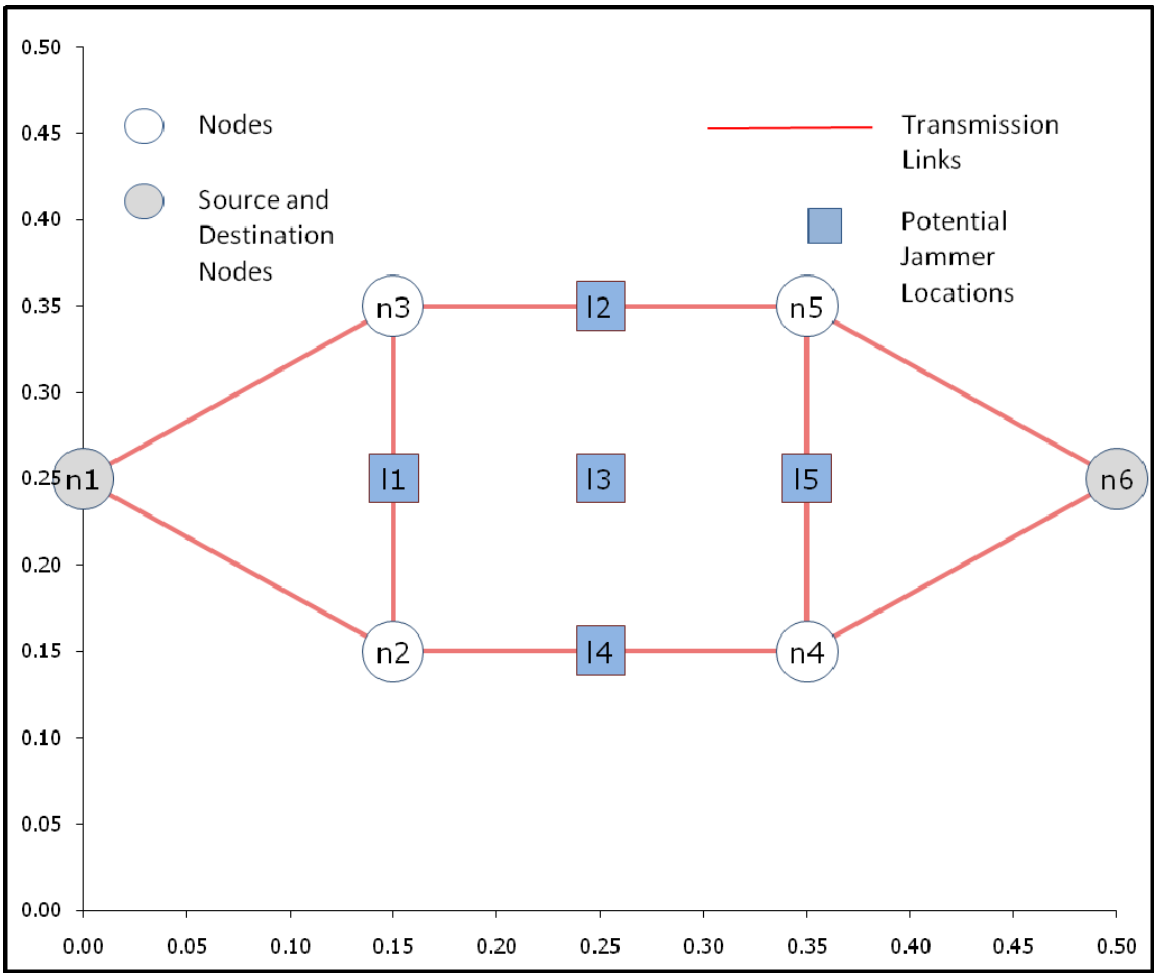

Figure 1. Sample Network for Validation

Figure 1 illustrates a simple mesh network with six nodes (n1, n2,...,n6) with maximum range equal to 0.25 placed on a square grid. By construction, n1 and n6 are both source and destination nodes. All links are bi-directional. For the sake of simplicity,

we fix the outside noise interference associated with each receiver to equal .05. We assume each node can emit a sum of 100 units of power. We consider five potential jammer locations (l1…l5). We assume the jammers to be used are uniform in their capabilities broadcasting on all frequencies with Power = 1 and maximum range equal to 0.25. The maximum achievable utility for this specific network obtained as the optimal solution to formulation SRRA is 5.22.

We first consider the placement of a single jammer at each of the potential jammer locations. We assume that the defender will reconfigure the network to operate in the most optimal manner after the attacker places the jammer. Table 1 shows the results after enumerating all possible solutions.

Utility	**Jammer Location**
3.58	l1
3.58	l5
3.85	l3
3.91	l2
3.91	l4

Table 1. Utility values for placement of a single jammer

In this example, l1 and l5 are equally effective. The symmetry of the network lends itself to this type of solution. l2 and l4 are also equally effective. However, placing a jammer at l5 or l1 is more effective than placing a jammer at l2 or l4. By placing a jammer at l5 or l1, we force the flows in the network to travel through "jammed" nodes. Take l5 for example. By placing a jammer at l5, we provide additional interference to n5 and n4. Flow traveling to and from n6 must pass through either n5 or n4. Therefore, all flows between n1 and n6 must travel through these "jammed" transshipment nodes. This reduces flow that can enter and exit n6. Balance of flow constraints force the same reduction of flow on n1. Since n1 and n6 are source and destination nodes, the objective function is reduced, hence the lower utility value. On the contrary, placing a jammer at l2 or l4 does not create this dilemma because a free path remains between n1 and n6 that does not have "jammed" transshipment nodes. l3 provides an equal effect on the transshipment nodes since it is placed in the center of the network.

Next, we consider the optimal placement of two jammers within the network (Table 2).

Utility	Jammer Locations	
3.3	l1	l2
3.3	l1	l3
3.3	l1	l4
3.3	l2	l5
3.3	l3	l5
3.3	l4	l5
3.31	l1	l5
3.31	l2	l4
3.42	l2	l3
3.42	l3	l4

Table 2. Utility values for placement of two jammers

We find that several pairs of jammers produce the same effect on the network due to its symmetry and the balance of flow between source and destination nodes. If we reduce flow from n1 to n6, we must also reduce it from n6 to n1. Note that the least effective pairs contain at least one jammer location that is not within range of n1 or n6.

B. ANALYSIS ON A LARGER NETWORK

Xiao et al. (2004) presented a fictional network with 50 nodes and 170 bidirectional links (Figure 2). Five nodes serve as both sources and destinations (n8, n10, n13, n25, n45). Each node is uniform and communicates with all other nodes within 0.25 units of range. Each node has 100 units of power to allocate across all of its broadcast channels. Outside noise interference associated with each receiver is a random number generated with a uniform distribution on the interval [.01, .1]. The value of the utility with no jammers in the network is 17.24 and matches (within 0.1%) the solution obtained in Xiao et al. (2004).

