NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

OPTIMIZING C4ISR NETWORKS IN THE PRESENCE OF ENEMY JAMMING

by

Sean M. Andrews

March 2010

Thesis Advisor:	W. Matthew Carlyle
Second Reader:	David L. Alderson

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Optimizing C4ISR Networks in the Presence of Enemy Jamming			**5. FUNDING NUMBERS**
6. AUTHOR(S) Sean M. Andrews			
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) Naval Air Weapons Center, Weapons Division			**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. IRB Protocol Number _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**
13. ABSTRACT (maximum 200 words) U.S. Navy forces are becoming increasingly dependent upon the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) networks that support them. This network is critical to the task of quickly putting effective weapons on important targets. Today, the delivery of weapons by U.S. Navy air and surface forces is increasingly dependent upon critical targeting information that is often provided by a network of third-party sensor and communication systems. Along with this increasing dependence is a growing threat to this network by enemy forces. Thus, an understanding of network capabilities and vulnerabilities is critical to the ability of our naval forces to successfully engage an adversary. The focus of this research is to develop a bi-level (attacker-defender) optimization model that enables us to map any current or planned C4ISR network requirements needed to execute a successful kill chain, and to uncover any vulnerabilities within the network.			
14. SUBJECT TERMS Attacker-Defender Model, Communications Networks, Network Vulnerabilities			**15. NUMBER OF PAGES** 69
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** 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

OPTIMIZING C4ISR NETWORKS IN THE PRESENCE OF ENEMY JAMMING

Sean M. Andrews
Lieutenant Commander, Supply Corps, United States Navy
B.S., United States Naval Academy, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
March 2010

Author: Sean M. Andrews

Approved by: W. Matthew Carlyle
Thesis Advisor

David L. Alderson
Second Reader

Robert F. Dell
Chairman, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

U.S. Navy forces are becoming increasingly dependent upon the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) networks that support them. This network is critical to the task of quickly putting effective weapons on important targets. Today, the delivery of weapons by U.S. Navy air and surface forces is increasingly dependent upon critical targeting information that is often provided by a network of third-party sensor and communication systems. Along with this increasing dependence is a growing threat to this network by enemy forces. Thus, an understanding of network capabilities and vulnerabilities is critical to the ability of our naval forces to successfully engage an adversary. The focus of this research is to develop a bi-level (attacker-defender) optimization model that enables us to map any current or planned C4ISR network requirements needed to execute a successful kill chain, and to uncover any vulnerabilities within the network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

BDA	Battle Damage Assessment
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CTR	Cell Tower Relay
GAMS	General Algebraic Modeling System
GUI	Graphical User Interface
ILP	Integer Linear Program
JOC	Joint Operations Center
SAT	Satellite
SOF	Special Operations Forces
TACAIR	Tactical Air
TOC	Tactical Operations Center
UAV	Unmanned Aerial Vehicle
UGS	Unmanned Ground Sensors

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Warfare Analysis and Integration Department within the Naval Air Systems Command is investigating current and planned Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) networks to understand their strengths and weaknesses. Their goal is to assist in the acquisition of systems that will make them stronger, faster, and more resilient in the face of an increasing demand for their services and increasing threats from our adversaries. Part of this effort is to characterize the structure, capabilities, and objectives of these networks with mathematical and computer models.

The focus of this research is to develop a bi-level (attacker-defender) optimization model that enables us to map any current or planned C4ISR network requirements needed to execute a successful kill chain, and to uncover any vulnerabilities within the network.

Today, the delivery of weapons by U.S. Navy air and surface forces is increasingly dependent upon critical targeting information that is often provided by a network of third-party sensor and communication systems. Along with this increasing dependence, is a growing threat to this network by enemy forces. Thus, an understanding of network capabilities and vulnerabilities is critical to understanding the ability of our naval forces to successfully engage an adversary.

We consider how changes to current network configurations based on modes of communication, asset placement, and enemy delay options can lessen network vulnerabilities to an enemy attack. The systematic study of these alternatives requires significant network optimization by implementing electronic countermeasures, modification, and additional communications links.

Our model provides optimal solutions for jammer placement and then is able to determine optimal communication paths based on those fixed jammer placements. Specific insights include redundant pathways, geographic separation of key nodes, and additional communications links.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to thank my wife, Cheryl, for her support throughout this entire process. Without her support and encouragement, the process would have been much more arduous.

Professor Matthew Carlyle, I appreciate your time, knowledge, direction, and patience during this thesis process and ensuring I stayed on the right path. It has been a challenging, but worthwhile, experience. I have gained an astonishing amount of knowledge from the time I have spent learning from you.

Professor David Alderson, thank you for lending me your time and experience towards the completion of this thesis.

Ken Amster, thanks for taking me on as a thesis student and providing me with the means and guidance to complete this thesis.

Finally, I would like to thank the professionals at China Lake for your hospitality and assistance during my visit to your distinguished organization.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND AND OVERVIEW

U.S. Navy forces, whether they are involved in conventional conflicts or hybrid warfare, are becoming increasingly dependent upon the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) networks that support the execution of their operation. These networks are critical to the task of putting weapons on targets. The process of putting a weapon on a target is known as a *kill chain*, and is divided into a series of six distinct steps:

- Find – locate target of possible interest,
- Fix – isolate target,
- Track – observe target continuously,
- Target – decide target is of interest,
- Engage – attack to with weapon with intent to destroy, and
- Assess – determine if attack success.

Today, the delivery of weapons by United States Navy air and surface forces is dependent upon critical target location information that is often provided to weapons and platforms by third party sensor systems forming our network. This increasing dependence on distributed series of information transmissions is made riskier by growing threats to these networks by enemy forces. Thus, an understanding of C4ISR network capabilities and vulnerabilities is critical to understanding the ability of our naval forces to successfully engage an adversary.

B. PROBLEM STATEMENT

The Warfare Analysis and Integration Department within the Naval Air Systems Command is investigating current and planned C4ISR networks to understand their strengths and weaknesses. Their goal is to assist in the acquisition of systems that will make them stronger, faster, and more resilient in the face of an increasing demand for

their services and of increasing threats from our adversaries. Part of this effort is to characterize the structure, capabilities, and objectives of these networks with mathematical and computer models (K. Amster, personal communication, July 17, 2009).

Currently, the Warfare Analysis and Integration Department at the Naval Air Systems Command uses a set of standard protocols for establishing and configuring communications networks (K. Amster, personal communication, July 17, 2009). Primary concerns focus simply on C4ISR network connectivity and most, if not all, networks are set up on an ad-hoc basis. In most cases, this is adequate, but it can leave a C4ISR network vulnerable to enemy attack.

The focus of this research is to develop a bi-level (attacker-defender) optimization model that enables us to map any current or planned C4ISR network requirements needed to execute a successful kill chain, and to uncover any vulnerabilities within the network. *Vulnerabilities* are described as a set of communications links whose loss or degradation has a significant impact on the performance of the C4ISR network.

Some of the questions we address are:

- How vulnerable is a particular C4ISR network to an adversary's attempt to disrupt it?
- How can we harden or modify the structure of a C4ISR network to reduce the adversary's ability to disrupt?
- How flexible is a C4ISR network in the face of a changing war-fighting environment?

C. SCOPE AND LIMITATIONS

We model the vulnerability of a C4ISR network using a bi-level (attacker-defender) optimization model, with the *attacker* being an enemy jamming our communications capabilities, and the *defender* being the operator(s) of the communications network. A typical network is designed to transmit three separate *modes* of communication, each with its own separate sub-network. Those modes are voice, data, and imagery transmissions. Our operator model of a single C4ISR network determines optimal (i.e., minimal time) communications flows to complete a kill chain, and our

attacker-defender model pinpoints vulnerabilities in the system, allowing us to determine hardening and optimization of current and future systems.

The operator model explicitly models a single C4ISR network and determines optimal communications flows in the absence of interference. The model determines the shortest paths from source to destination of individual messages minimizing the total transmission and processing time of all communications in a network.

The attacker-defender model explicitly considers an attacker's capability to jam, or interfere with, communications. Jammers can cause interference with reception of signals of one or more modes of communication at one or more nodes in our C4ISR network, depending on the jammer type and placement.

The baseline scenario consists of a fictional strike plan where a communications network is established in order to locate and eliminate an enemy threat. The communications network is comprised of the following assets (or nodes):

- Joint Operations Center,
- Tactical Operations Center,
- Satellite,
- Tactical Air,
- Cell Tower Relay,
- Special Operations Forces,
- Unmanned Aerial Vehicle – Large,
- Unmanned Aerial Vehicle – Small, and
- Unmanned Ground Sensors.

These assets are responsible for tracking and targeting a lone enemy contact. The communications infrastructure consists of landlines, satellite communications, cell phone, line of sight radio, data uplinks, and unmanned aerial vehicle control to relay information and ensure a successful mission.

Each step in the kill chain (Find, Fix, Track, Target, Engage, and Assess) requires the receipt of information at a node (or nodes), within the network. Nodes are points in the network at which information signals are either transmitted or received. The

progression from one step to the next occurs only after specific actions are taken and the transmission of information to another node or set of nodes is complete.

Several modifications to the baseline scenario are modeled. These modifications include implementation of electronic countermeasures to interrupt the effects of jammers, changing node locations and configurations, and adding communications links to our network to provide alternative communication pathways.

D. RESULTS

All models and scenarios tested solve in fractions of a second, and preliminary testing indicates these models scale up to larger, more complex networks with only moderate increases in runtime.

Our baseline scenarios show significant vulnerabilities. As little as two jammers can produce considerable delays in communications flow. We observe increases in transmission and processing times for communications ranging from 47% to 126% times greater than optimal communications flow.

Follow-on scenarios show resiliency through the implementation of electronic countermeasures, modification or configuration changes, and reinforcement through additional links within the communications network. With these measures in place, jammers have little effect on communications flows and incur only slight increases in transmission and processing times for communications. Increases top off at only 15%.

We conclude that vulnerabilities exist when networks have limited ability to employ countermeasures, confined area of operations, and limited alternate pathways. Resiliency occurs through redundancy of pathways, geographic separations of key nodes, and reinforcement of networks by presenting additional pathways for communications flow.

II. MODEL DEVELOPMENT

A. SCENARIO

Our scenarios model a basic strike plan on a single, stationary target. Assets (or nodes) used to conduct this plan include a Joint Operations Center, Tactical Operations Center, Satellite, Tactical Air (fighter aircraft), Cell Tower Relay (used for mobile cell phone communications), Unmanned Aerial Vehicle—Large, Unmanned Aerial Vehicle—Small, Special Operations Forces, and Unmanned Ground Sensors. Each baseline scenario involves the transfer of communication signals, or messages from one node to another within in the network as part of a kill chain. Each message utilizes one of three modes: voice, imagery, or data. Each step in the kill chain requires the receipt of messages at a node within the network. The progression to the next step occurs after a delay corresponding to specific actions taken at the corresponding node. The scenario is finished upon completion of the "Assess" stage in the kill chain, signaled by the receipt of a "final" message at the destination node.

The enemy has the ability to delay communications through jamming. Jamming is the generation of signals (electromagnetic or infrared) by powerful transmitters in order to block reception of communication, radar, or infrared signals at a receiver. "Radio broadcasts or radio messages can be jammed by beaming a more powerful signal on the same frequency at the area in which reception is to be impaired, using carefully selected noise modulation to give maximum impairment of intelligibility of reception" (Markus & DeLia, 2010). Communication disruption corresponds to a delay in incoming message transmissions to an affected node; due to an increased noise-to-signal ratio. Most communication protocols will require retransmission until a successful receipt has been acknowledged. For example, rather than taking sixty seconds to receive a message, a jammed node might take ninety seconds or longer, depending on the number of retransmissions required. The enemy's objective is to delay communications for as long as possible with their allotted *jammers*. Jamming equipment can be placed by the attacker at any of a set of pre-disclosed *locations*. For this scenario, there are four possible jamming locations, each affecting different sets of C4ISR nodes in the network.

In our scenarios, a jammer has an effective radius range of five miles although this can be made to be dependent on the type of jammer, location, etc. Each jammer has the capability to affect a single mode of communication, but can affect any nodes within its five mile radius. Again, these assumptions are easily generalized to depend on jammer type, geography, etc.

Each asset is associated with at least one node in our network. We use a multi-commodity network flow model of our C4ISR network (see Ahuja, Magnanti, & Orlin, 1993, for a comprehensive discussion on network flow models). Assets that participate in more than one stage in a kill chain, or that move during operation, have multiple node names representing the same asset at different times and locations within the network. Table 1 associates each asset with its corresponding node name(s).

Asset	**Node Name**
Joint Operations Center	JOC
Tactical Operations Center	TOC
Satellite	SAT
Tactical Air	TACAIR1, TACAIR2, TACAIR3
Cell Tower Relay	CTR
Unmanned Aerial Vehicle – Large	UAV1, UAV2, UAV3
Special Operations Forces 1	SOF1
Special Operations Forces 2	SOF2
Special Operations Forces 3	SOF3
Unmanned Aerial Vehicle – Small	UAV_s1, UAV_s2, UAV_s3
Unmanned Ground Sensors 1	UGS1
Unmanned Ground Sensors 2	UGS2

Table 1. Node data

We develop our entire scenario on a single network of nodes to accomplish a strike plan. Figure 1 provides a map of the nodes represented in this network. The only difference between our scenarios is the specific patterns of communication signals used to complete the kill chain. For example, one scenario uses the Joint Operations Center as the decision authority while another uses the Tactical Operations Center as the decision authority. Use of one over the other changes the paths of communication signals, thus increasing or decreasing the completion time of a kill chain and changing the overall exposure of the communicating paths to jamming.

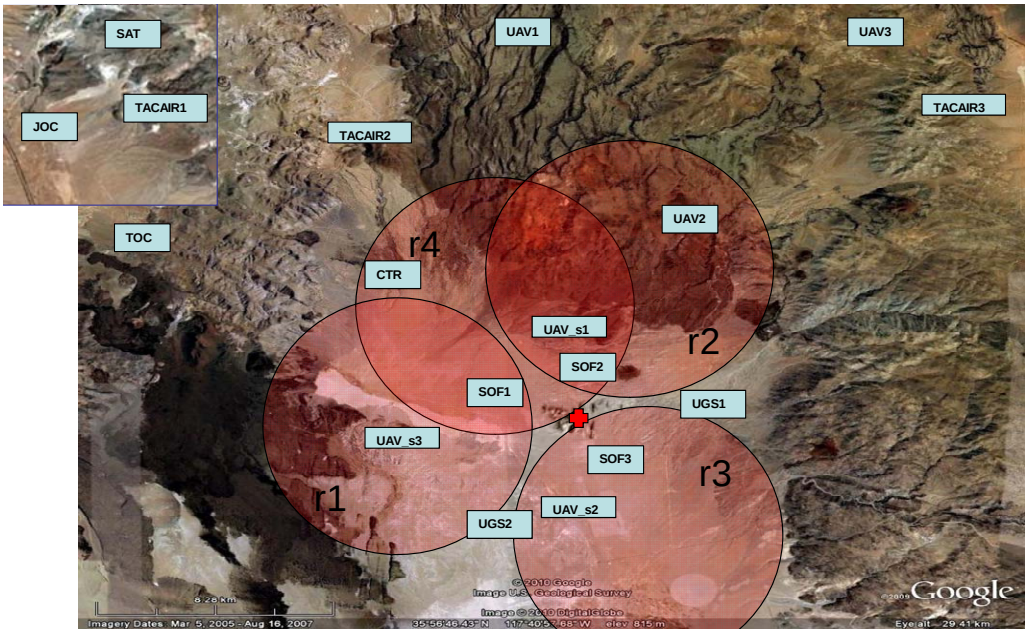

Figure 1. Map of nodes within the communications network (From: Google Maps, March 8, 2010). Each disk indicates 5-mile radius around a potential jamming location. The cross near the center of the SOF nodes indicates a possible target.

