



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**THE OPTIMAL EMPLOYMENT OF A DEEP SEAWEB  
ACOUSTIC NETWORK FOR SUBMARINE COMMUNICATIONS  
AT SPEED AND DEPTH USING A DEFENDER-ATTACKER-  
DEFENDER MODEL**

by

Andrew D. Hendricksen

September 2013

Thesis Advisor:  
Thesis Co-Advisor:  
Second Reader:

W. Matthew Carlyle  
Joseph A. Rice  
Robert E. Burks

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                 |                                                                |                                                            |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------|--|
| <b>REPORT DOCUMENTATION PAGE</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                 |                                                                | <i>Form Approved OMB No. 0704-0188</i>                     |  |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                 |                                                                |                                                            |  |
| <b>1. AGENCY USE ONLY (Leave blank)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                 | <b>2. REPORT DATE</b><br>September 2013                        | <b>3. REPORT TYPE AND DATES COVERED</b><br>Master's Thesis |  |
| <b>4. TITLE AND SUBTITLE</b><br>THE OPTIMAL EMPLOYMENT AND DEFENSE OF A DEEP SEAWEB ACOUSTIC NETWORK FOR SUBMARINE COMMUNICATIONS AT SPEED AND DEPTH USING A DEFENDER-ATTACKER-DEFENDER MODEL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                 |                                                                | <b>5. FUNDING NUMBERS</b>                                  |  |
| <b>6. AUTHOR(S)</b> Andrew D. Hendricksen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                 |                                                                |                                                            |  |
| <b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b><br>Naval Postgraduate School<br>Monterey, CA 93943-5000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                 |                                                                | <b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>            |  |
| <b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b><br>N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                 |                                                                | <b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>      |  |
| <b>11. SUPPLEMENTARY NOTES</b> 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                 |                                                                |                                                            |  |
| <b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b><br>Approved for public release; distribution is unlimited                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                 |                                                                | <b>12b. DISTRIBUTION CODE</b><br>A                         |  |
| <b>13. ABSTRACT (maximum 200 words)</b><br>The need for submarines to execute communications at speed and depth (CSD) is a vital link in our nation's and our allies' defense network. A promising method to do this without limiting the inherent stealth and advantage of submarines is to utilize Deep Seaweb, an underwater acoustic communication network. The challenge is to be able to optimally employ such a network in a constantly changing environment. In particular, our goal is to develop a network that is resilient to a given number of adversary attacks that can disable individual nodes. To this end, we build and solve a defender-attacker-defender (DAD) optimization model that provides the optimal location of repeater nodes that maintains as much of the function of the network as possible, even after a worst-case attack. We analyze four initial basic network configurations and compare the resulting optimum node placements when the network is not subject to attack, when the network is subject to two attacks, and when the flow of each network configuration is completely blocked by attacks. |                                                                 |                                                                |                                                            |  |
| <b>14. SUBJECT TERMS</b> Defender-Attacker-Defender (DAD), Dual-Integer Linear Program (DILP), Attacker-Defender (AD), Subproblem, Network Optimization, Tri-Level Optimization, Communications Networks, Sensor Networks, Network Design, Network Interdiction, Undersea Distributed Networks, Seaweb, Submarine Communications at Speed & Depth (CSD), Ocean Acoustics, Acoustic Communications, Acomms, FORCEnet, Deep Sound Channel (DSC)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                 |                                                                | <b>15. NUMBER OF PAGES</b><br>117                          |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                 |                                                                | <b>16. PRICE CODE</b>                                      |  |
| <b>17. SECURITY CLASSIFICATION OF REPORT</b><br>Unclassified                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>18. SECURITY CLASSIFICATION OF THIS PAGE</b><br>Unclassified | <b>19. SECURITY CLASSIFICATION OF ABSTRACT</b><br>Unclassified | <b>20. LIMITATION OF ABSTRACT</b><br>UU                    |  |

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**THE OPTIMAL EMPLOYMENT AND DEFENSE OF A DEEP SEAWEB  
ACOUSTIC NETWORK FOR SUBMARINE COMMUNICATIONS AT SPEED  
AND DEPTH USING A DEFENDER-ATTACKER-DEFENDER MODEL**

Andrew D. Hendricksen  
Lieutenant, United States Navy  
B.S., University of Utah, 2004