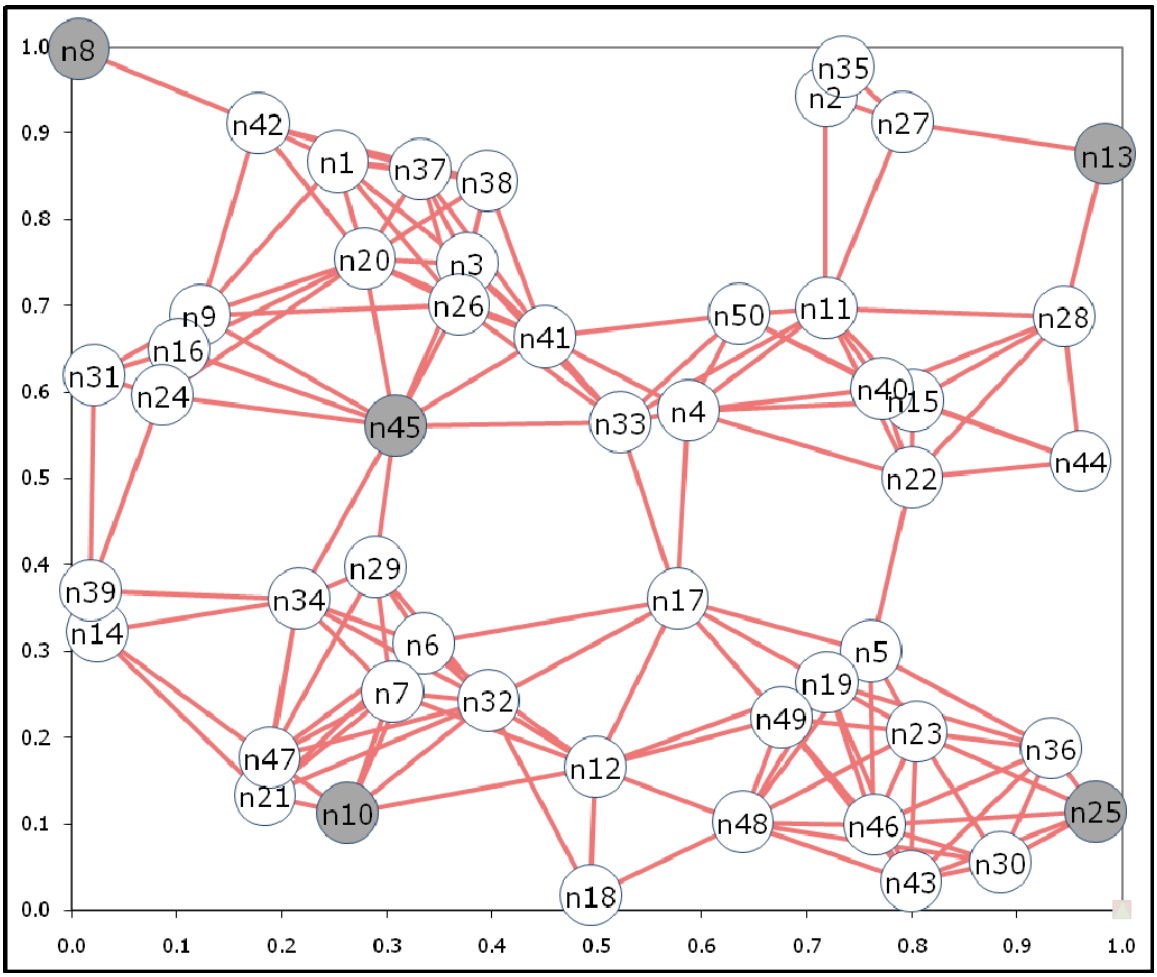

Figure 2. Sample Network from Xiao et al. (2004)

We next consider an intelligent adversary who wants to disrupt communication in this network in the worst possible way. We assume this attacker has the ability to place jammers at a finite number of pre-selected locations. The mathematical program, SRRA-Attack, solves for the best combination of available jammer locations.

In general, the attacker may or may not have control over the pre-selection of potential jammer sites. There are a number of factors that may affect the ability of an adversary to place a jammer successfully among the operator's network. These include terrain barriers, heavy security, or risk of visual detection.

C. HEURISTICS FOR JAMMER PLACEMENT

We consider several heuristics for the pre-selection of potential jammer locations. These heuristics may or may not be realistic in practice, as several factors play in the consideration of a potential jammer location.

1. Node Density

We consider four jammer locations in areas of the network where the numbers of arcs appear to be dense (Figure 3). The goal of the jammer placement is to reduce the flow between the source and destination nodes and consequently reduce the objective function value. We speculate that adding interference to several transshipment nodes will cause a significant decrease in utility.

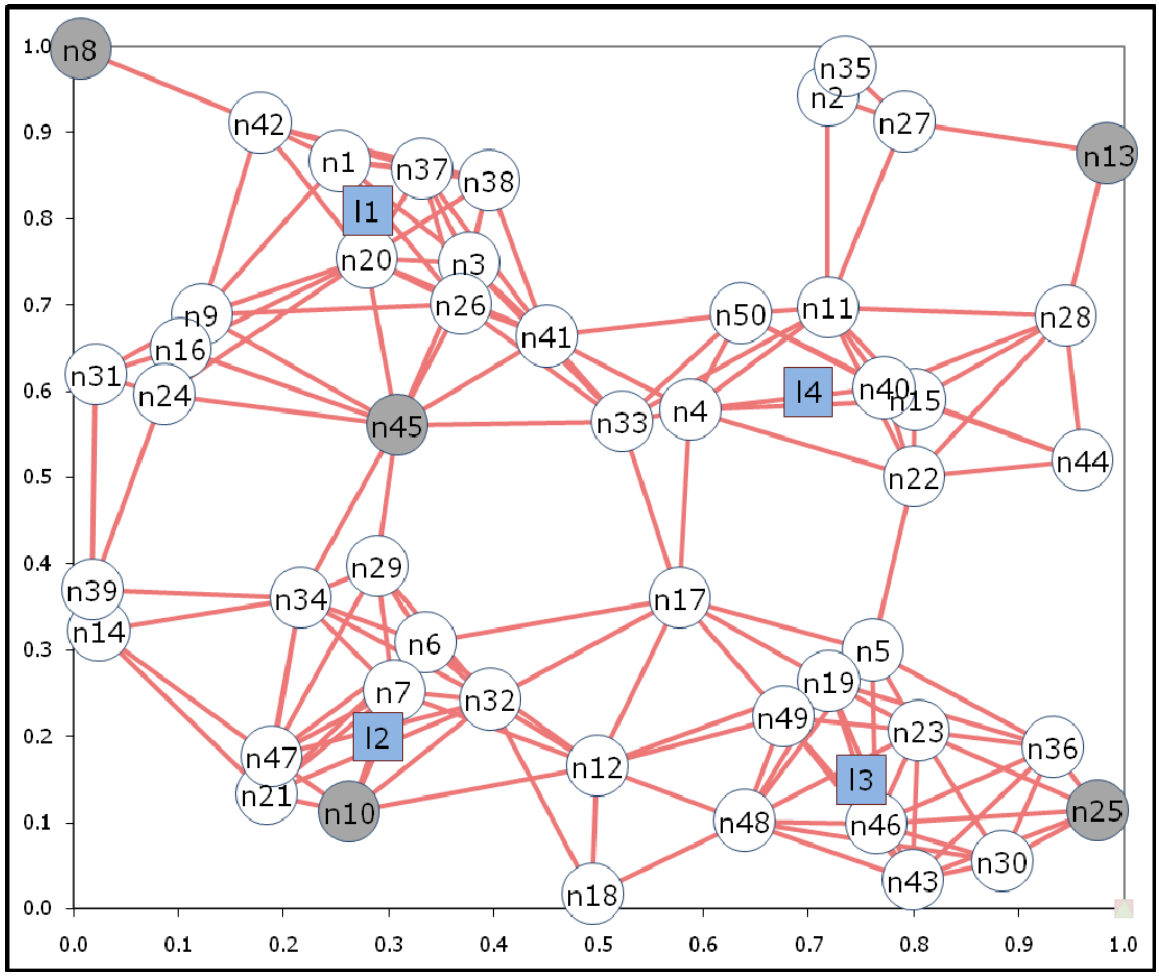

Figure 3. Jammer locations according to node density

When the attacker can place a single jammer among these locations, the utility values in Table 3 are close in value. l1, l2, and l3 are nearer in distance to source and destination nodes than l4. l1 is not within an effective range of n8. However, since n8 has one adjacent arc, n8 reduces its flow when we affect transshipment nodes near the tail of the arc adjacent to n8. We use the balance of flow constraints to force the other source and destination nodes to reduce their flows as well.

l2 is almost as effective as l1 and very close in distance to n10. By interfering with n10 and its adjacent transshipment nodes, we reduce the value of the flow from n10 and reduce the utility value.

Utility	**Jammer Location**
15.86	l1
15.94	l2
16.39	l3
17.03	l4

Table 3. Utility values for placement of one jammer (node density)

The utility values obtained from the placement of two jammers in Table 4 are also similar in value. We note that l1 and l2 appear in most of the pairs. That is not surprising since they are the most effective individual jammer locations.

Utility	**Jammer Locations**	
14.48	l1	l2
15	l1	l3
15.07	l2	l3
15.65	l1	l4
15.75	l2	l4
16.19	l3	l4

Table 4. Utility values for placement of two jammers (node density)

2. Source and Destination Nodes

We consider five jammer locations in close proximity to the five source and destination nodes (Figure 4). Since we base the objective function on the amount of flow between source and destination nodes, we speculate that jammer locations within range of these nodes will have considerable effects.