The arcs in this network are expressed in terms of the three modes of communication that utilize it. Figures 2, 3, and 4 define these arcs and provide a graphical representation of the different communications flows within our network.

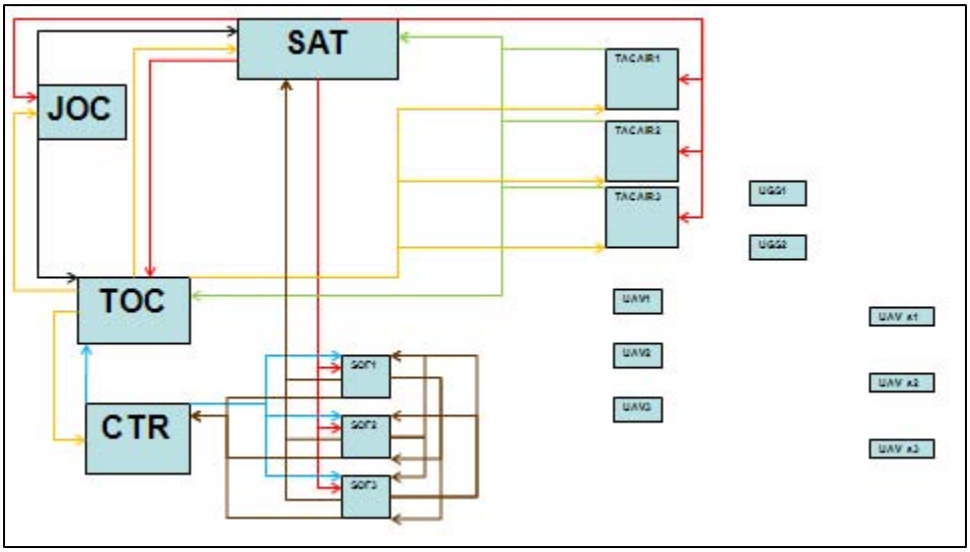

Figure 2. Graphical representation of voice sub-network. Network is not geographically accurate. Individual colors represent arcs from the same source node. For example, all communications flows from JOC are one color, TOC is another, etc.

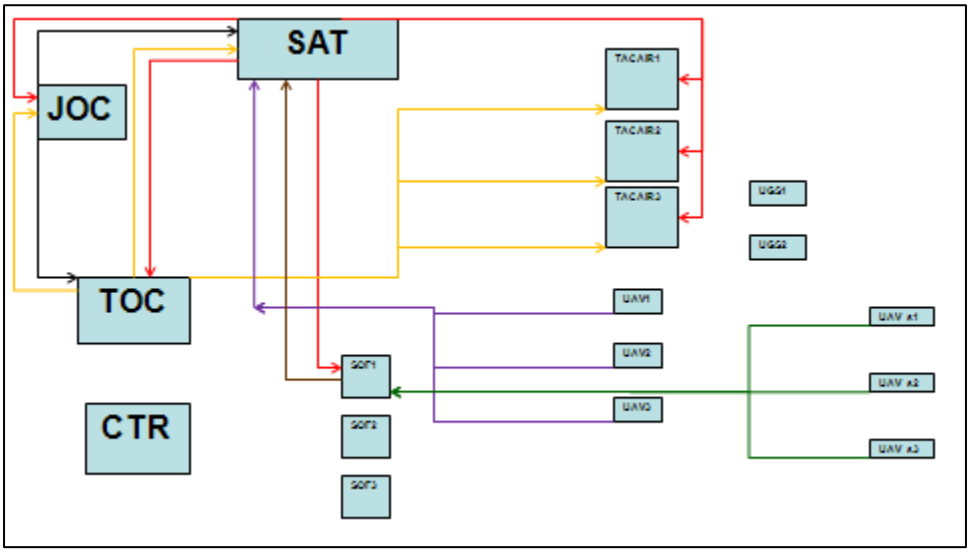

Figure 3. Graphical representation of image sub-network. Network is not geographically accurate. Individual colors represent arcs from the same source node.

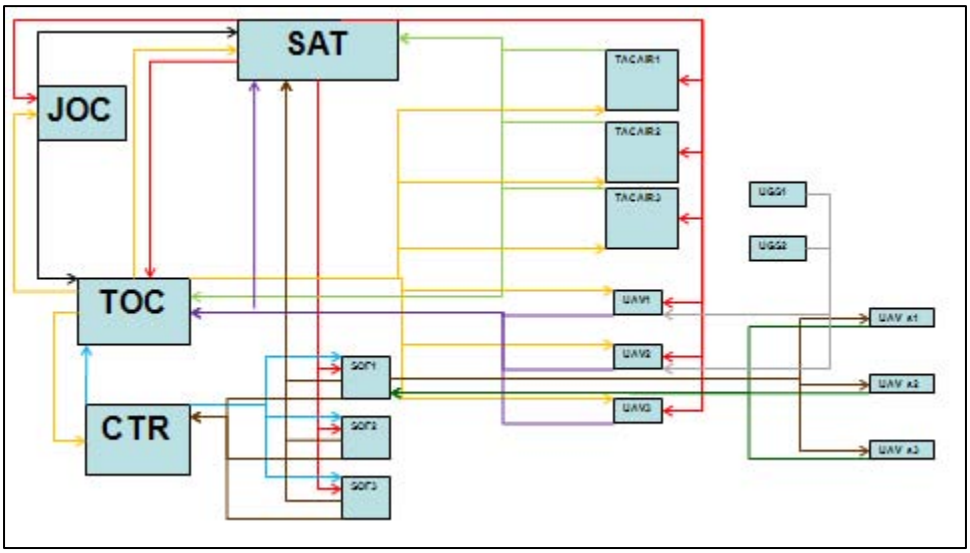

Figure 4. Graphical representation of data sub-network. Network is not geographically accurate. Individual colors represent arcs from the same source node.

1. Scenario Timelines

Each scenario is specified by a *timeline* of communications that correspond to a kill chain. These timelines layout the scenario by the type of information required (commodity) for transmission from node to node. Additionally, it conveys the "from," "to" nodes as well as "time," in seconds, needed to transmit the messages. Completion of the scenario occurs only after transmission of the last message in the timeline. Since these communications occur in series, the total communication time for a sequence of messages is just the sum of the individual times for each message plus any fixed delays that occur at each node. Only items utilizing one of the three commodities are used in our model (grey shaded items). Decision items incur fixed delays at a node and are unaffected by jamming. Tables 2, 3, and 4 provide a layout of the timelines for our three scenarios.

No.	Description	Commodity	From	To	Time (secs)
1	UAV_s1 sends pictures to SOF1	Imagery	UAV_s1	SOF1	180
2	SOF1 decides if possible target	Decision	SOF1	SOF1	60
3	SOF1 request UAV1 for possible target verification	Voice	SOF1	TOC	180
4	UAV1 moves into position	Decision	UAV1	UAV2	240
5	UAV2 sends pictures and starts to track	Imagery	UAV2	TOC	180
6	TOC determines target worth attacking	Decision	TOC	TOC	180
7	UAV2 automatically sends coordinates to TACAIR1 support	Data	UAV2	TACAIR1	6
8	TACAIR1 flies close enough to deliver weapon	Decision	TACAIR1	TACAIR2	300
9	Weapon flies to target	Decision	WEP	WEP	60
10	UAV2 takes pictures, sends to TOC, BDA	Imagery	UAV2	TOC	180
11	Determine target successfully attacked	Decision	TOC	TOC	240

Table 2. Scenario One timeline lists the sequence of events in this scenario. Information flows appear in grey, and decisions in white.

No.	Description	Commodity	From	To	Time (secs)
1	UAV_s1 sends pictures to SOF1	Imagery	UAV_s1	SOF1	180
2	SOF1 decides if possible target	Decision	SOF1	SOF1	60
3	SOF1 request UAV1 for possible target verification	Voice	SOF1	TOC	60
4	UAV1 moves into position	Decision	UAV1	UAV2	240
5	UAV2 sends pictures TOC	Imagery	UAV2	TOC	180
6	TOC determines target worth attacking	Decision	TOC	TOC	180
7	TOC informs SOF1 to begin to laze target	Voice	TOC	SOF1	60
8	SOF1 begins to laze target	Data	SOF1	TACAIR1	6
9	TACAIR1 flies close enough to deliver weapon	Decision	TACAIR1	TACAIR2	300
10	Weapon flies to target via laser guided munitions	Decision	WEP	WEP	60
11	UAV2 takes pictures, sends to TOC, BDA	Imagery	UAV2	TOC	180
12	Determine target successfully attacked	Decision	TOC	TOC	240

Table 3. Scenario Two timeline lists the sequence of events in this scenario. Information flows appear in grey, and decision in white.

No.	Description	Commodity	From	To	Time (secs)
1	UAV_s1 sends pictures to TOC and starts to track	Imagery	UAV_s1	SOF1	180
2	TOC determines target worth attacking	Decision	TOC	TOC	180
3	UAV_s2 automatically sends coordinates to TACAIR support	Data	UAV_s2	TACAIR1	6
4	TACAIR flies close enough to deliver weapon	Decision	TACAIR1	TACAIR2	300
5	Weapon flies to target	Decision	WEP	WEP	60
6	UAV_s3 takes pictures, sends to TOC, BDA	Imagery	UAV_s3	TOC	180
7	Determine target successfully attacked	Decision	TOC	TOC	240

Table 4. Scenario Three timeline lists the sequence of events in this scenario. Information flows appear in grey, and decisions in white.

B. MODEL OVERVIEW

We designed a bi-level (attacker-defender) model designed to map the communications of a strike network and its vulnerability to attacker using General Algebraic Modeling System (GAMS) as the tool for optimization.

Inputs to GAMS include the nodes, arcs, transmission messages (including starting and ending nodes), modes of communication (which are modeled as commodities), their specific arcs, and jamming locations. Output provides optimal placement of jamming equipment and cost for each message.

There is a growing body of research focusing on attacker-defender models for studying the resiliency of operational systems (see Brown, Carlyle, Salmeron, & Wood, 2006, for a comprehensive discussion on defending critical infrastructures). The above article focuses on applying bi-level and tri-level optimization models to make critical infrastructure more resilient to an attack. Additional literature has been written that applies the attacker-defender model framework to IP-based networks where linear programming models are used to identify maximum data flow for an IP network (Barkley, 2008), and to jamming wireless communications networks through the placement of jammers using mathematical programs to obtain the optimal operation and jamming of these networks (Shankar, 2008). This thesis however, allows for increasing

complexity in our communication networks. Refer to references [6] and [7] for more general discussion of designing networks that are resilient to failures (Barkley, 2008).

C. STRIKE NETWORK VULNERABILITY

Within a strike network, a finite number of messages are required in order to complete a kill chain. So in essence, we define a kill chain as a set of messages requiring transmission. The successful completion of a kill chain occurs upon receipt of the final message. On a lower level, we can define each message as shortest-path problem with the message using the shortest path from source to destination node. Therefore, the kill chain is a list of successive messages or shortest-path problems. Figure 2 gives visual representation individual messages within a kill chain.

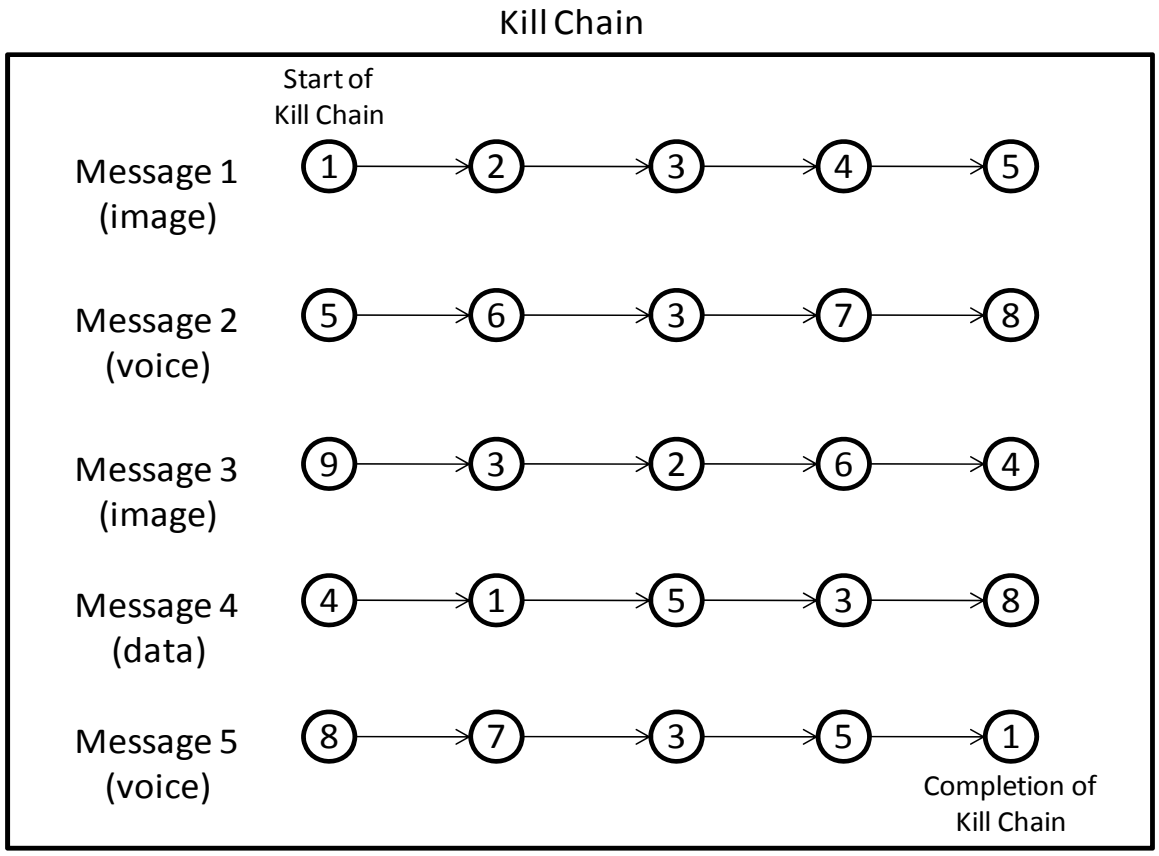

Figure 5. Hypothetical representation of successive messages depicted in a kill chain

Jamming has the opportunity to affect multiple shortest paths depending upon the node it affects. For example, a kill chain could be composed of five shortest-paths as

illustrated in Figure 5. Each shortest-path uses five nodes to complete its path. Jamming would be capable of affecting all five paths if they all possessed at least one identical node. Figure 6 gives a visual representation of this effect on a kill chain.