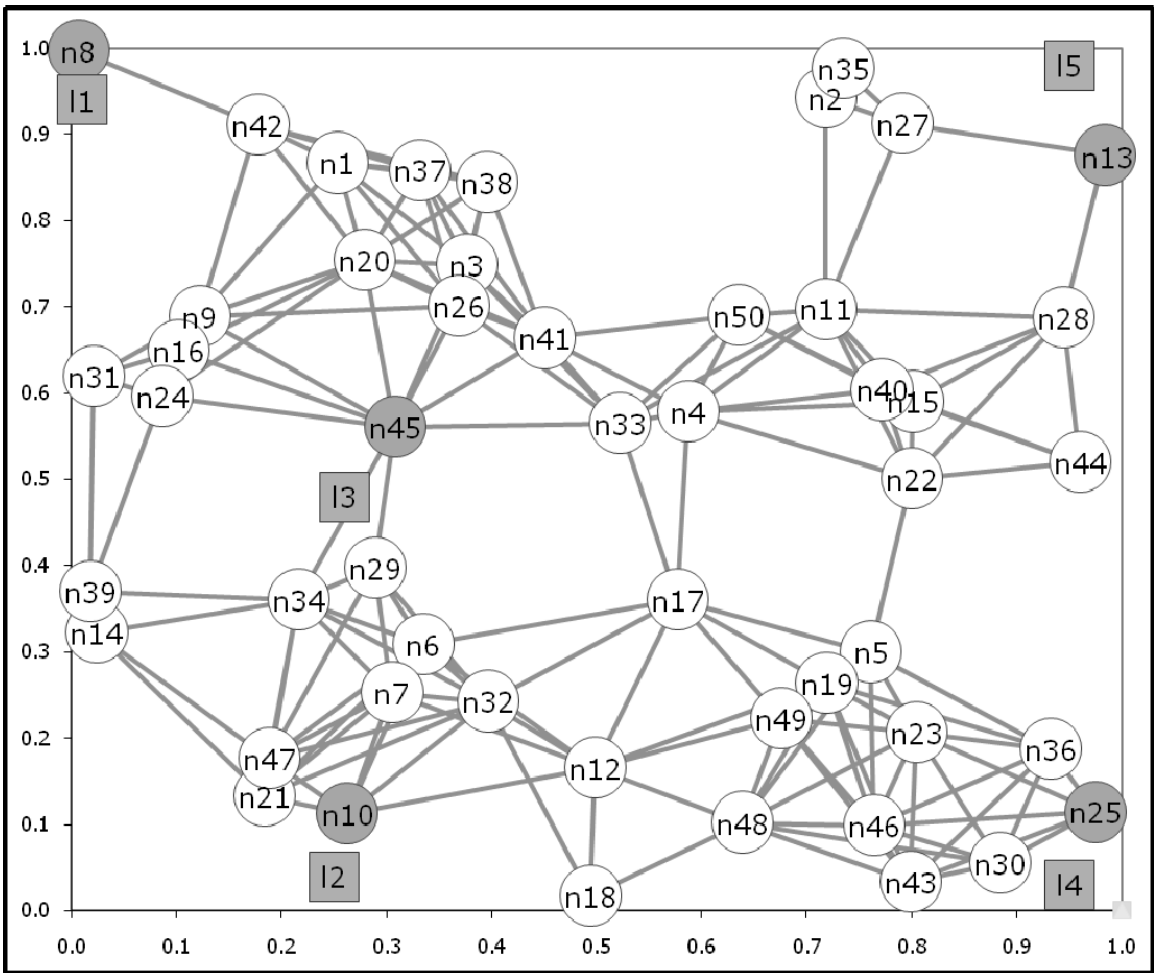

Figure 4. Jammer locations near sources and destinations

We produce a larger range of utility values with these jammer locations (Table 5). l1 is the most effective jammer location. This is because l1 adds interference to n8 and most of its adjacent transshipment nodes. This significantly decreases the flow at n8 and consequently decreases the flow at the other source and destination nodes. l5 is the next

most effective jammer location. Similar to l1, l5 is within close range of n13 and its two adjacent transshipment nodes. By interfering with all three of these nodes, l5 reduces the flow at n13 and the rest of the source and destination nodes. l2, l3, and l4 are located near n10, n45, and n25 respectively. These source and destination nodes are different from n8 and n13 in that they have several adjacent arcs and transshipment nodes. Many of these adjacent transshipment nodes are minimally affected by the jammer interference and allow more flow to pass through them.

Utility	Jammer Location
14.01	l1
14.39	l5
16.02	l4
16.6	l3
16.7	l2

Table 5. Utility values for placement of one jammer (supply and destination)

As before, the two best individual jammer locations appear in the most effective pair of jammer locations (Table 6). However, that logic does not follow for all scenarios. When we activate different jammer locations, we reroute flows and redistribute resources by solving a different SRRA formulation for each scenario. Therefore, an individual jammer location's performance ranking may not intuitively lead to the ranking of a pair of jammer locations. For example, one might expect l3 and l4 to be more effective than l2 and l4. However, the results are actually identical.

Utility	Jammer Locations	
11.19	l1	l5
12.79	l1	l4
13.18	l4	l5
13.4	l1	l3
13.47	l1	l2
13.86	l3	l5
13.88	l2	l5
15.5	l2	l4
15.5	l3	l4
16.06	l2	l3

Table 6. Utility values for placement of two jammers (supply and destination)

3. Network Cut

We notice four locations where arcs divide the network into two distinct lower and upper sections. We consider four jammer locations on these arcs to produce a network cut and assume that this division will restrict flow between these sections (Figure 5). We base this assumption on the max flow-min cut concept (Leighton, 1999). Furthermore, we believe that this reduced flow will significantly reduce the objective function.

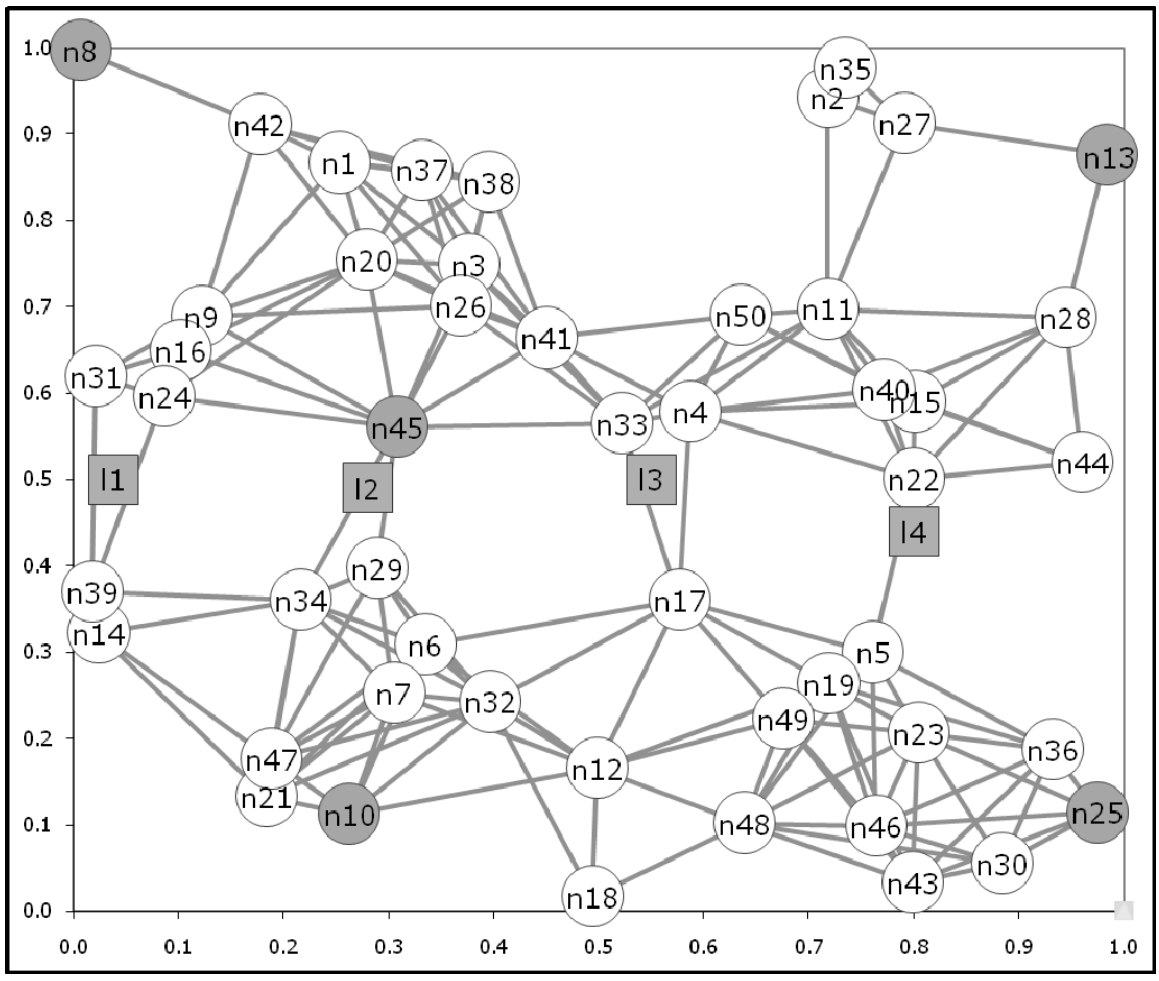

Figure 5. Jammer locations (network cut)

We first analyze the effect of each individual jammer location on the network. We see a generally weak effect on the total utility (Table 7). l2 is the most

effective jammer location because it directly restricts the flow on n45. The effect of the other jammer locations is almost negligible because many other paths exist for communication between source and destination nodes.

Utility	Jammer Location
16.66	l2
17.04	l1
17.08	l3
17.14	l4

Table 7. Utility values for placement of one jammer (network cut)

When we place jammers at two locations, we get similar results (Table 8). The effect of the jammer locations is almost insignificant. We also achieve similar effects from placing jammers at all four locations (Table 9).

This strategy is mediocre because source and destination nodes can still communicate within their own portion of the network. The objective function rewards the network for flow that enters and exits the five source and destination nodes. As long as all source and destination nodes exchange one unit of flow between each other, there is no penalty for sharing the majority of flow with fewer peers. In the case where we place jammers at all four jammer locations, a minimal amount of flow moves between the lower and upper portion of the network.

Utility	Jammer Locations	
16.4	l2	l3
16.46	l1	l2
16.5	l2	l4
16.86	l1	l3
16.91	l1	l4
16.96	l3	l4

Table 8. Utility values for placement of two jammers (network cut)

Utility	Jammer Locations			
15.66	l1	l2	l3	l4

Table 9. Utility value for placement of four jammers (network cut)

D. ENUMERATING ALL POSSIBLE SOLUTIONS

We consider a simple grid of potential jammer locations, spaced 0.1 units apart. By evaluating each of these 121 possible locations, we find the most effective solutions and verify the conclusions gained in the previous strategies.

1. Most and Least Effective Jammer Locations

We evaluate all 121 potential jammer locations for the placement of one jammer and find the most and least effective jammer locations in the network. The results support our prior conclusions.

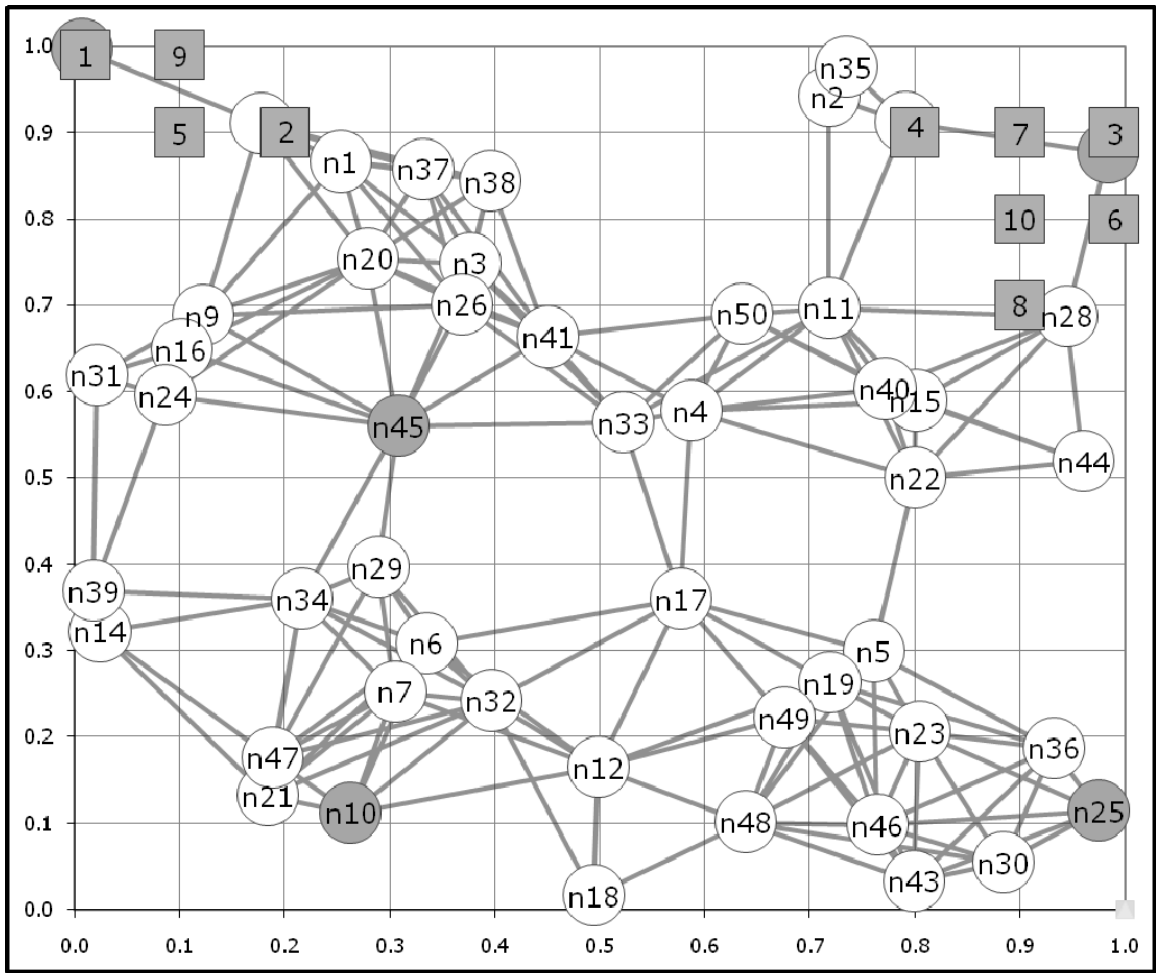

Figure 6. Ten most effective jammer locations

The most effective single jammer labeled 1 (Figure 6). This is consistent with earlier conclusions. n8 is almost a single point of failure because it has one adjacent arc. Placing a jammer near n8 or its adjacent node causes a significant decrease in utility. We see a similar result near n13 because it has only two adjacent arcs. We illustrate the results in Table 10.

Utility	Jammer Location
3.44	1
11.13	2
12.32	3
14.42	4
14.74	5
14.9	6
14.91	7
14.96	8
15.1	9
15.12	10

Table 10. Utility values for most effective jammer locations

Like the previous scenarios, the most effective pair of jammer locations is comprised of the two most effective individual jammer locations. We note that the utility achieved by placing a jammer at both 1 and 2 is negative. We also note that the most effective jammer is included in all of the pairs in Table 11. These results are a natural extension of the nature of the log-utility objective function (Chapter II, Section A-2).

Utility	Jammer Locations	
-1.81	1	2
-1.46	1	3
0.84	1	4
1.18	1	6
1.21	1	7
1.40	1	8
1.46	1	10

Table 11. Utility values for most effective pairs of jammer locations

The chart in Figure 7 shows a comparison of the 30 most effective placements of one or two jammers in the network. In the case of one jammer, we note that only the five best locations have an extremely significant effect on the network. The other locations are similarly weak in comparison. In the case of two jammers, one jammer is always located next to a source and destination node. In the 30 best cases, that jammer is always located near n8.