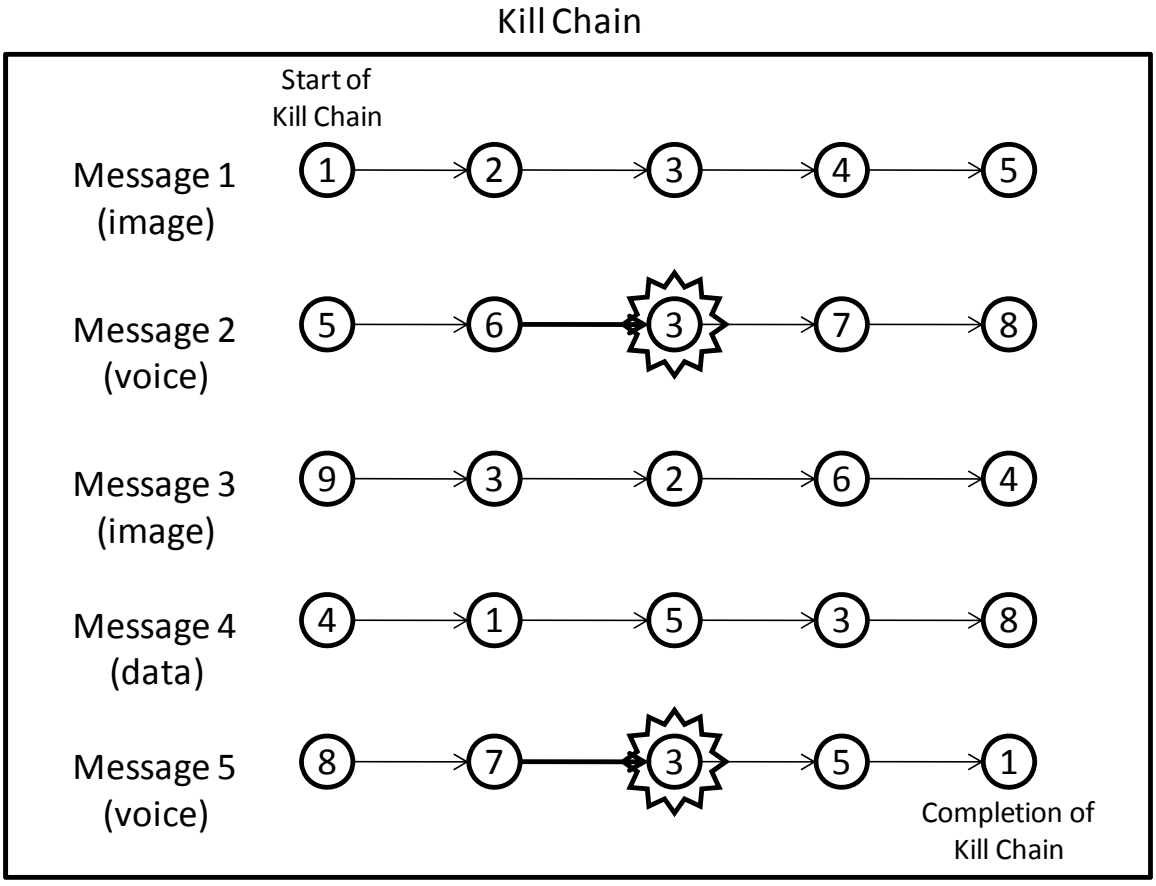

Figure 6. Hypothetical representation of a jammers' effect on one node in multiple messages. Here, node 3 voice transmissions are jammed. Starred nodes incur delays, which correspond to increased transmission time on the highlighted arcs.

This model assists in identifying those nodes and allows us the opportunity to strengthen the network.

1. Model Assumptions

The key assumptions made in this formulation are:

- Jammers have an effective radius range of five miles.
- Jammers affect specific commodities and are placed at one of four locations.

- Only incoming transmissions are affected, outgoing transmissions unimpeded.

2. Set [~cardinality]

$n \in N$ nodes in communication network (alias *i*, *j*) [~10]

$(i, j) \in A$ arcs (links) in communication network [~25]

$k \in K$ distinct messages required to create and execute a complete strike plan [~10]

$m \in M$ mode of transmission (e.g., data, voice, video) [~3]

$(i, j) \in A_m \subseteq A$ arcs capable of carrying mode *m* traffic

$m(k)$ mode of transmission required for message *k*

$s^k \in N$ source node for message *k*

$t^k \in N$ destination node for message *k*

$r \in R$ jamming locations

3. Data [units]

c_{ij}^m cost (e.g., transmit time) for message of mode m on link $(i, j) \in A$ [sec]

q_{jr}^m delay incurred at (receiving) node *j* if jammer used at location *r* for messages of mode m [sec]

$\overline{jammers}$ maximum number of jammers adversary can place [cardinality]

4. Variables [units]

$XMIT_{ij}^k$ message *k* uses link $(i, j) \in A_{m(k)}$ [binary]

JAM_r adversary places a jammer at location *r* [binary]

5. Formulation [Dual Variables for Inner Minimization]

$$\max_{JAM} \min_{XMIT} \sum_{k \in K} \sum_{(i,j) \in A_{m(k)}} \left(c_{ij}^{m} + \sum_{r \in R} q_{jr}^{m} JAM_r \right) XMIT_{ij}^{k} \qquad (A0)$$

$$\text{s.t.} \quad \sum_{j:(i,j) \in A_{m(k)}} XMIT_{ij}^{k} - \sum_{j:(j,i) \in A_{m(k)}} XMIT_{ji}^{k} = \begin{cases} 1 & i = s^k \\ -1 & i = t^k \\ 0 & \text{o.w.} \end{cases} \qquad \forall i \in N, k \in K \ [-\alpha_i^k] \quad (A1)$$

$$XMIT_{ij}^{k} \geq 0 \qquad \forall (i,j) \in A_{m(k)}, k \in K \quad (A2)$$

$$\sum_{r \in R} JAM_r \leq \overline{jammers} \qquad (A3)$$

$$JAM_r \in \{0,1\} \qquad \forall r \in R \qquad (A4)$$

6. Discussion

The objective function (A0) calculates the total transmission time (including delays introduced by any jamming) for the messages over each of their communications paths indicated by the *XMIT* variables. Constraints (A1) ensure that each required message follows a path from source to sink. Constraints (A2) define the domain of the transmit variables. Constraints (A3) limit the number of jammers emplaced by the adversary, and constraints (A4) define the domain of the jamming variables. If a set of jammer locations is known, and fixed, the resulting problem is a minimum-cost network flow problem. When all the JAM_r variables are fixed at $JAM_r = 0$, we have the standard operator's model in the absence of any enemy jamming capability.

7. Dual-ILP Reformulation

$$\max_{JAM, \alpha} \quad \sum_{k \in K} \alpha_{t^k}^{k} \qquad (D0)$$

$$\text{s.t.} \quad \alpha_j^k - \alpha_i^k - \sum_r q_{jr}^{m} JAM_r \leq c_{ij}^{k} \qquad \forall k \in K, (i,j) \in A_{m(k)} \quad (D1)$$

$$\alpha_{s^k}^{k} \equiv 0 \qquad \forall k \in K \qquad (D2)$$

$$\sum_{r \in R} JAM_r \leq \overline{jammers} \qquad (A3)$$

$$JAM_r \in \{0,1\} \qquad \forall r \in R \qquad (A4)$$

8. Discussion

The objective (D0) calculates the sum of the individual message shortest-path lengths. Constraints (D1) relate the presence of a jammer to the resulting arc length bound on node distance labels. Constraints (D2) set the dual variable at the origin of each individual message to zero, this is not necessary, but removes an unneeded degree of freedom in the dual variables for each message. Constraints (A2) again limit the number of jammers emplaced, and constraints (A4) define the domain of the binary variables.

III. EXPERIMENT RESULTS

A. RESULTS

We run four groups of three scenarios all in GAMS. Our output provides us with several key pieces of information. The operator model determines the optimal communications flow by providing the optimal *XMIT* variables. The attacker-defender model determines the optimal JAM_r variables and then determines the resulting optimal flows by solving the minimum cost flow model with the JAM_r variable fixed at their optimal values, yielding optimal *XMIT* variables. Table 5 provides JAM_r variable data, Table 6 a list of the communication flow paths for each message *k1* through, and Figure 7 gives a graphical representation of the GAMS output. They are the result of our baseline Scenario Two with two jammers.

Jammer Location	**Jammers Placed at Location (1.0 = yes, 0.0 = no)**
r1	1.0
r2	0.0
r3	0.0
r4	1.0

Table 5. This table provides the JAM_r variable results from Scenario Two with two jammers. The table lists possible jammer locations and indicates whether a jammer is placed by a 1.0 (jammer is placed in this location) or a 0.0 (jammer is not placed in this location).

Message	Path
k1	UAV_s1 → SOF1
k2	SOF1 → SAT → TOC
k3	UAV2 → SAT → TOC
k4	TOC → SAT → SOF1
k5	SOF1 → SAT → TACAIR1
k6	UAV2 → SAT → TOC

Table 6. Provides list of the communication flow paths for each message *k1* through *k6*.

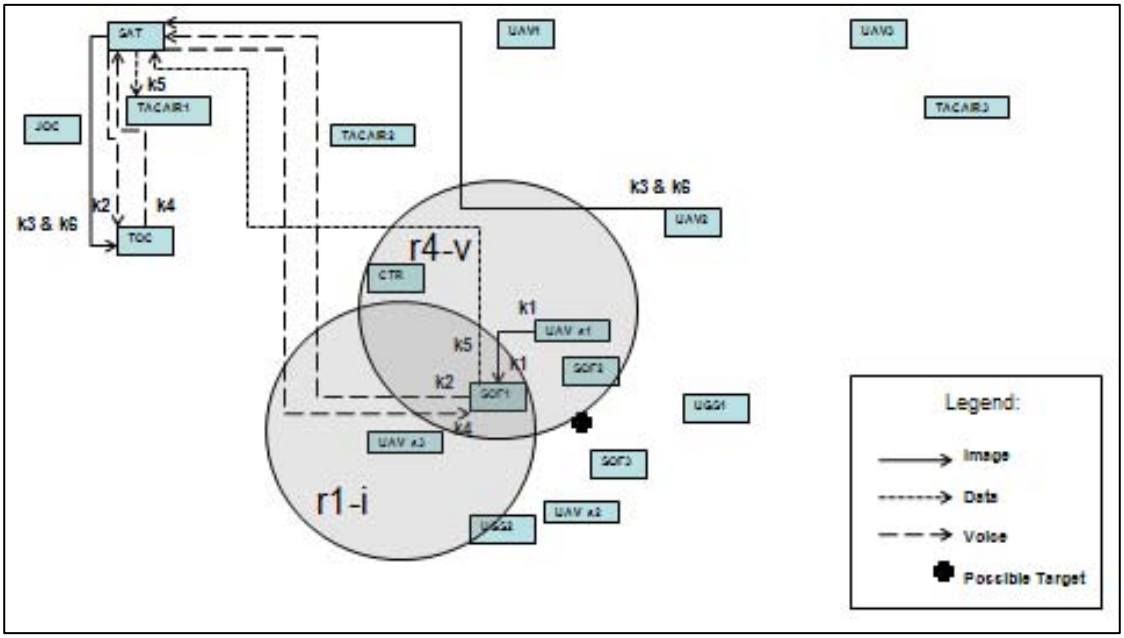

Figure 7. A graphical representation of the GAMS output provided in Table 6. Labels for messages *k1* through *k6* are placed at the source and destination nodes of each. Different line styles symbolize separate modes of communication. The solid line represents image, the small dotted line represents data, and the elongated dotted line represents voice communications. The same legend above is applied to all future diagrams in this thesis.

We run each scenario five times, varying the number of jammers from zero to four. We summarize all pertinent information in a table format. Notice in the summary tables that as we increase the number of jammers available for use, not all locations are utilized for a scenario. In those cases, an additional jammer would not increase the total cost and, therefore, no extra jammer is used, as illustrated in Table 7.

Jammers	Cost (seconds)	Locations
0	1152	-
1	1632	r1
2	1812	r1, r4
3	1812	r1, r4
4	1812	r1, r4

Table 7. This table provides a summary of the output data from Scenario Two. The first column lists the iteration of jammers from zero to four. The second column lists the iteration of cost data for each jammer scenario. All values are provided in seconds. The third column lists optimal placement of jammers. Only one jammer is placed at each location for all of our scenario runs.

B. VARYING THE NUMBER OF JAMMERS

Initially, we concentrate on maximizing the networks cost from the enemy's perspective. The enemy's goal is to maximize the minimum cost path (i.e., delay, the flow of communications through the kill chain process using jammers). In our scenario, the enemy has the option of placing jammers in four different locations (*r1*, *r2*, *r3*, and *r4*). Using our model, we can identify the optimal placement of these jammers. We apply the following restrictions: voice transmissions are affected when a jammer is placed at location *r4*, image transmissions are affected at locations *r1* and *r2*, and data transmissions are affected at location *r3*. We assume that the maximum number of jammers allowed is four.

1. Scenario One

Figures 8, 9, and 10 illustrate the kill chain for Scenario One. Our solution determines the optimal JAM_r variables and then determines the resulting optimal flows by solving the minimum cost flow model with the JAM_r variable fixed at their optimal values, yielding optimal *XMIT* variables. Figure 8 is an initial look at the C4ISR network

with no jammers. Figure 9 illustrates the solution to the scenario with one jammer. Per our model, the optimal placement of this jammer is location *r1*. Placing the jammer at this location jams the image flow from UAV_s1 to SOF1. No other flows are delayed. Figure 10 illustrates the solution for the scenario with two jammers. This run demonstrates the model's ability to change flow in order to maintain the shortest path from source to destination node. In Figure 9, voice transmission flowed from SOF1 to CTR to TOC. In Figure 10, the model altered the path to flow from SOF1 to SAT to TOC. Additional jammers do not have any added affect on this scenario because those locations do not contain nodes that have any inbound flows.

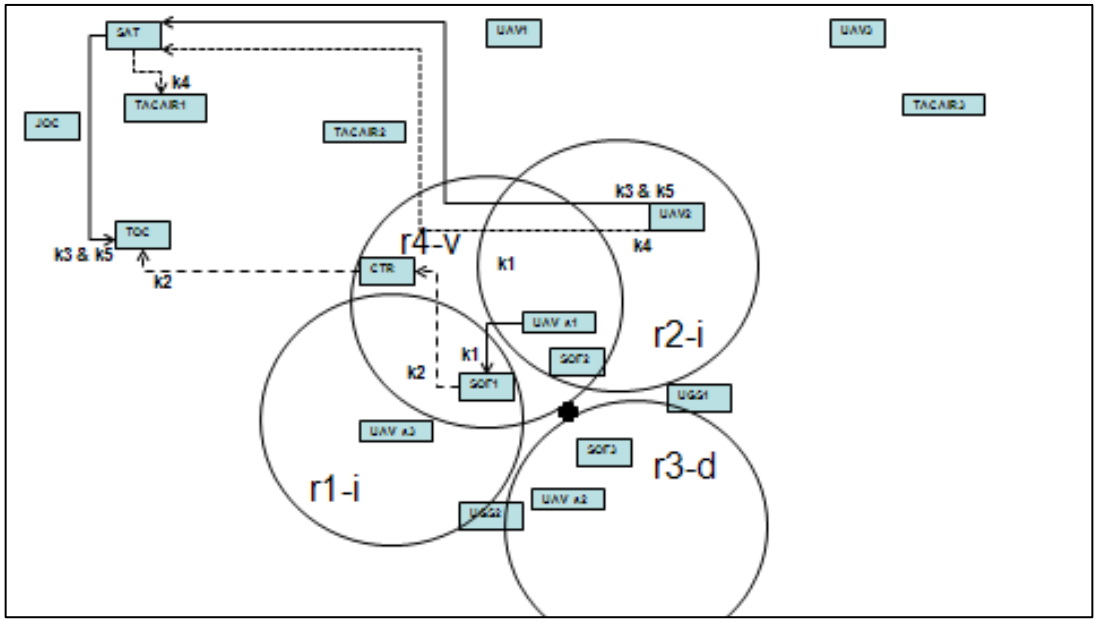

Figure 8. Diagram of Scenario One with appropriate arcs. Disks indicate area of effect for jamming locations *r1* through *r4*. Each location has an appropriate flow (*i* - image, *v* - voice, or *d* – data) it is capable of jamming. No jammers are placed; therefore, no flows are jammed.

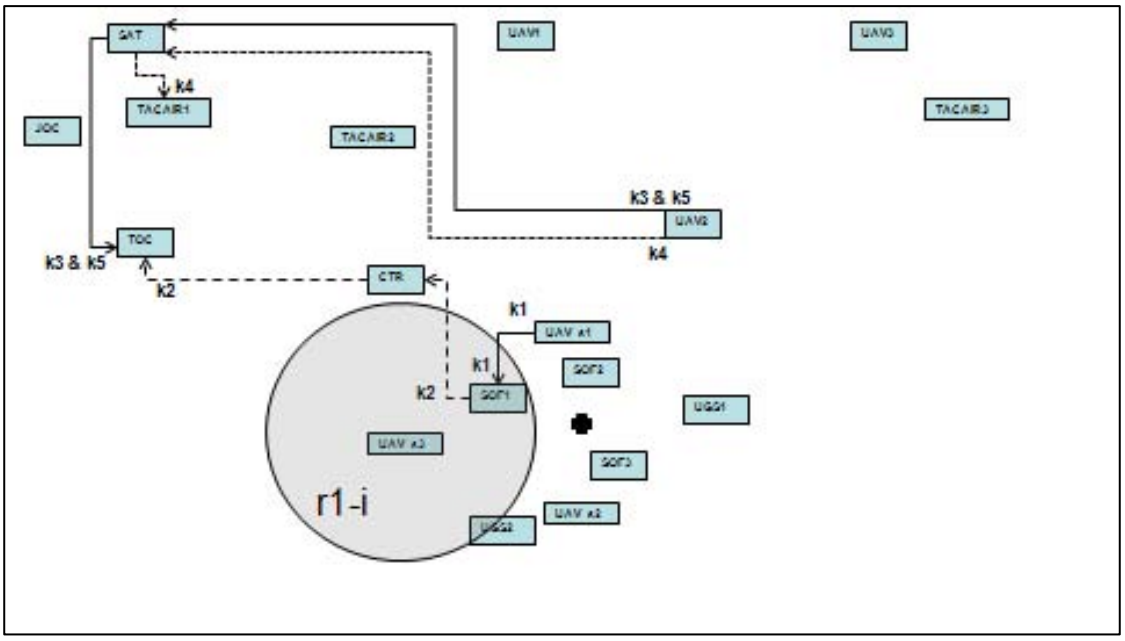

Figure 9. Diagram of Scenario One with appropriate arcs. A jammer is placed at location *r1* affecting image flow.

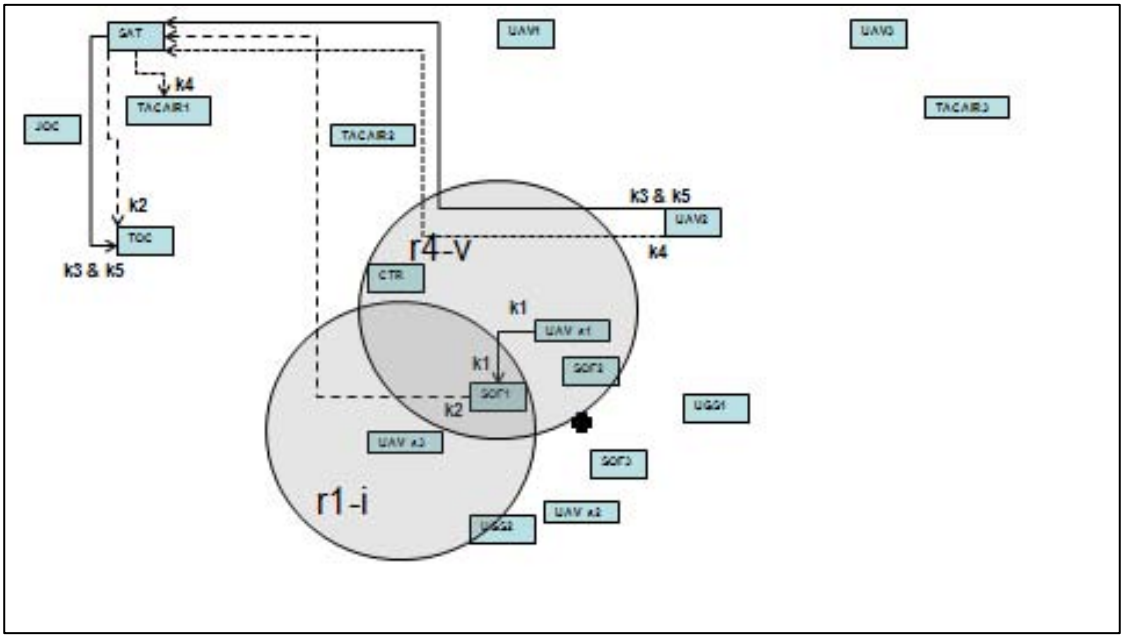

Figure 10. Diagram of Scenario One with appropriate arcs. Jammers are placed at locations *r1* and *r4*, affecting image and voice flow, respectively. Although, another jammer is placed in location *r4*, it does not impact this scenario since flow is rerouted to avoid any delays.

Jammers	Cost (seconds)	Locations
0	1032	-
1	1512	r1, r4
2	1512	r1, r4
3	1512	r1, r4
4	1512	r1, r4

Table 8. Summary of Scenario One's output. Additional jammers do not have any effect on this network because those locations do not contain nodes that have any inbound flows. Our image commodity is the only inbound communications flow within range of any jammer location (*r4*), but it only affects voice communications.

2. Scenario Two

Figures 11, 12, and 13 illustrate the kill chain for Scenario Two. Figure 11 is an initial look at the C4ISR network with no jammers. Figure 12 illustrates the solution for the scenario with one jammer placed at *r1*, jamming image flow. No other flows are delayed. Figure 13 illustrates the solution for the scenario with two jammers. Again, this run demonstrates the models' ability to change flow in order to maintain the shortest path from source to destination node. Additional jammers do not have any added effect on this scenario because those locations do not contain nodes that have any inbound flows.

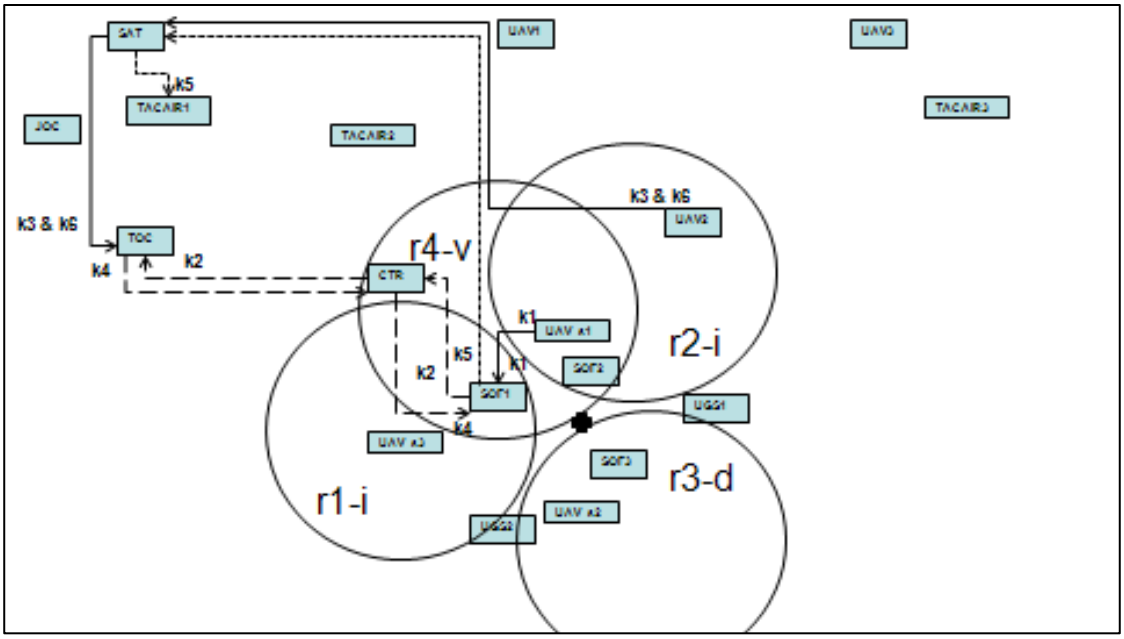

Figure 11. Diagram of Scenario Two with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

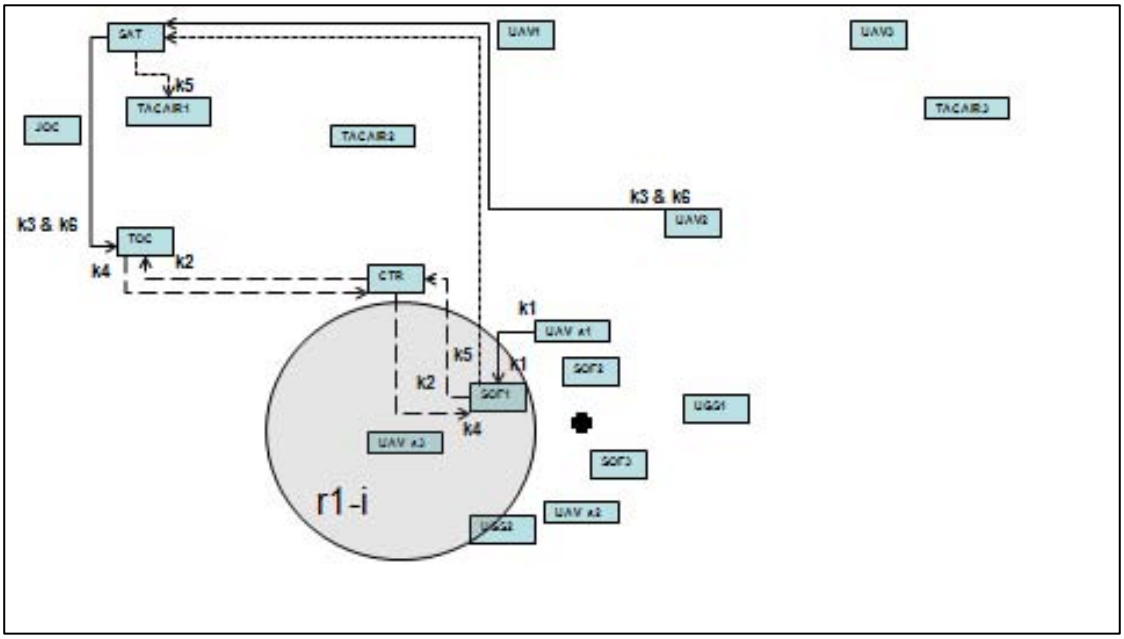

Figure 12. Diagram of Scenario Two with appropriate arcs. A jammer is placed at location *r1*, affecting image flow.

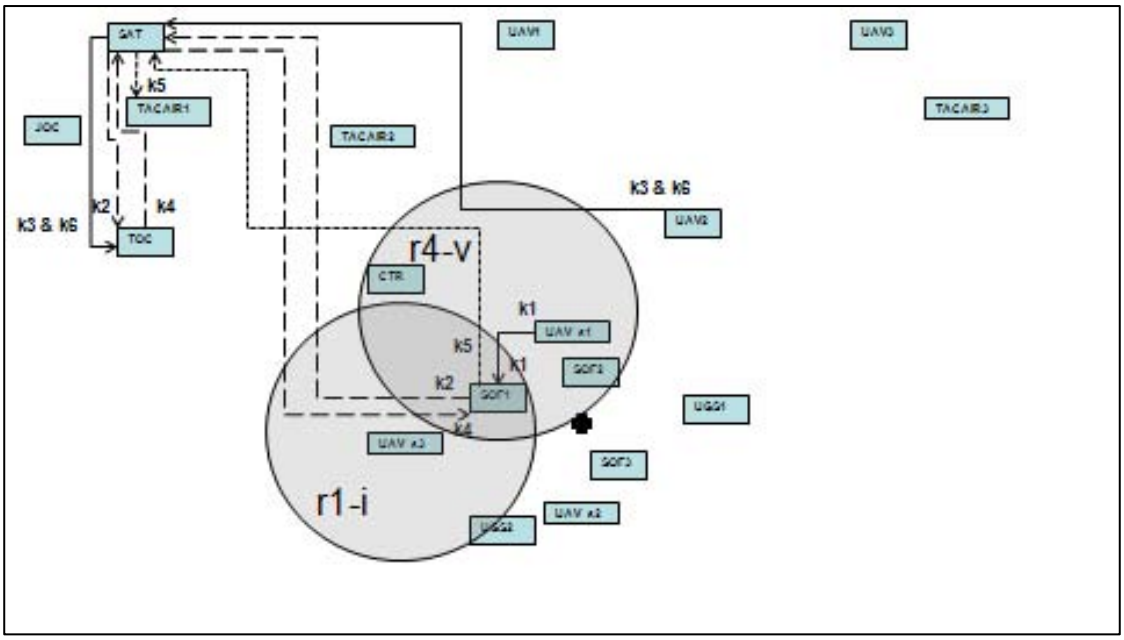

Figure 13. Diagram of Scenario Two with appropriate arcs. Jammers are placed at locations *r1* and *r4*, affecting image and voice flow, respectively.

Jammers	Cost (seconds)	Locations
0	1152	-
1	1632	r1
2	1812	r1, r4
3	1812	r1, r4
4	1812	r1, r4

Table 9. Summary of Scenario Two's output. Additional jammers do not have any effect on this network because those locations do not contain nodes that have any inbound flows.

3. Scenario Three

Figures 14 and 15 illustrate the kill chain for Scenario Three. Figure 14 is an initial look at the C4ISR network with no jammers. Figure 15 illustrates the solution for the scenario with one jammer placed at *r1*, jamming image flow. No other flows are delayed. This scenario has the greatest vulnerability since all communications flow through SOF1. Additional jammers do not have any added effect on this scenario because those locations do not contain nodes that have any inbound flows.