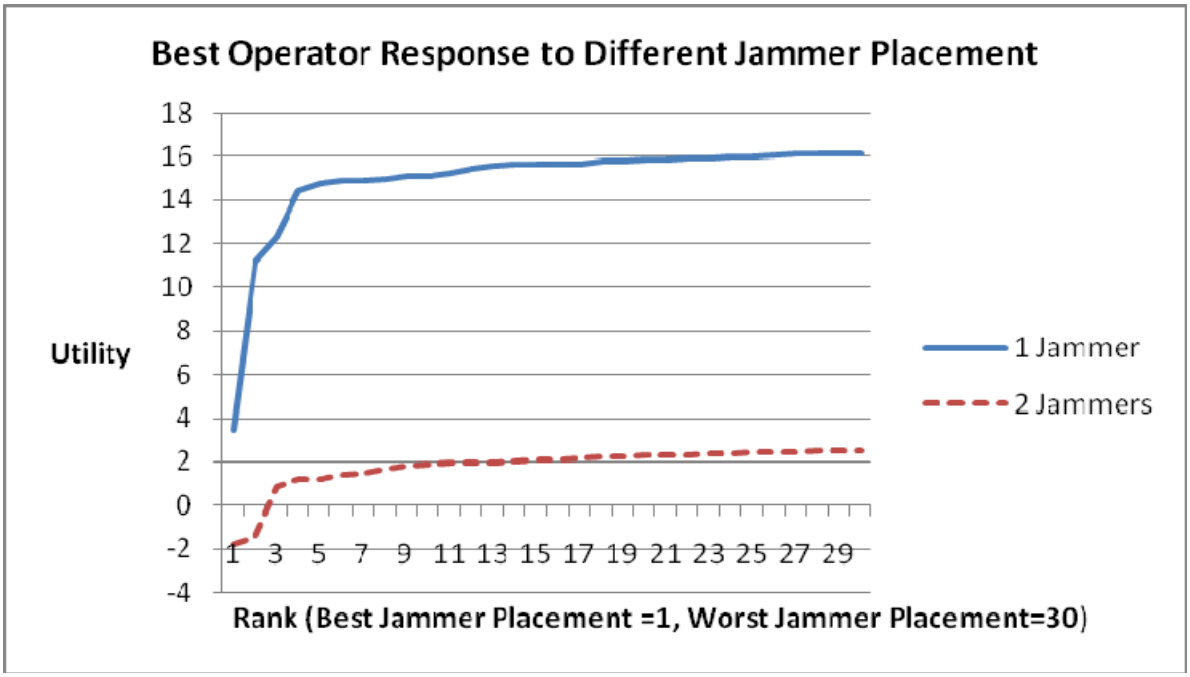

Figure 7. Best operator response to different jammer placement

We further validate our conclusions by observing the ten least effective jammer locations (Figure 8).

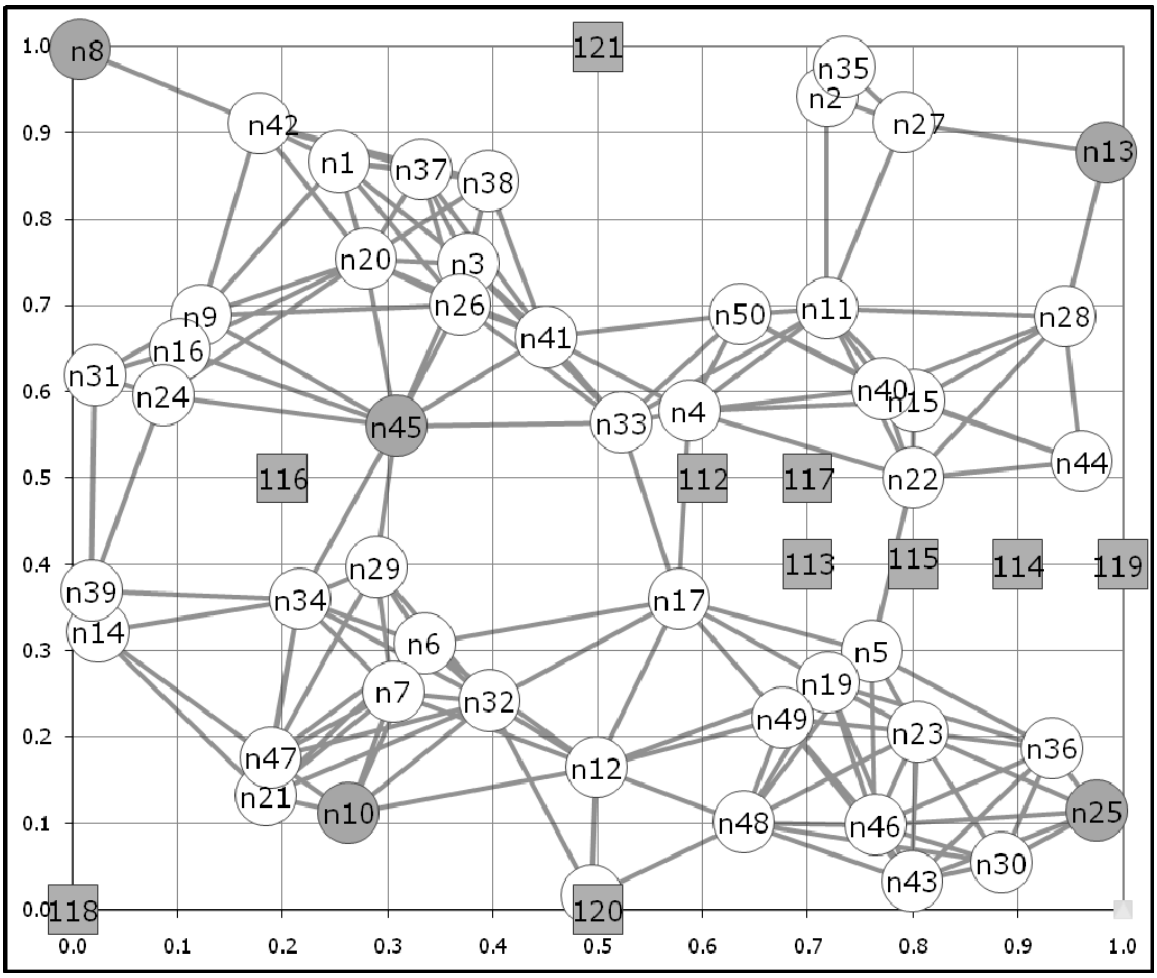

Figure 8. Ten least effective jammer locations

Note that location 121 does not have any effect on the network because it is not within effective range of any of the nodes. The other jammer locations have little effect for the same reasons we found previously. Most of them are far from source and destination nodes. Several are near transshipment nodes that are not critical to flows along the network. This supports our prior conclusions.

The placement of individual jammers at locations 112-121 yields utility in range [17.09, 17.24]. The placement of two jammers at locations 112-121 yields utility in range [17.09, 17.13]. We note that the utility with no jammers in 17.24.

We show the results of enumerating all 121 jammer locations within a contour map in Figure 9 that highlights effective jammer placement with dark areas and ineffective jammer placement with light areas. Such a figure can serve as a decision support tool for commanders to understand where to allocate security assets.