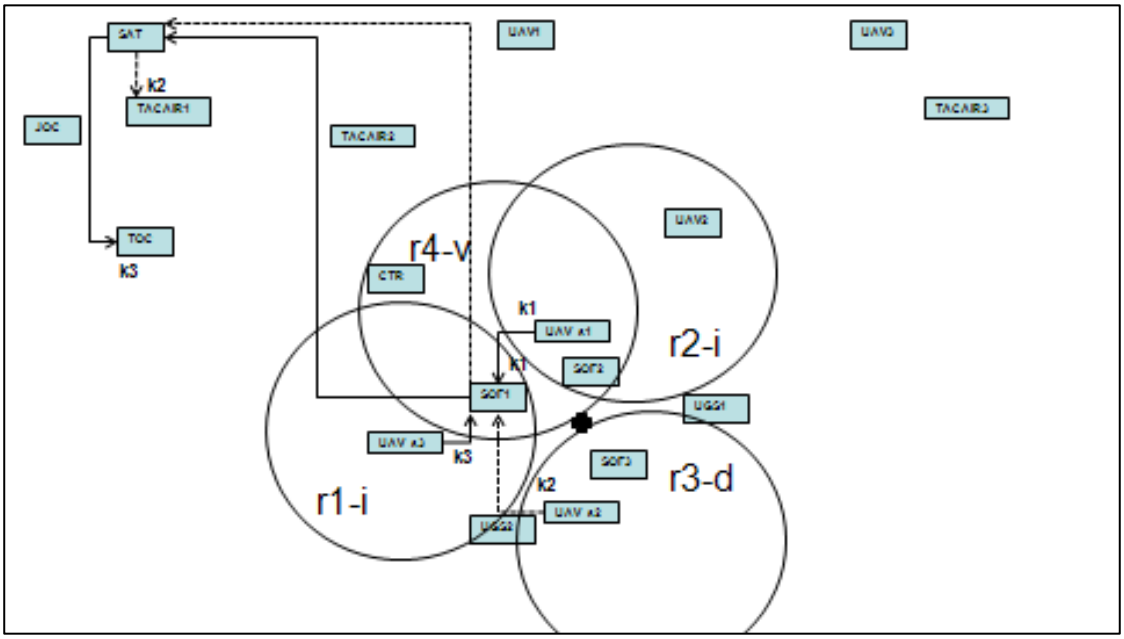

Figure 14. Diagram of Scenario Three with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

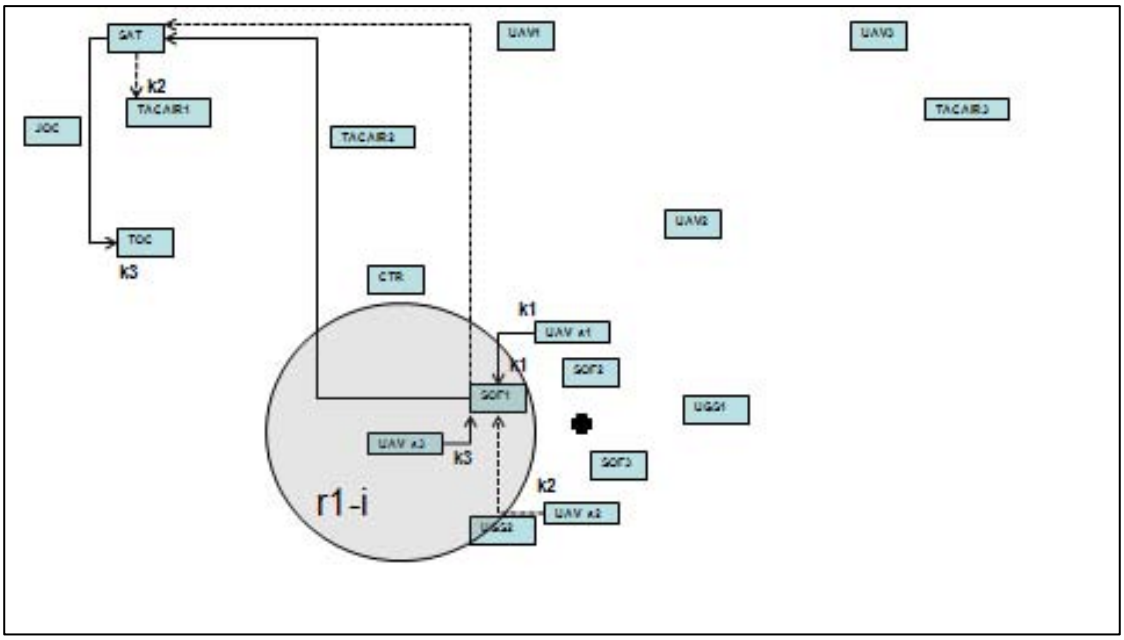

Figure 15. Diagram of Scenario Three with appropriate arcs. A jammer is placed at location *r1,* affecting image flow.

Jammers	Cost (seconds)	Locations
0	762	-
1	1722	r1
2	1722	r1
3	1722	r1
4	1722	r1

Table 10. Summary of Scenario Three's output. Additional jammers do not have any effect on this network because those locations do not contain nodes that have any inbound flows.

C. IMPLEMENTATION OF ELECTRONIC COUNTERMEASURES

Next, we discuss implementing procedures to nullify a jammer location. For our previous runs, we conclude that location *r1* has the most influence on our network, since in all three scenarios; *r1* was the location of choice when placing a single jammer. Neutralization is accomplished by destruction of jammer or by active or passive electronic countermeasures. Passive electronic countermeasures seek to enhance or change the nature of the energy reflected back to enemy radars, but they do not generate their own energy; while active electronic countermeasure equipment generates energy

either in the form of noise to confuse an enemy's electromagnetic sensors, or by radiating false or time-delayed signals to deceive radio or radar equipment and their operators (Miller & DeLia, 2010).

1. Scenario One

Figures 16 and 17 illustrate the kill chain for Scenario One. Figure 16 is an initial look at the C4ISR network with no jammers. Figure 17 illustrates the solution for the scenario with one jammer placed at *r4*, jamming voice flow. The flow is delayed since the model changed flow in order to maintain the shortest path from source to destination node for message 2. Additional jammers do not have any added effect on this scenario because those locations do not contain nodes that have any inbound flows.

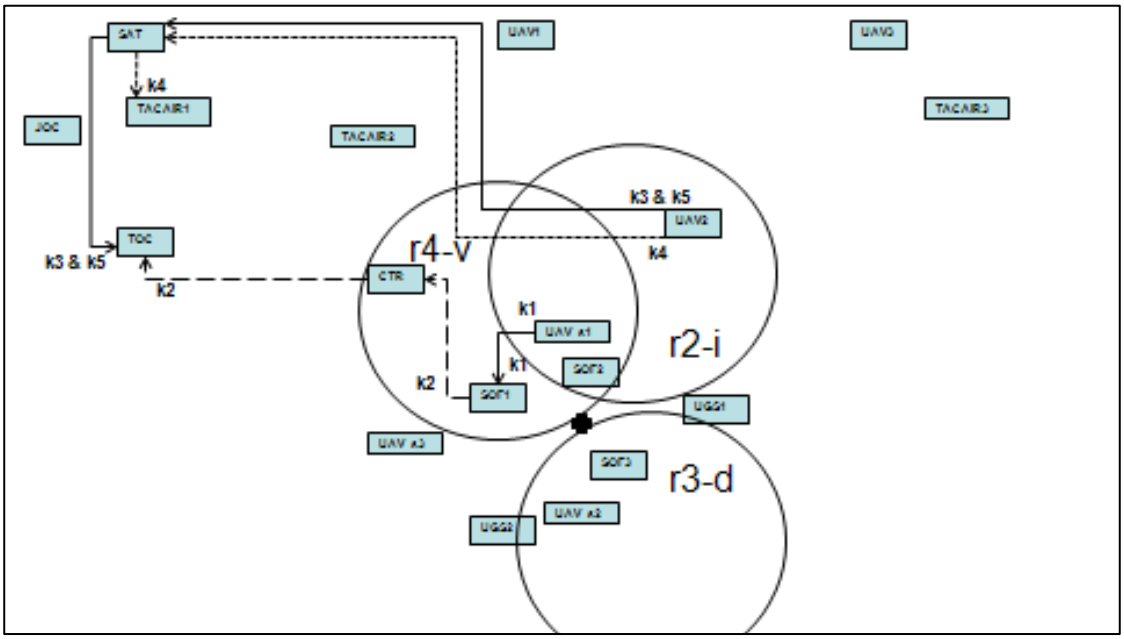

Figure 16. Diagram of Scenario One with appropriate arcs. Jammer location *r1* is removed to represent our ability to employ electronic countermeasures to negate any jamming capability. No jammers are placed; therefore, no flows are jammed.

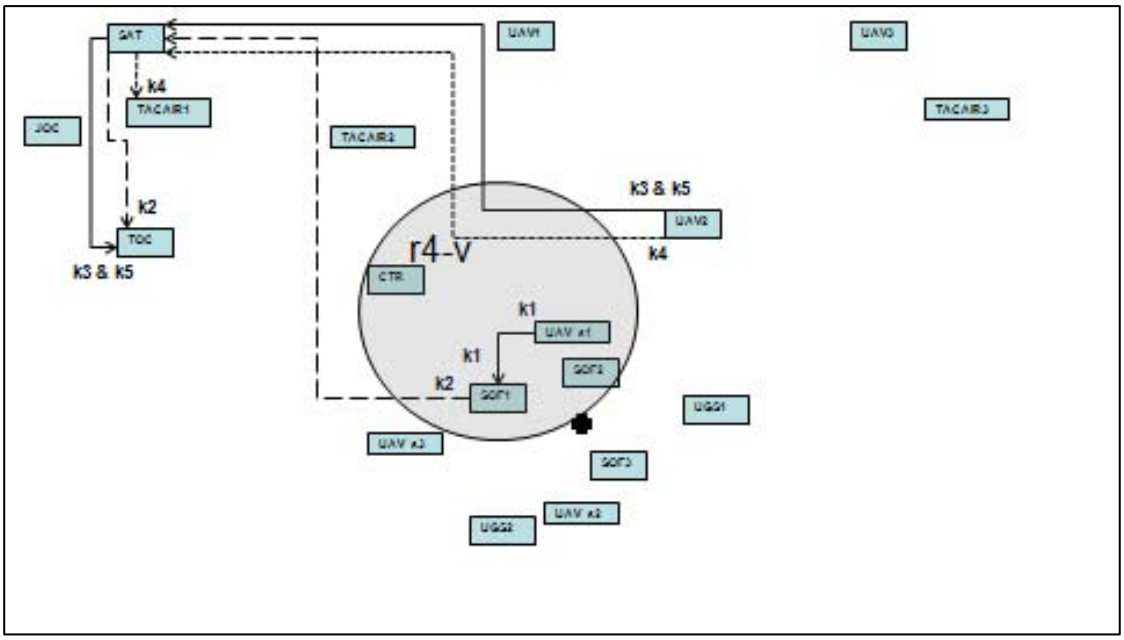

Figure 17. Diagram of Scenario One with appropriate arcs. Jammer is placed at location *r4*, affecting voice flow.

The resulting cost of this network is 1,032 seconds. Placing jammers of given types at any of a given set of locations has no effect on this scenario because those locations do not contain nodes that have any inbound flows. Our image commodity is the only inbound communications flow within range of any jammer location (*r4*) but it only affects voice communications.

2. Scenario Two

Figures 18 and 19 illustrate the kill chain for Scenario Two. Figure 18 is an initial look at the C4ISR network with no jammers. Figure 19 illustrates the solution for the scenario with one jammer placed at *r4*, jamming voice flow. No other flows are delayed. Two additional voice flows avoid jamming since the model changed flow in order to maintain the shortest path from source to destination node for message 2 and 4. Additional jammers do not have any added effect on this scenario because those locations do not contain nodes that have any inbound flows.

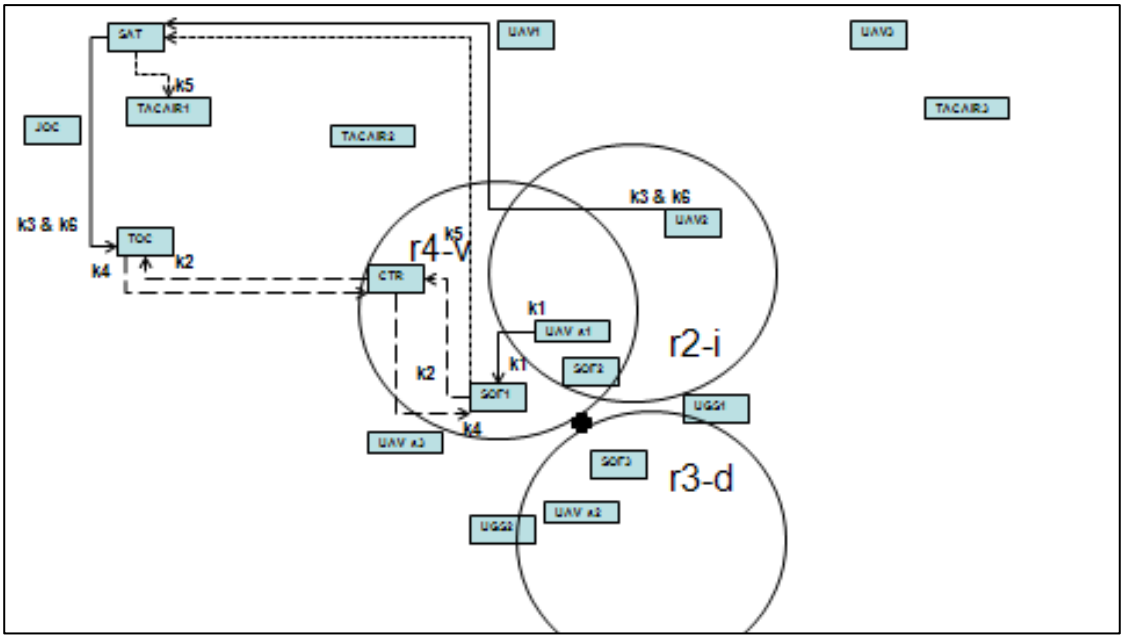

Figure 18. Diagram of Scenario Two with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

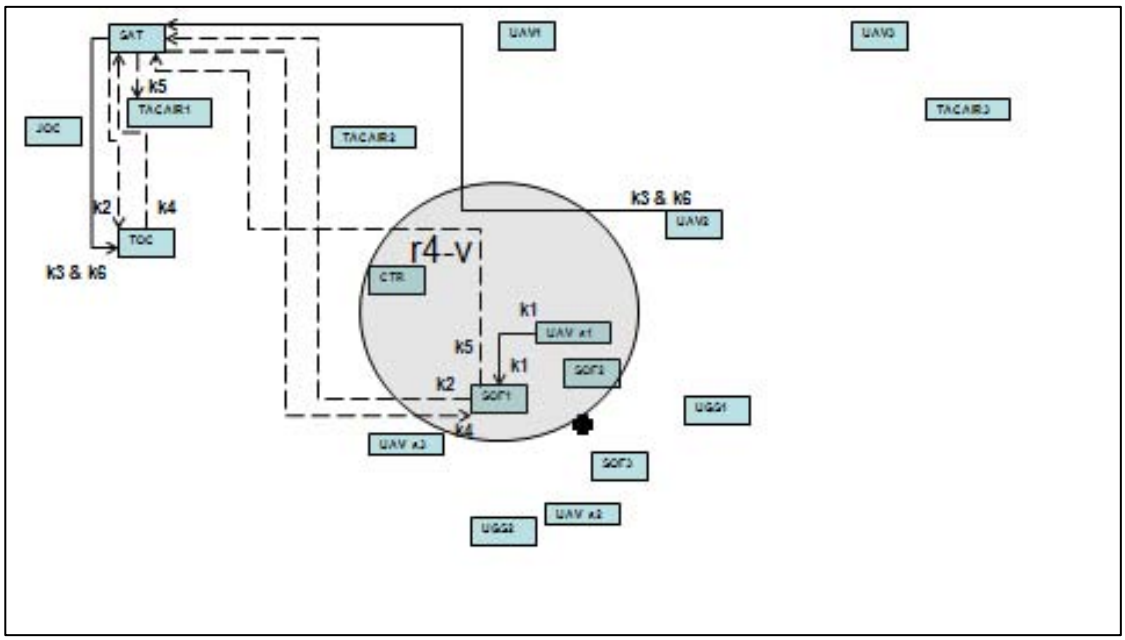

Figure 19. Diagram of Scenario Two with appropriate arcs. A jammer is placed at location *r4*, affecting voice flow.

Jammers	Cost (seconds)	Locations
0	1152	-
1	1332	r4
2	1332	r4
3	1332	r4
4	1332	r4

Table 11. Summary of Scenario Two's output. Additional jammers do not have any effect on this network because those locations do not contain nodes that have any inbound flows.

3. Scenario Three

Figure 20 illustrates the kill chain for Scenario Three. It is an initial look at the C4ISR network with no jammers. The additions of jammers do not have any effect on this scenario because those locations do not contain nodes that have any inbound flows. Our image and data commodities are the only inbound communications flow within range of any jammer location (*r4*) but it only affects voice communications.

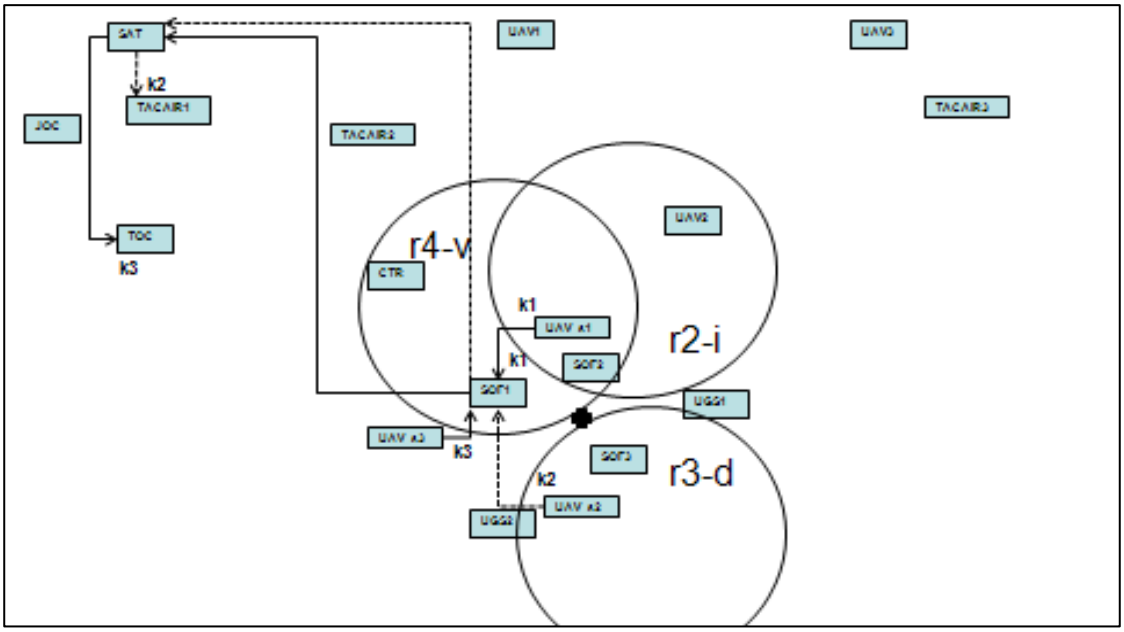

Figure 20. Diagram of Scenario Three with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

The resulting cost of this network is 762 seconds. Placing jammers of given types at any of a given set of locations has no effect on this scenario because those locations do

not contain nodes that have any inbound flows. Our image and data commodities are the only inbound communications flow within range of any jammer location (*r4*) but it only affects voice communications.

D. CHANGING NODE LOCATIONS AND CONFIGURATION

Next, we will take a look at changing the locations and configurations of our nodes to lessen the effect of jammers. The goal of changing locations is to limit a jammers ability to affect multiple nodes or affect the same node with multiple jammers. Figure 21 provides an updated map of new node locations and configurations. The following changes have been made to this network; CTR and UAV2 have been moved out of jamming range; all assets have been moved out of jammer location *r4* so it no longer has any affect on our scenarios; and SOF1 and SOF3 switched positions.

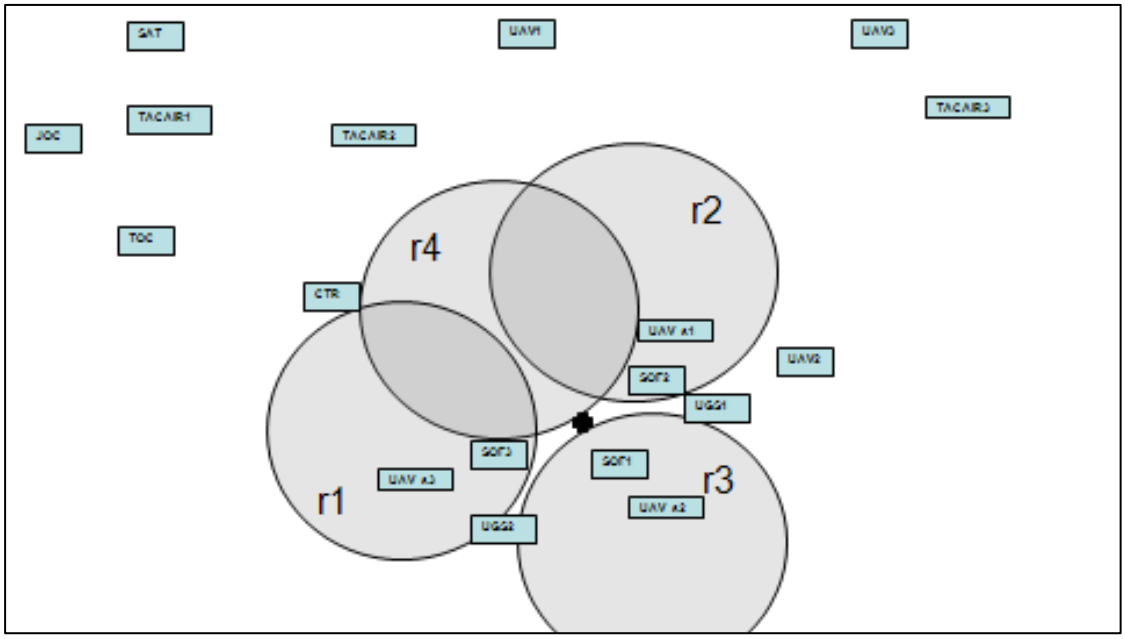

Figure 21. Diagram of updated nodes within the communications network. Disks indicate jamming locations as well as area of effect. The cross indicates possible target.

By making the above changes to our baseline scenario, jammers have very little effect on our network. The following diagrams give us a look at these scenarios.

1. Scenario One

Figure 22 illustrates the kill chain for Scenario One. It is an initial look at the C4ISR network with no jammers. By swapping SOF1 and SOF3 nodes, this scenario is no longer affected by jammers because those locations do not contain nodes that have any inbound flows. Our image commodity is the only inbound communications flow within range of any jammer location (*r3*) but it only affects data communications.

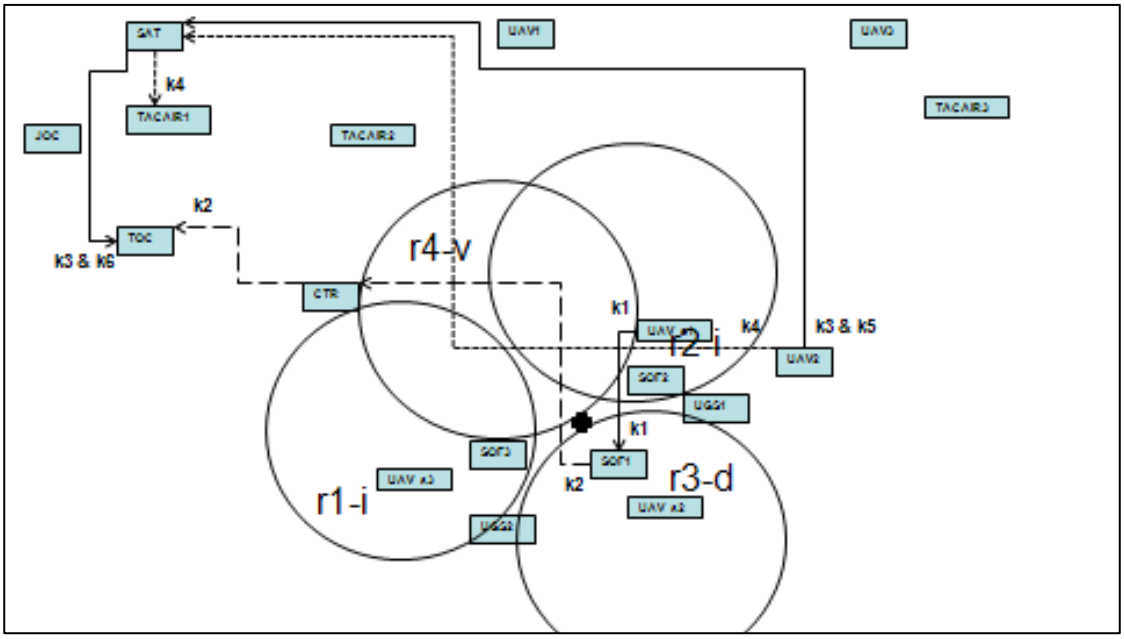

Figure 22. Diagram of Scenario One with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

The resulting cost of this network is 1,032 seconds. Placing jammers of given types at any of a given set of locations has no affect on this scenario because those locations do not contain nodes that have any inbound flows. Our image commodity is the only inbound communications flow within range of any jammer location (*r3*) but it only affects data communications.

2. Scenario Two

Figure 23 illustrates the kill chain for Scenario Two. It is an initial look at the C4ISR network with no jammers. As with Scenario One, by swapping SOF1 and SOF3 nodes, this scenario is no longer affected by jammers, because those locations do not

contain nodes that have any inbound flows. Our image and voice commodities are the only inbound communications flow within range of any jammer location (*r3*) but it only affects data communications.

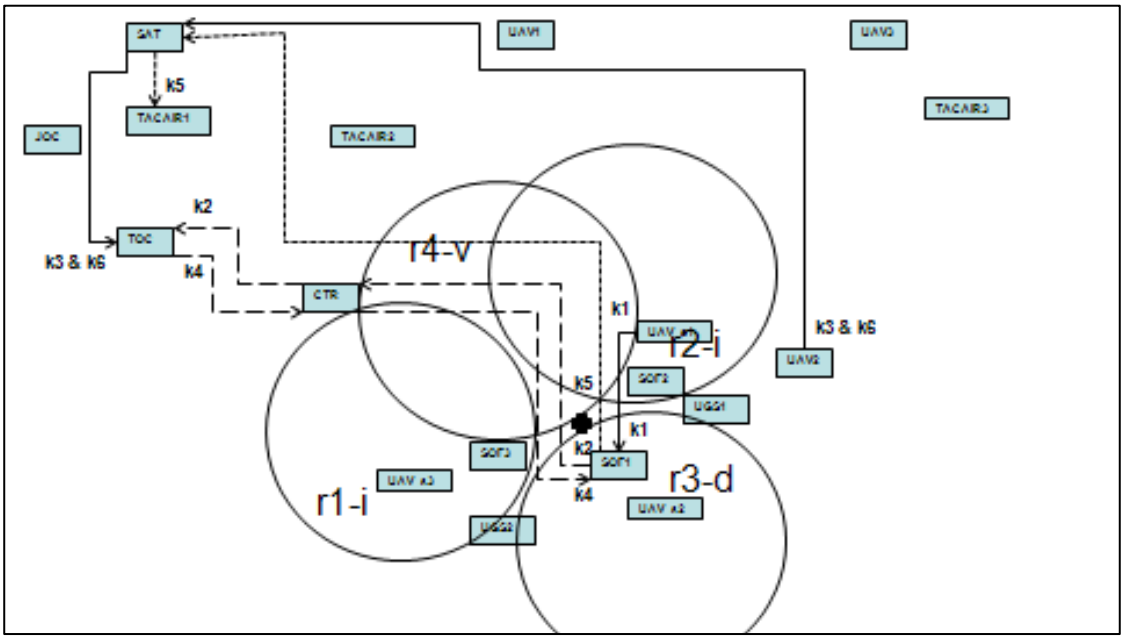

Figure 23. Diagram of Scenario Two with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

The resulting cost of this network is 1,152 seconds. Placing jammers of given types at any of a given set of locations has no affect on this scenario because those locations do not contain nodes that have any inbound flows. Our image and voice commodities are the only inbound communications flow within range of any jammer location (*r3*) but it only affects data communications.

3. Scenario Three

Figures 24 and 25 illustrate the kill chain for Scenario Three. Figure 24 is an initial look at the C4ISR network with no jammers. Figure 25 illustrates the solution for the scenario with one jammer placed at *r3*, jamming data flow. No other flows are delayed because those locations do not contain nodes that have any inbound flows.

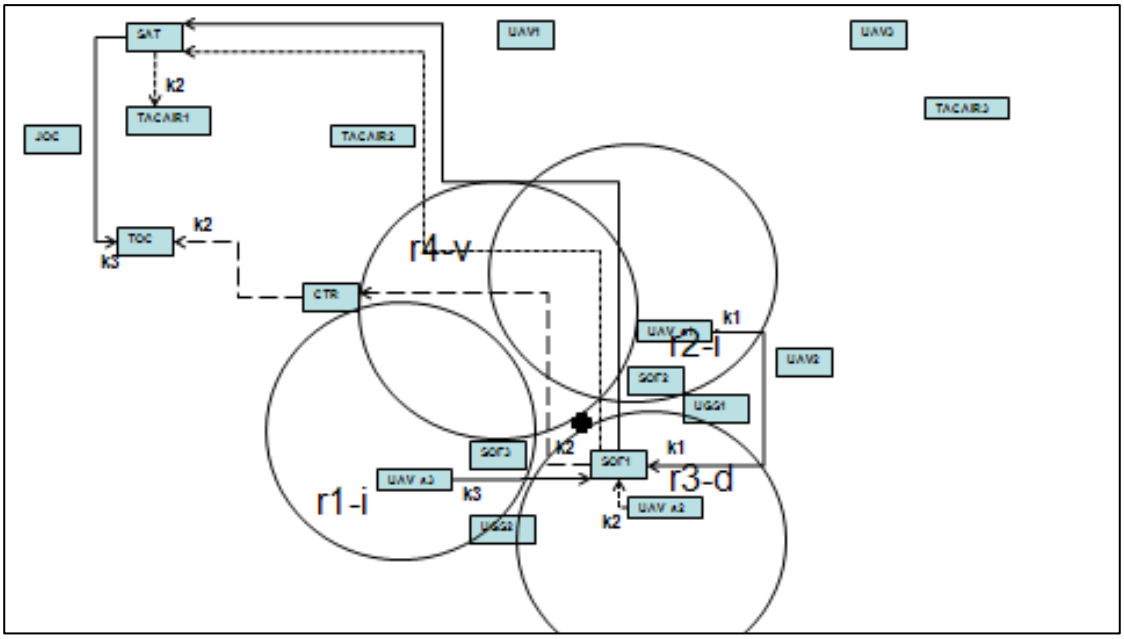

Figure 24. Diagram of Scenario Three with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

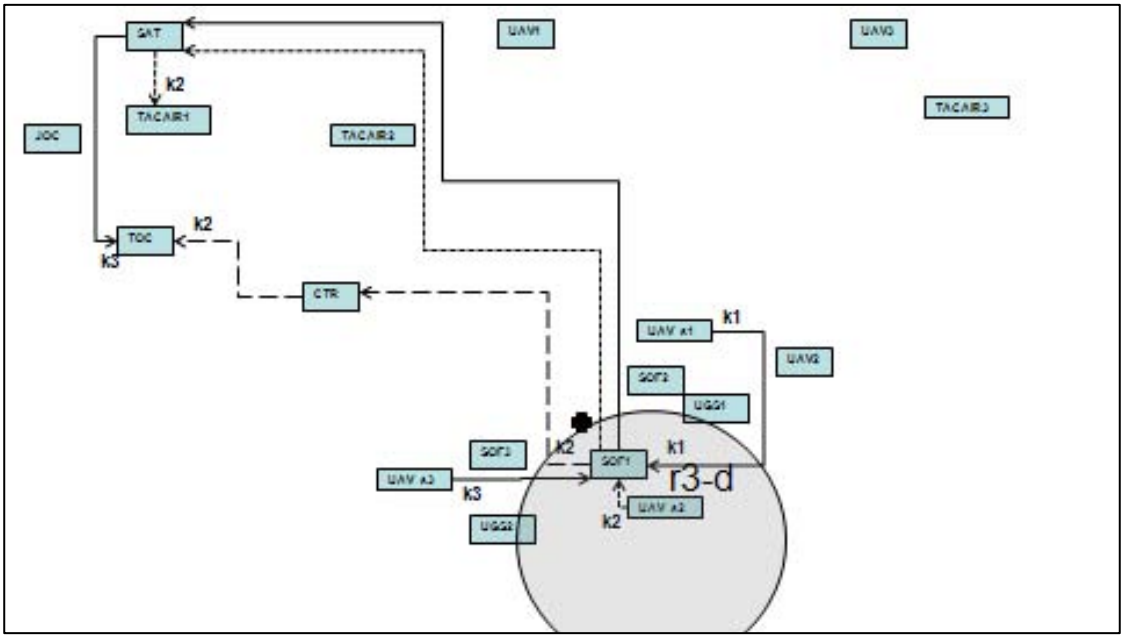

Figure 25. Diagram of Scenario Three with appropriate arcs. A jammer is placed at location *r3*, affecting data flow.