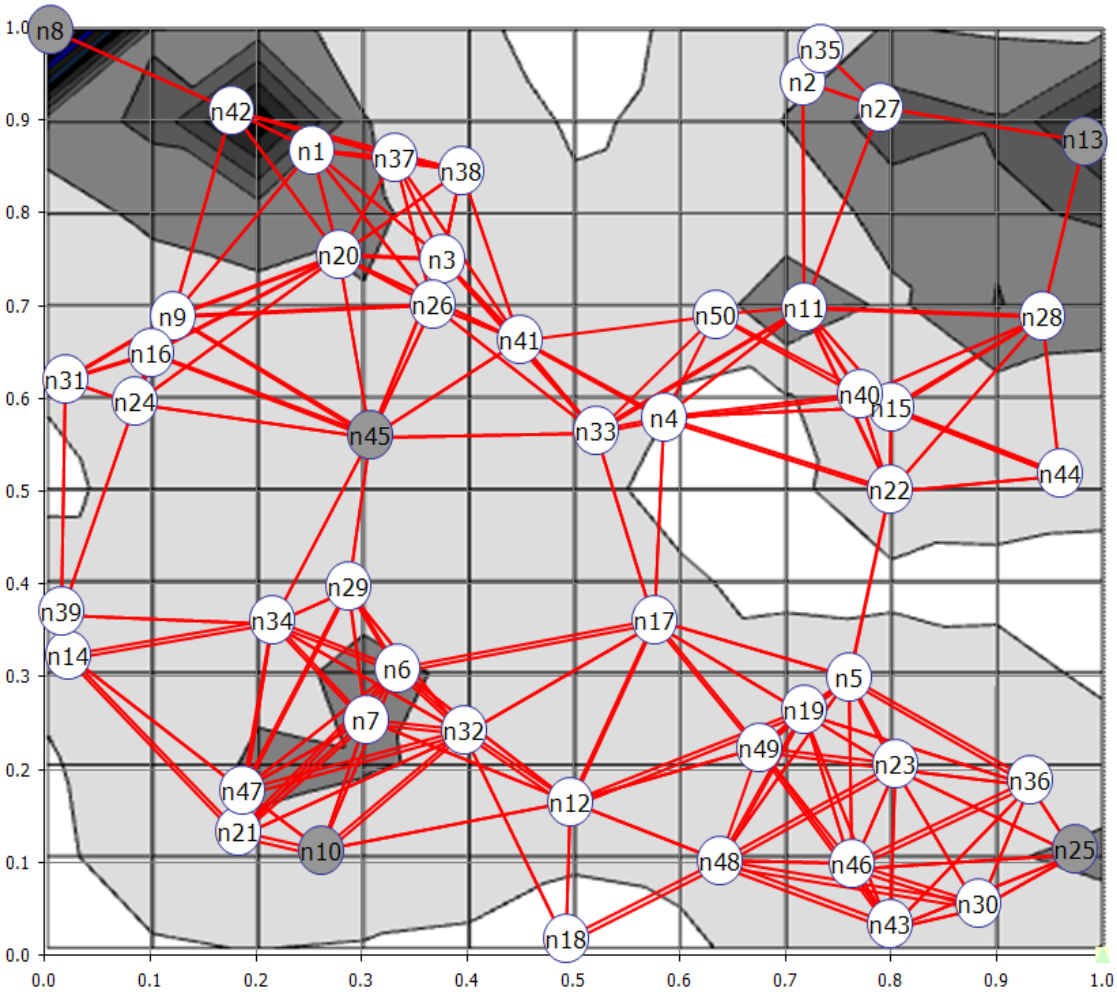

Figure 9. The effect of placing one jammer

We note that the majority of the network contains regions where the placement of a single jammer is equally effective. As expected, placing a jammer near source and destination nodes is the most effective attack. However, other options are available as well. We can place a jammer near n11, n28, n6, or n7 and achieve effective results. In fact, the results can be as effective as placing a jammer near n25 or n10. We also see that placing a jammer near n4 or n18 is almost completely ineffective. We presume that those nodes have limited flow passing through them.

2. Secured Source and Destination Nodes

We find that placing jammers near source and destination nodes is the most effective strategy for reducing the log-utility of flows in a wireless network. However, this may not be a realistic approach in practical application. It is likely that commanders will surround source and destination nodes with considerable security. This can include a fixed perimeter defense in addition to roving patrols. This defensive posture may make it difficult to place jammers within an effective range of source and destination nodes. Additionally, other security obstacles may arise that prevent an attacker from placing a jammer in a given location.

We consider the 30 most effective jammer locations outside a 0.25 unit radius of all of the source and destination nodes and denote them (C1,…C30). The results show that these candidate locations are near critical transshipment nodes (Figure 10).

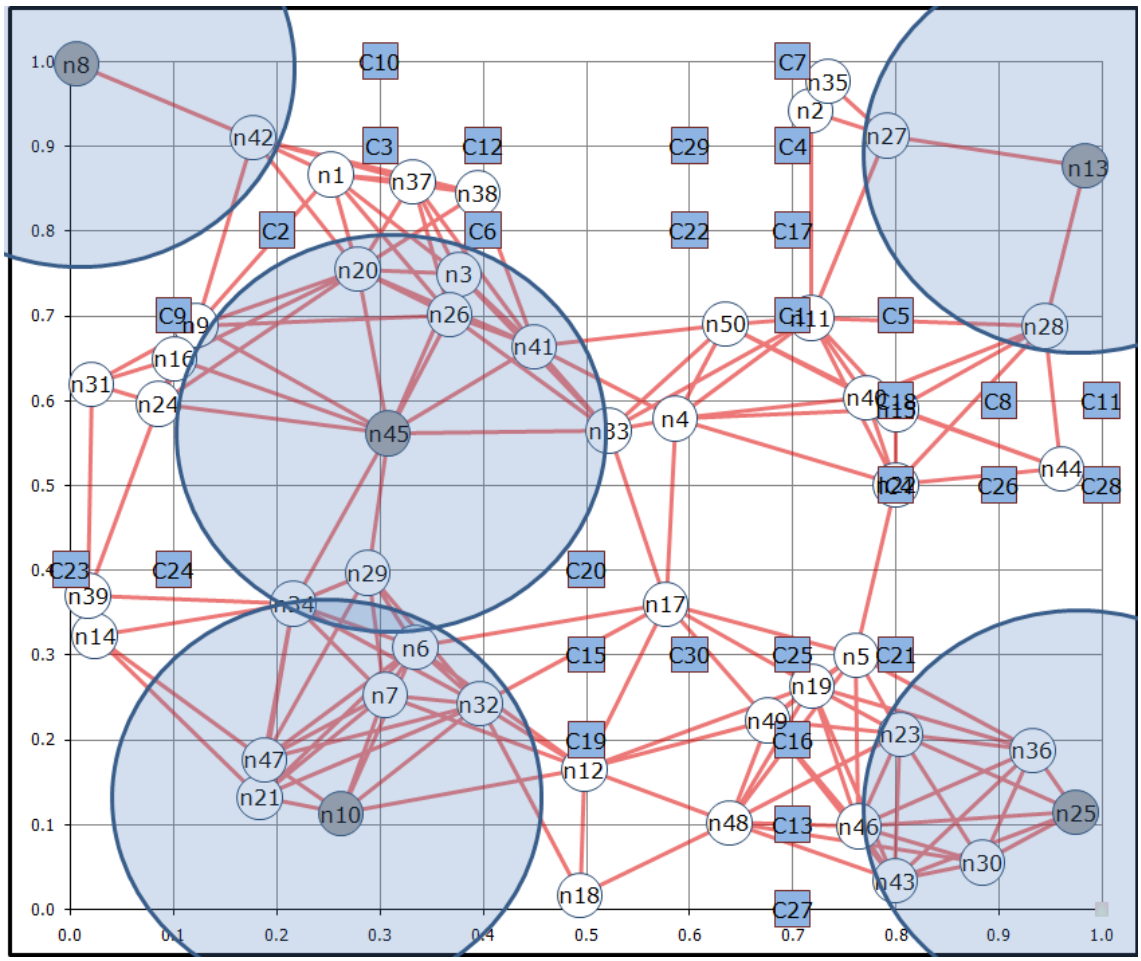

Figure 10. 30 most effective jammer locations not near source and destination nodes

We take a closer look at the 15 most effective jammer locations outside a 0.25 unit radius of all of the source and destination nodes (Figure 11). The jammer locations surround critical transshipment nodes near n8 and n13. This is not surprising since those nodes have few adjacent arcs.