Jammers	Cost	Locations
0	762	-
1	822	r3
2	822	r3
3	822	r3
4	822	r3

Table 12. Summary of Scenario Three's output. Additional jammers do not have any effect on this network because those locations do not contain nodes that have any inbound flows.

E. STRENGTHENING IMAGE AND DATA SUB-NETWORKS

Finally, we examine the impact of strengthening the network by adding arcs. Of the three commodities, image is the most vulnerable since its network is the most sparse, e.g., not as many arcs in the network as compared to the other commodities. Additionally, a delay on the image sub-network (480 secs) costs approximately two and a half times more than a delay on the voice sub-network (180 secs) and eight times more than a delay on the data sub-network (60 secs).

To strengthen the image sub-network, we establish additional arcs between unmanned aerial vehicle – small and the other two SOF nodes (SOF2 and SOF3). These additions add six arcs to the image sub-network. Additionally, we use those arcs to strengthen data sub-network. Figures 26 and 27 define the new arcs.

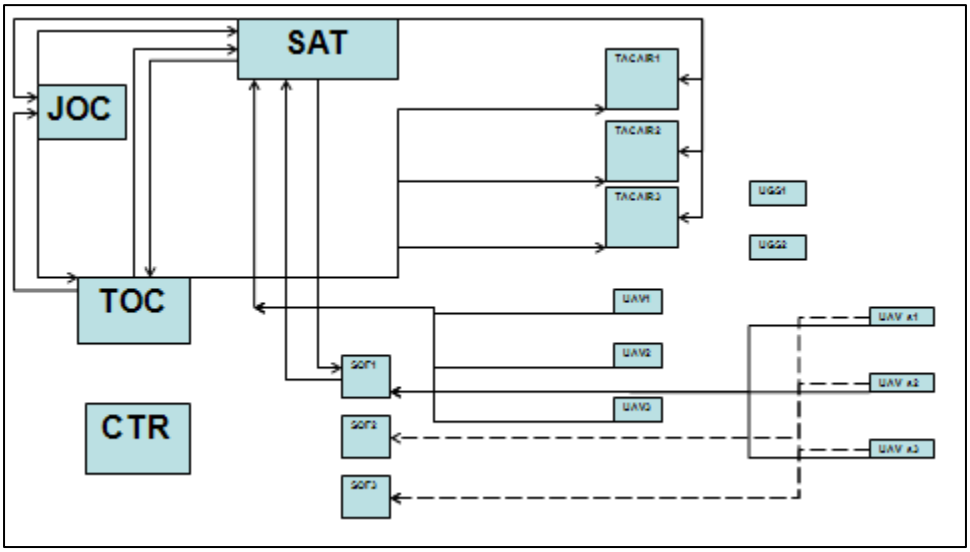

Figure 26. Graphical representation of new image sub-network. Dotted lines designate new arcs. Network is not geographically accurate.

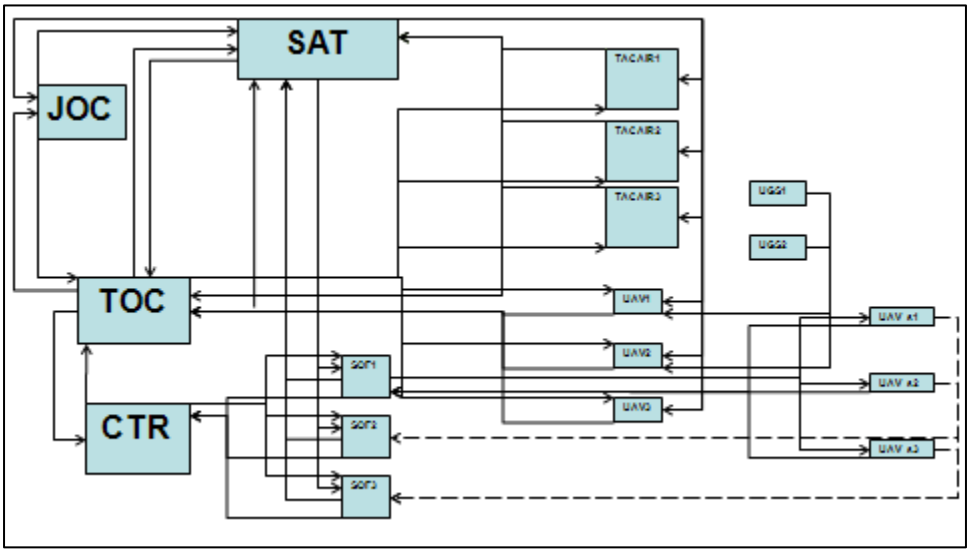

Figure 27. Graphical representation of new data sub-network. Dotted lines designate new arcs. Network is not geographically accurate.

1. Scenario One

Figures 28, 29, and 30 illustrate the kill chain for Scenario One. Figure 28 is an initial look at the C4ISR network with no jammers. Figure 29 illustrates the solution for the scenario with one jammer placed at *r1*, jamming image flow. Figure 30 illustrates the solution for the scenario with two jammers placed at location *r1* and *r4*. Again, this run

demonstrates the models' ability to change flow in order to maintain the shortest path from source to destination node. Additional jammers do not have any added effect on this scenario because those locations do not contain nodes that have any inbound flows. The scenario remains unchanged from our baseline due to the increase in arcs for image and data sub-networks.

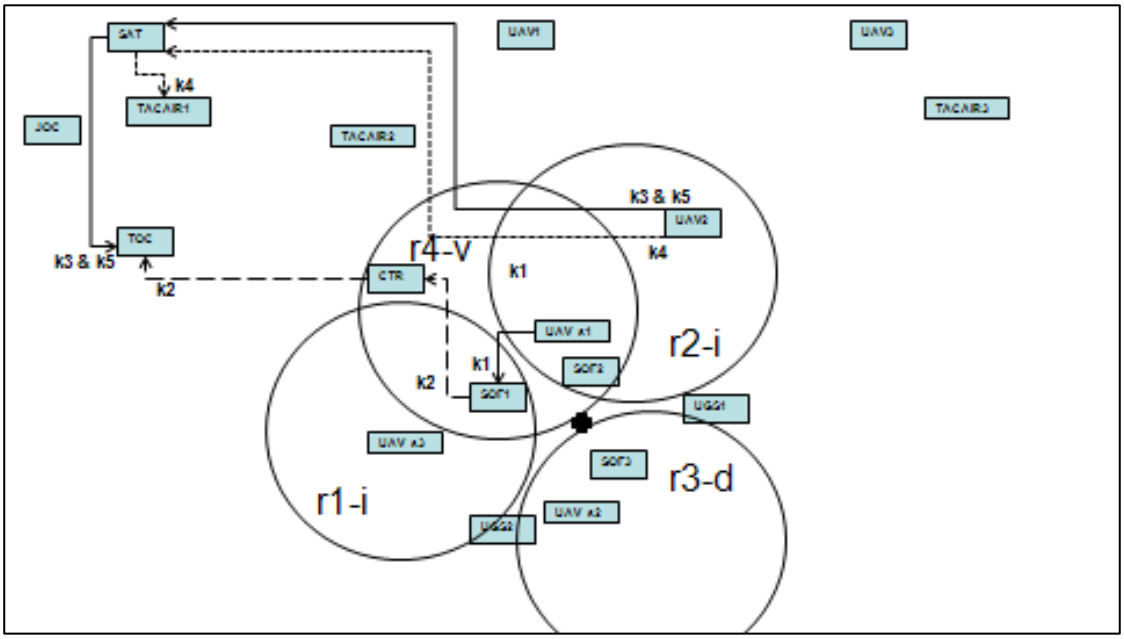

Figure 28. Diagram of Scenario One with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

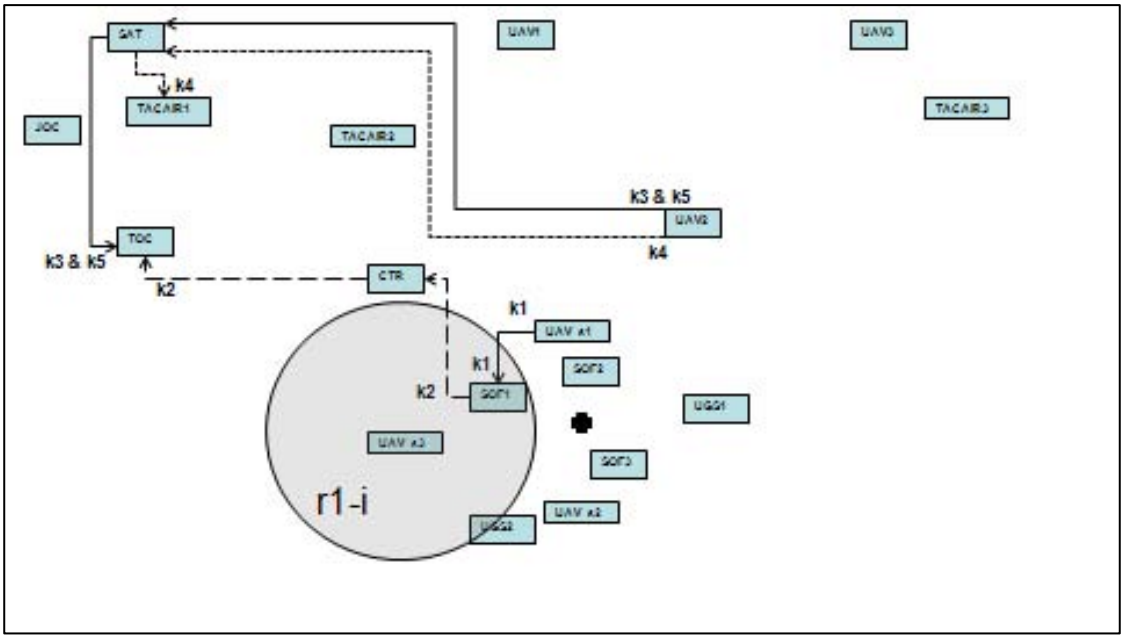

Figure 29. Diagram of Scenario One with appropriate arcs. A jammer is placed at location *r1*, affecting image flow.

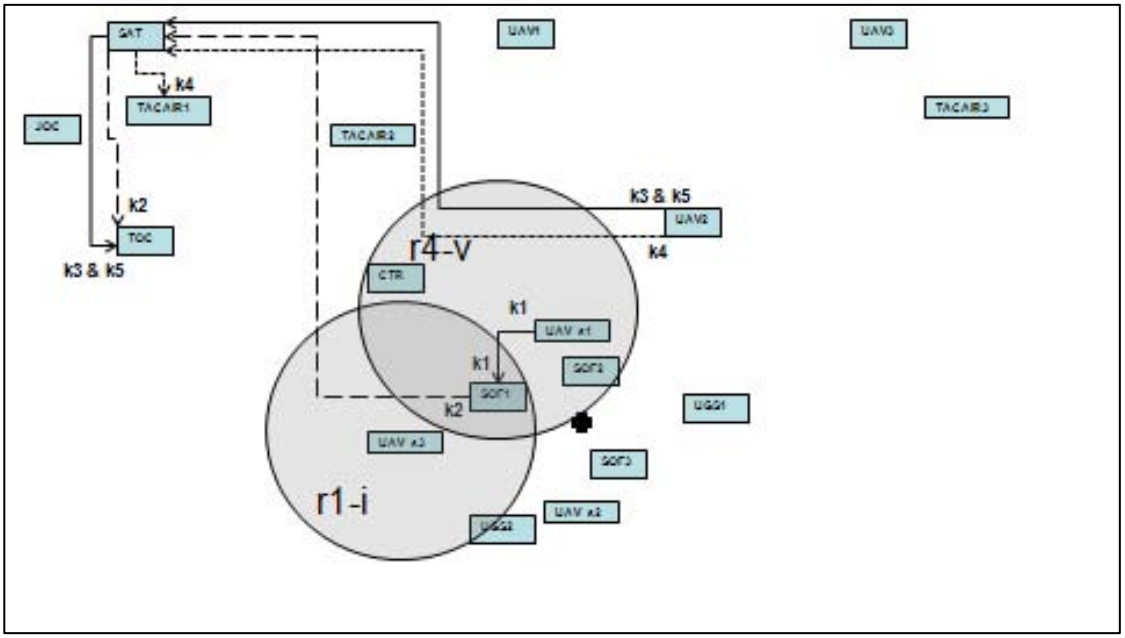

Figure 30. Diagram of Scenario One with appropriate arcs. Jammers are placed at locations *r1* and *r4*, affecting image and voice flow, respectively. Although another jammer is placed in location *r4*, it does not impact this scenario since flow is rerouted to avoid any delays.

Jammers	Cost (seconds)	Locations
0	1032	-
1	1512	r1, r4
2	1512	r1, r4
3	1512	r1, r4
4	1512	r1, r4

Table 13. Summary of Scenario One's output. Additional jammers do not have any effect on this network because those locations do not contain nodes that have any inbound flows. Our image commodity is the only inbound communications flow within range of any jammer location (*r4*), but it only affects voice communications.

2. Scenario Two

Figures 31, 32, and 33 illustrate the kill chain for Scenario Two. Figure 31 is an initial look at the C4ISR network with no jammers. Figure 32 illustrates the solution for the scenario with one jammer placed at *r1*, jamming image flow. Figure 33 illustrates the solution for the scenario with two jammers placed at location *r1* and *r4*. Again, the model changes flow in order to maintain the shortest path from source to destination node. Additional jammers do not have any added effect on this scenario because those locations do not contain nodes that have any inbound flows. The scenario remains unchanged from our baseline due to the increase in arcs for image and data sub-networks.

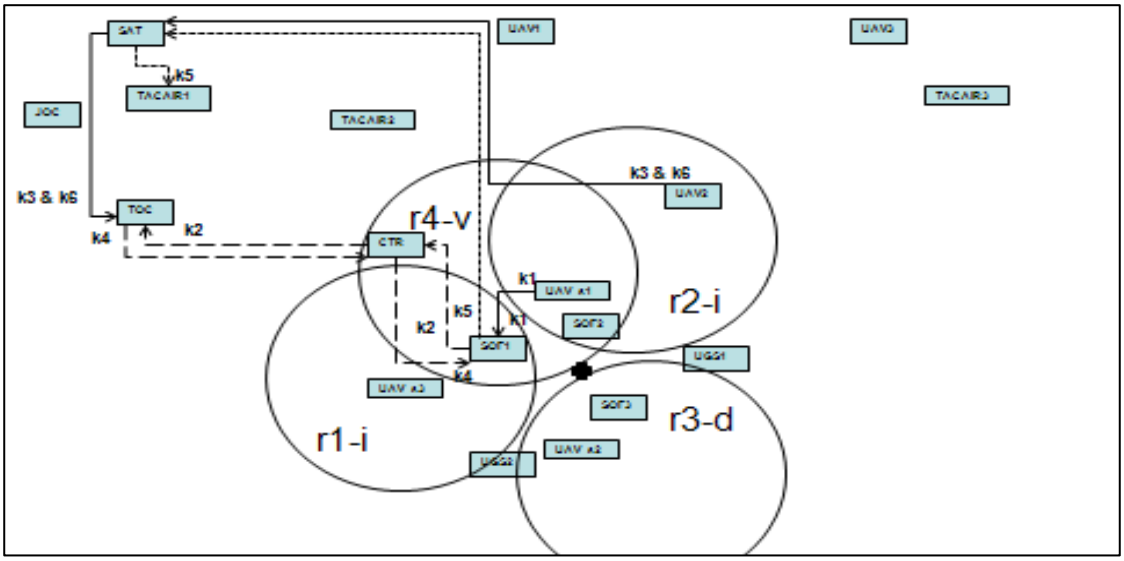

Figure 31. Diagram of Scenario Two with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

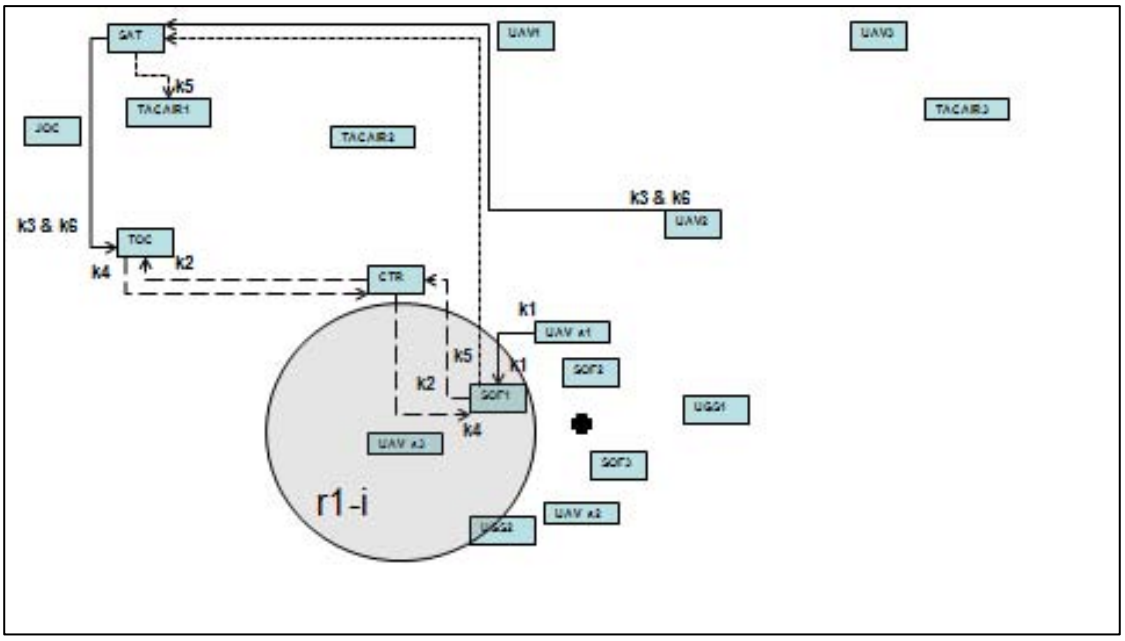

Figure 32. Diagram of Scenario Two with appropriate arcs. A jammer is placed at location *r1*, affecting image flow.

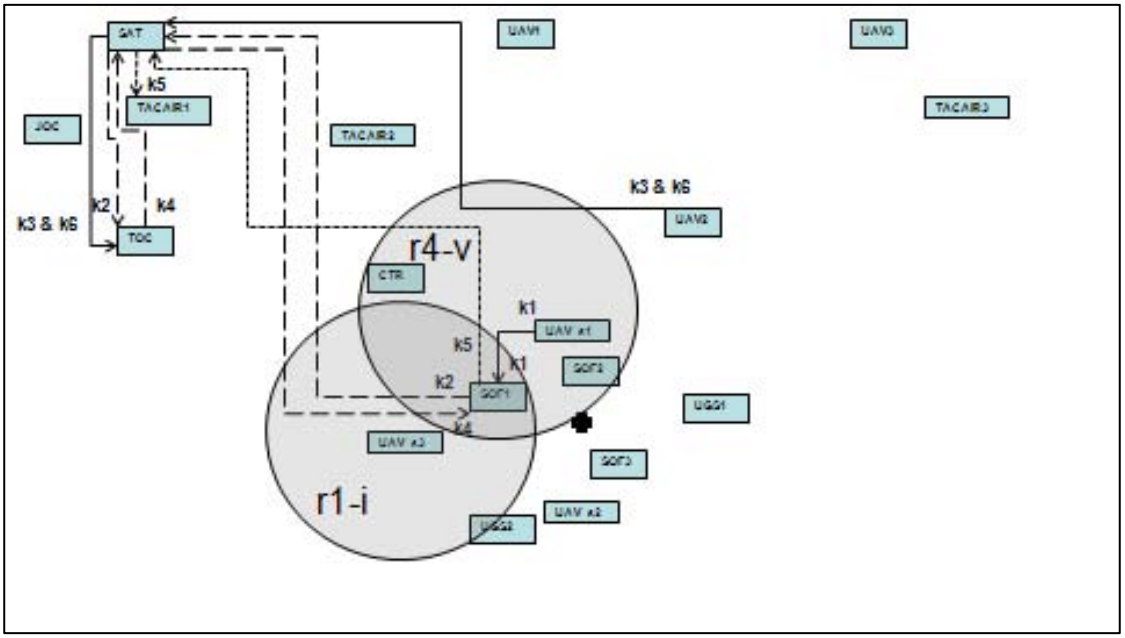

Figure 33. Diagram of Scenario Two with appropriate arcs. Jammers are placed at locations *r1* and *r4*, affecting image and voice flow, respectively.

Jammers	Cost (seconds)	Locations
0	1152	-
1	1632	r1
2	1812	r1, r4
3	1812	r1, r4
4	1812	r1, r4

Table 14. Summary of Scenario Two's output. Additional jammers do not have any effect on this network because those locations do not contain nodes that have any inbound flows.

3. Scenario Three

Scenario Three provides the only changes due to the increase in image and data sub-networks. Figures 34 and 35 illustrate the kill chain for Scenario Three. Figure 34 is an initial look at the C4ISR network with no jammers. Figure 35 illustrates the solution for the scenario with one jammer placed at *r1*, jamming image flow. The model changes image flow in order to maintain the shortest path by directing flow from SOF1 to SOF3. Additional jammers do not have any added effect on this scenario because those locations do not contain nodes that have any inbound flows. Our image commodity is the only inbound communications flow within range of any jammer location (*r3*) but it only affects data communications.

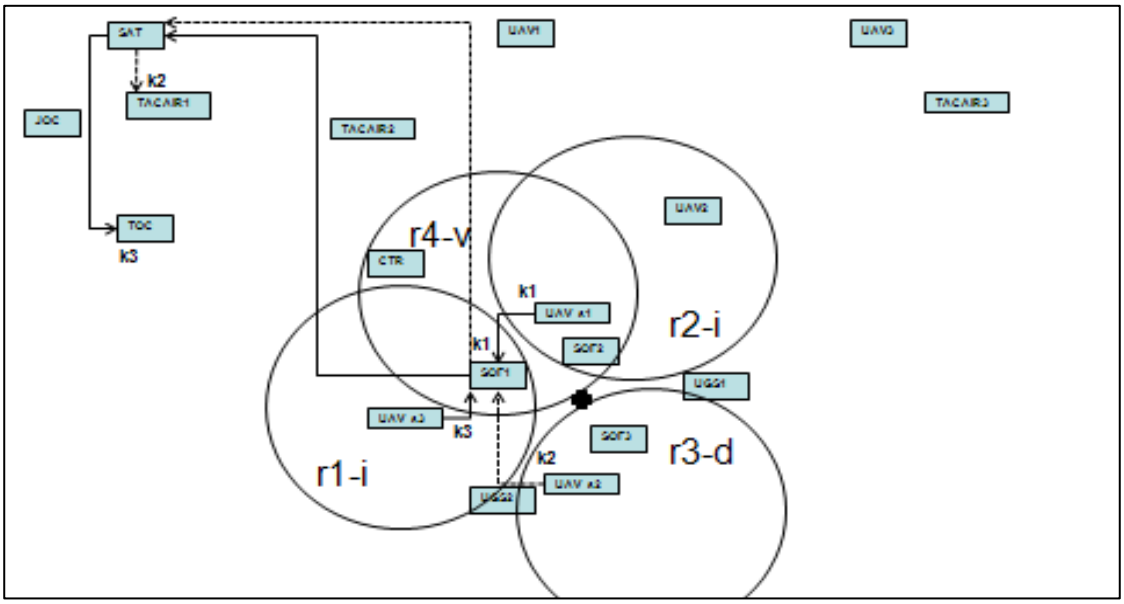

Figure 34. Diagram of Scenario Three with appropriate arcs. No jammers are placed; therefore, no flows are jammed.

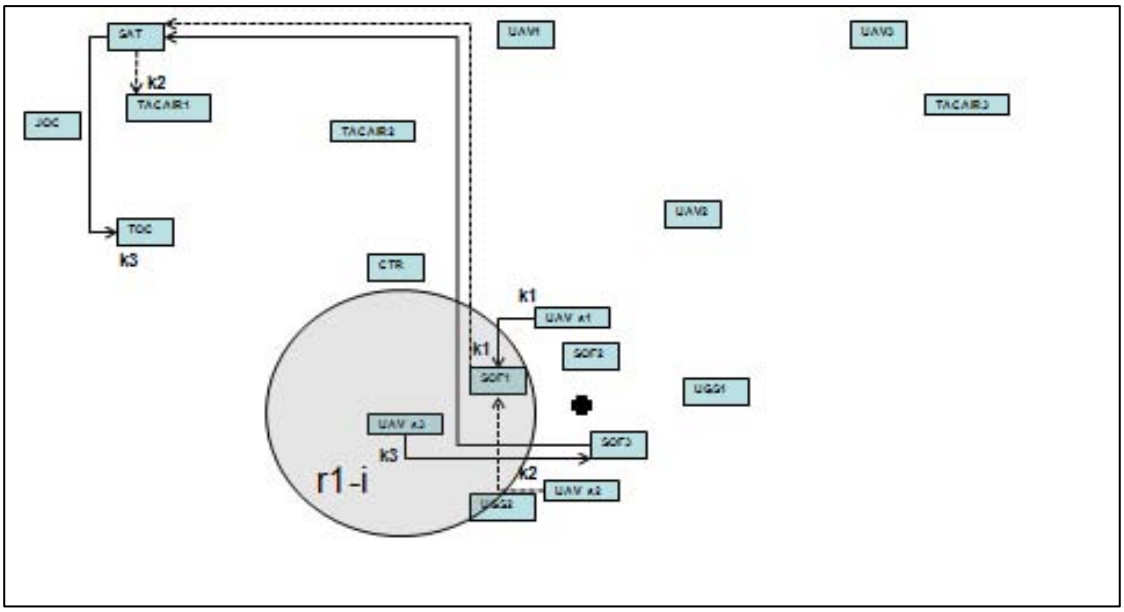

Figure 35. Diagram of Scenario Three with appropriate arcs. A jammer is placed at location *r1*, affecting image flow.

Jammers	Cost (seconds)	Locations
0	762	-
1	1242	r1
2	1242	r1
3	1242	r1
4	1242	r1

Table 15. Summary of Scenario Three's output. Additional jammers do not have any effect on this network because those locations do not contain nodes that have any inbound flows. Our image commodity is the only inbound communications flow within range of any jammer location (*r3*), but it only affects data communications.

F. WHAT THE RESULTS REVEAL

By implementing electronic countermeasures, modifying node locations and configurations, and strengthening the communications network through additional links, we have been able create a network which is less vulnerable and more robust in terms of its effectiveness against an enemy's ability to attack. The attacker-defender model, in particular, is able to determine the optimal JAM_r variables and then determine the resulting optimal flows by solving the minimum cost flow model with the JAM_r variable

fixed at their optimal values, yielding optimal *XMIT* variables. It provides specific insights on redundant pathways, separation of key nodes; and additional communications links.

IV. CONCLUSION

A. SUMMARY

In this thesis, we describe two models. Our operator model of a single C4ISR network determining optimal (i.e., minimal time) communications flows, and our attacker-defender model pinpoints vulnerabilities in the system, allowing us to determine hardening and optimization of current and future systems.

All models and scenarios tested solve in fractions of a second, and preliminary testing indicates these models scale up to larger, more complex networks with only moderate increases in runtime.

B. OPERATIONAL USES

This optimization model enables its user to perform and array of analysis on multiple communications networks. The number of possible combinations for model parameters is large considering number of jammers, their location, range, capacity, nodes, their placement, configurations, and solutions.

Currently, the Warfare Analysis and Integration Department at the Naval Air Systems Command uses standard protocols while configuring communications networks. Primary concerns focus on C4ISR network connectivity and therefore most, if not all, networks are set up on an ad-hoc basis. In most cases this is adequate, but it can leave a C4ISR network vulnerable to enemy attack. This tool enables the user to set up a network against a possible enemy, run a scenario, gather results, and reconfigure if necessary to obtain a better result.

C. FUTURE DEVELOPMENT

Possible future development can be seen in the creation of a graphical user interface (GUI) that interacts with GAMS, improvements in the GAMS formulation to include additional communications within a network rather than key elements of a kill chain, and increased network complexity.

1. Create a Graphical User Interface (GUI)

Currently, all pertinent information is entered directly into GAMS to run the formulation. This task can become daunting given more complex networks. A GUI would improve user interface and lessen the possibility of mistakes. It additionally gives the user more flexibility when configuring networks by decreasing preparation time.

2. Strengthen Formulation

The formulation only takes into account communications needed to complete a kill chain. Even still, not all items within a kill chain are accounted for. This thesis concentrates its efforts on imagery, voice, and data communications. Delays at nodes, due to decisions, and control communications used for controlling UAVs, as well as others, are not used in this formulation.

The inclusion of these parts would provide a more detailed account of how communication networks behave while also providing an improved means of configuring networks to lessen the affects of an enemy attack.

3. Network Complexity

Future testing should include larger scenarios with more complex communications requirements. Further model develop should also include handling multiple simultaneous targets, as would occur during major operations.

LIST OF REFERENCES

Ahuja, R. K., Magnanti, T. L., & Orlin, J. B. (1993). *Network flows: Theory, algorithms, and applications*. Upper Saddle River, NJ: Prentice Hall.

Barkley, T. R. (2008). An attacker defender model for IP based networks. MS thesis, Monterey, CA: Naval Postgraduate School.

Brown, G., Carlyle, M., Salmeron, J., & Wood, K. (2006). Defending critical infrastructure. *Informs,* 36 (6), 530–544.

Markus, John, & DeLia, P. J. (2008). "Jamming." Retrieved March 8, 2010, from http://www.accessscience.com/content.aspx?searchStr=jamming&id=358300

Miller, B., & DeLia, P.J. (2009). "Electronic warfare". Retrieved March 21, 2010, from http://www.accessscience.com/content.aspx?searchStr=electronic+warfare&id=225900

Shankar, A. (2008). Optimal jammer placement to interdict wireless network services. MS thesis, . Monterey, CA: Naval Postgraduate School.

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. Professor W. Matt Carlyle
   Naval Postgraduate School
   Monterey, California

4. Professor David L. Alderson
   Naval Postgraduate School
   Monterey, California

5. Dr. Donald K. Wagner
   Office of Naval Research
   Mathematical, Computer and Information Sciences (Code 311)
   Arlington, Virginia

6. Ken Amster
   Senior Analyst, Warfare Analysis Division
   Naval Air Warfare Center, Weapons Division
   China Lake, California