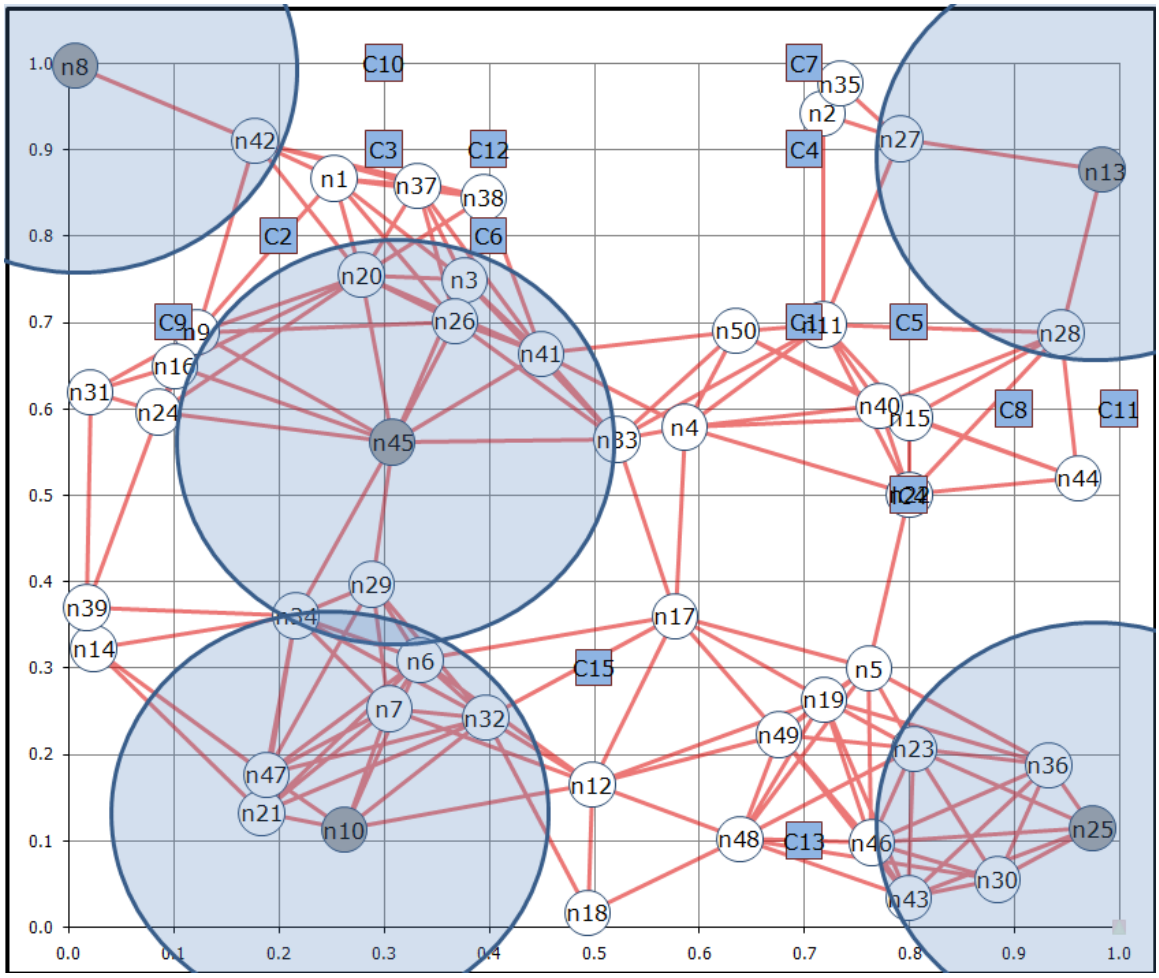

Figure 11. 15 most effective jammer locations not near source and destination nodes

We evaluate the effectiveness of placing the one, two, three, or four jammers at the best available locations outside the perimeter of source and destination nodes (Figure 12). We find that this strategy can be more effective than placing jammers near some of the source and destination nodes. For instance, placing jammers near transshipment nodes adjacent to n13 and n8 is more effective than placing jammers next to n10, n45, or n25. Note that the best combination of four jammers outside the protected perimeter has a lesser effect than a single jammer placed next to a source or destination node.

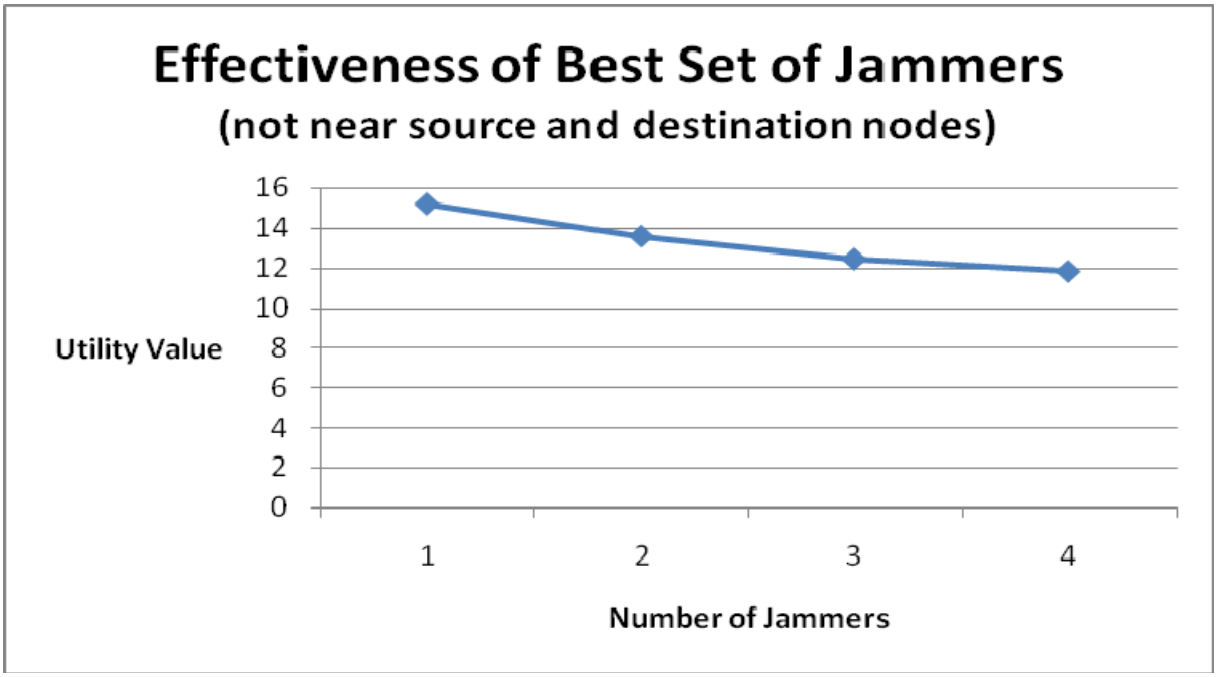

Figure 12. Results of the most effective jammer location sets not near source and destination nodes

We rank each of the 30 best individual jammer locations and pairs of jammer locations not near source and destination nodes in Figure 13. Excluding the very best candidate locations, most of them have a very similar effect on the network.

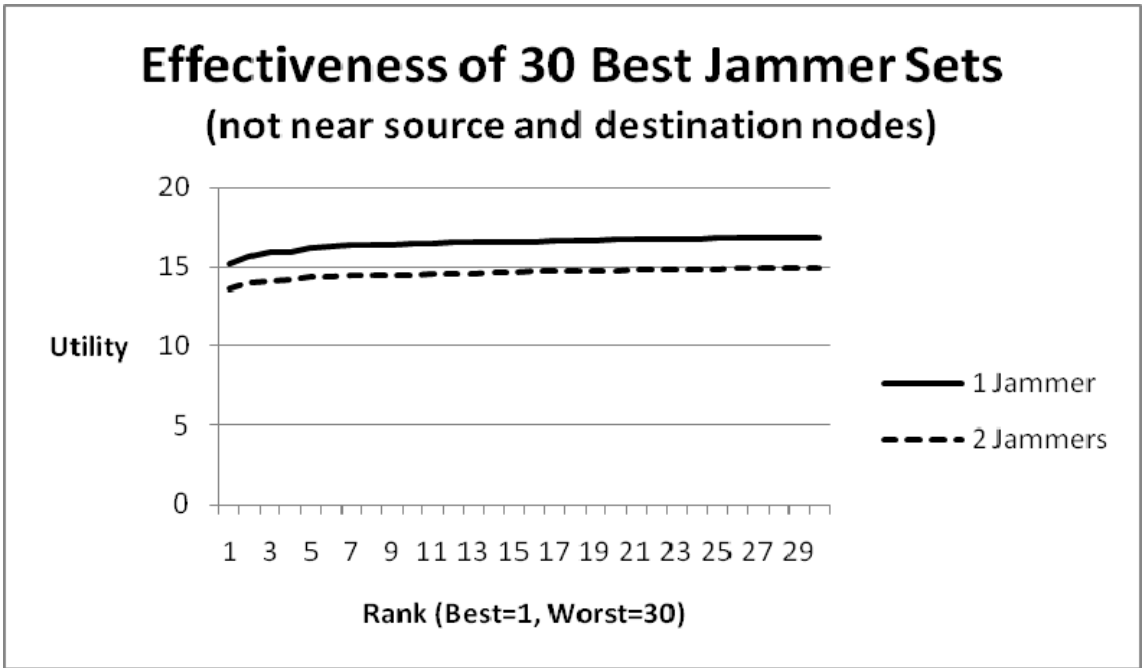

Figure 13. Results of the most effective jammer location sets not near source and destination nodes

E. SUMMARY AND DISCUSSION

We find that the most effective placement of a single jammer is near a source or destination node. However, if that is not an option, placing a jammer near a transshipment node with a large amount of flow moving through it can produce similar results. The network cut does not produce effective results under the log-based objective function. Placing a jammer where the node density is high can be effective, but only if the jammer is near transshipment nodes that have a high amount of flow passing through them. We portray these results in Figure 14.

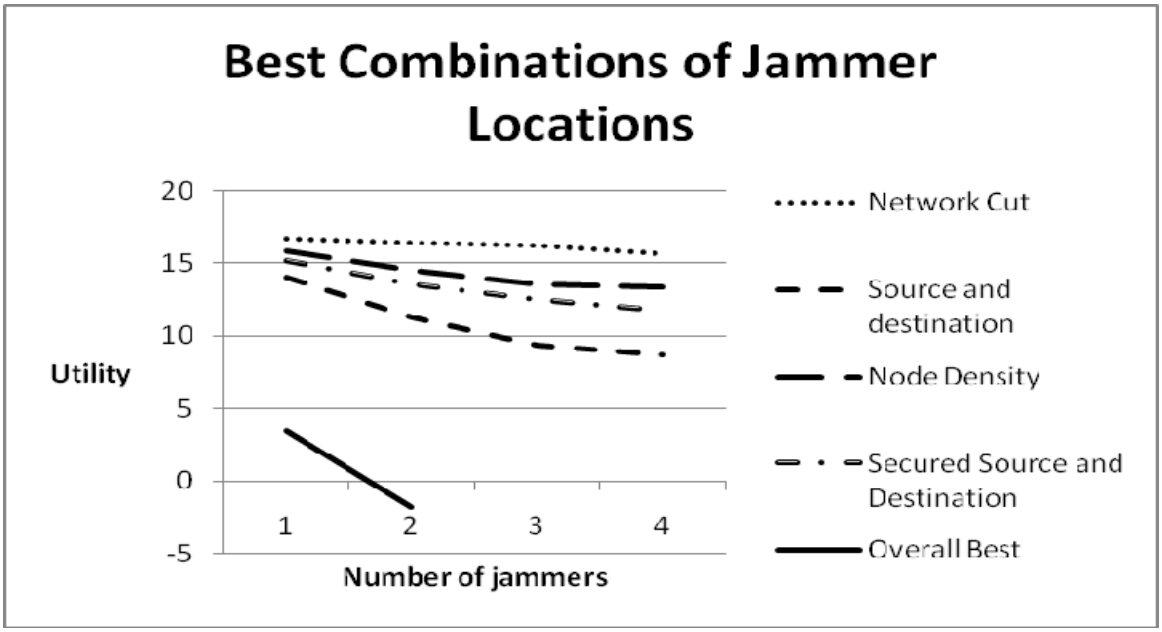

Figure 14. Results of the most effective jammer location sets among different heuristics

IV. SUMMARY AND CONCLUSIONS

The tools developed in this thesis provide commanders with a quantitative means of optimizing network resource allocation and assessing the effect of jamming devices within a network. This will enable commanders to employ these systems more effectively in training and real-world operations.

We developed an interdiction model that determines the effect of jammers on the utility of a wireless network with optimized routing and resource allocation. To our knowledge, this is the first attempt to apply bi-level models to this problem. We analyzed the effects of this model on a sample network. We found that the most effective placement of a jammer is near source and destination nodes or transshipment nodes that have a large amount of flow passing through them. Placing jammers at other locations provides little or no effect on the network.

The examples in this thesis contain several assumptions that may not be realistic in practice. We can adjust these assumptions to reflect a given real-world scenario. For example, we can vary the capabilities of the nodes and jammers, rather than keeping all of them uniform. We can also consider directional jammers instead of the omni-directional jammers portrayed in this thesis. We can consider various objective functions to reflect better the goals of the network manager.

We have developed a decision support tool that facilitates the rapid analysis of other networks having various characteristics. This can include the portrayal of terrain and security obstacles, increased electromagnetic interference, and single points of failure. We can also extend the research beyond the realm of local area networks. Examples include satellite networks, cellular phone networks, and GPS networks.

This thesis portrays a network that uses frequency division multiple access (FDMA). The work can be extended to study other types of modulation including code-division multiple access (CDMA), time division multiple access (TDMA), and random access protocols (Xiao, 2004). We also assume that packet loss and the overall quality of service have no effect on the formulation (Xiao, 2004). In reality, those are primary concerns for military commanders.

We also assume that the *attacker* and *defender* (network operator) have perfect information about the network. This is the underlying assumption behind the SRRA-Attack formulation in this thesis. Each party knows every detail including the capabilities and ranges of every node and jammer, the noise associated with every receiver, and the existence and location of every link in the network. This is, of course, unrealistic for a practical setting. We can compare scenarios where the attacker makes assumptions about the network topology in comparison to where he has perfect information. We can use these comparisons to deem the value of information and how it can affect the attacker's choices.

LIST OF REFERENCES

[1] G. Brown, M. Carlyle, J. Salmeron, K. Wood (2006). "Defending Critical Infrastructure." Interfaces, Volume 36, Number 6, pp. 530-544.

[2] T. Cover, J. Thomas (1991). "Elements of Information Theory." John Wiley & Sons, Inc., New York.

[3] GAMS Development Corporation (2008). "General Algebraic Modeling System (GAMS)." Retrieved on June 16, 2008, from GAMS website: http://www.gams.com/.

[4] R. Hayden, R. Rientjes, W. Ryder, R. Wall (2006). "Wireless technologies: A knowledge opportunity on developing countries." Educational Technology Research and Development, Volume 49, Number 3, pp. 115-118.

[5] M. Johansson, L. Xiao, S. Boyd (2003). "Simultaneous Routing and Power Allocation in CDMA Wireless Data Networks." IEEE International Conference on Communications, Volume 1, pp. 51-55.

[6] M. Johansson, L. Xiao (2004). "Scheduling, Routing, and Power Allocation for Fairness in Wireless Networks." IEEE Vehicular Technology Conference, Volume 3, pp. 1355-1360.

[7] "Joint Doctrine for Electronic Warfare" (2000). Department of Defense.

[8] T. Leighton, S. Rao (1999). "Multicommodity max-flow min-cut theorems and their use in designing approximation algorithms." Journal of the ACM, Volume 46, Issue 6, pp. 787-832.

[9] M. Neely, E. Modiano, C. Rohrs (2005). "Dynamic Power Allocation and Routing for Time-varying Wireless Networks." IEEE Journal on Selected Areas in Communications, Volume 23, pp. 89-103.

[10] M. Resende (Ed.), P. Pardalos (Ed.) (2006). Handbook of Optimization in Telecommunications. Springer.

[11] L. Rosati, G. Reali (2006). "Jointly Optimal Routing and Resource Allocation in Hybrid Satellite/Terrestrial Networks." 2006 International Workshop on Space and Satellite Communications, pp. 29-33.

[12] M. Stahlberg (2000). "Radio Jamming Attacks against Two Popular Mobile Networks." 2000 Seminar on Network Security.

[13] L. Xiao, M Johansson, S. Boyd (2004). "Simultaneous Routing and Resource Allocation." IEEE Transactions on Communications, Volume 52, pp. 1136-1144.

[14] Stanford Business Software (2008). “Mixed Integer Nonlinear Optimization Solver (MINOS).” Retrieved on June 16, 2008 from http://www.sbsi-sol-optimize.com/asp/sol_product_minos.htm .

[15] W. Xu, W. Trappe, Y. Zhang, and T. Wood (2005). “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks.” Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing, pp. 46-57.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Commanding General, Training and Education Command
   MCCDC, Code C46
   Quantico, Virginia

4. Director, Marine Corps Research Center
   MCCDC, Code C40RC
   Quantico, Virginia

5. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

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

7. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

8. MCCDC OAD Liaison to Operations Research Department
   Naval Postgraduate School
   Monterey, California

9. David Alderson
   Naval Postgraduate School
   Monterey, California

10. Hong Zhou
    Naval Postgraduate School
    Monterey, California

11. W. Matthew Carlyle
    Naval Postgraduate School
    Monterey, California

12. Brian Steckler
    Naval Postgraduate School
    Monterey, California