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN OPERATIONS RESEARCH**

from the

**NAVAL POSTGRADUATE SCHOOL  
September 2013**

Author: Andrew D. Hendricksen

Approved by: W. Matthew Carlyle  
Thesis Advisor

Joseph A. Rice  
Thesis Co-Advisor

Robert E. Burks  
Second Reader

Robert F. Dell  
Chairman, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

The need for submarines to execute communications at speed and depth (CSD) is a vital link in our nation's and our allies' defense network. A promising method to do this without limiting the inherent stealth and advantage of submarines is to utilize Deep Seaweb, an underwater acoustic communication network. The challenge is to be able to optimally employ such a network in a constantly changing environment. In particular, our goal is to develop a network that is resilient to a given number of adversary attacks that can disable individual nodes. To this end, we build and solve a defender-attacker-defender (DAD) optimization model that provides the optimal location of repeater nodes that maintains as much of the function of the network as possible, even after a worst-case attack. We analyze four initial basic network configurations and compare the resulting optimum node placements when the network is not subject to attack, when the network is subject to two attacks, and when the flow of each network configuration is completely blocked by attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

|             |                                                                    |           |
|-------------|--------------------------------------------------------------------|-----------|
| <b>I.</b>   | <b>INTRODUCTION.....</b>                                           | <b>1</b>  |
| <b>A.</b>   | <b>BACKGROUND .....</b>                                            | <b>1</b>  |
| <b>B.</b>   | <b>POSSIBLE APPLICATIONS OF SEAWEB.....</b>                        | <b>3</b>  |
| <b>C.</b>   | <b>PAST RESEARCH .....</b>                                         | <b>4</b>  |
| <b>II.</b>  | <b>PHYSICS BACKGROUND AND SUMMARY .....</b>                        | <b>7</b>  |
| <b>A.</b>   | <b>ACOUSTIC UNDERSEA NETWORKS.....</b>                             | <b>7</b>  |
| <b>B.</b>   | <b>SEAWEB .....</b>                                                | <b>8</b>  |
| 1.          | Seaweb Components .....                                            | 9         |
| 2.          | Seaweb Implementations.....                                        | 13        |
| <b>C.</b>   | <b>SUBLINK.....</b>                                                | <b>16</b> |
| <b>D.</b>   | <b>DEEP SEAWEB.....</b>                                            | <b>25</b> |
| 1.          | Reliable Acoustic Path.....                                        | 26        |
| 2.          | Deep Sound Channel.....                                            | 27        |
| 3.          | Deep Seaweb Concept.....                                           | 30        |
| <b>III.</b> | <b>NETWORK MODEL FORMULATION .....</b>                             | <b>35</b> |
| <b>A.</b>   | <b>DESIGNING A RESILIENT NETWORK.....</b>                          | <b>35</b> |
| 1.          | Network Setup .....                                                | 35        |
| 2.          | Sets and Indices .....                                             | 36        |
| 3.          | Data .....                                                         | 36        |
| 4.          | Variables [type] .....                                             | 37        |
| 5.          | Formulation SUBNET_DAD: .....                                      | 37        |
| 6.          | Discussion.....                                                    | 37        |
| <b>B.</b>   | <b>SOLVING SUBNET_DAD WITH DECOMPOSITION .....</b>                 | <b>38</b> |
| 1.          | New Data.....                                                      | 39        |
| 2.          | Formulation SUBNET_AD: .....                                       | 39        |
| 3.          | Discussion.....                                                    | 39        |
| 4.          | New Data.....                                                      | 40        |
| 5.          | Formulation SUBNET_ROUTING:.....                                   | 40        |
| 6.          | Discussion.....                                                    | 40        |
| 7.          | Formulation SUBNET_AD_DUALILP: .....                               | 41        |
| 8.          | Discussion.....                                                    | 41        |
| <b>C.</b>   | <b>MASTER PROBLEM FORMULATION .....</b>                            | <b>41</b> |
| 1.          | Sets and Indices .....                                             | 42        |
| 2.          | Data .....                                                         | 42        |
| 3.          | Variables [type] .....                                             | 42        |
| 4.          | Model Formulation .....                                            | 43        |
| 5.          | Discussion.....                                                    | 43        |
| <b>D.</b>   | <b>ALGORITHM.....</b>                                              | <b>44</b> |
| 1.          | Variables used in the algorithm not previously defined [type]..... | 44        |
| 2.          | Algorithm SUBNET_DECOMP .....                                      | 44        |
| 3.          | Discussion.....                                                    | 45        |

|                    |                                                                                                 |           |
|--------------------|-------------------------------------------------------------------------------------------------|-----------|
| <b>IV.</b>         | <b>RESULTS, CONCLUSIONS, AND FUTURE WORK.....</b>                                               | <b>47</b> |
| <b>A.</b>          | <b>RESULTS .....</b>                                                                            | <b>47</b> |
| 1.                 | Configuration A .....                                                                           | 48        |
| 2.                 | Configuration B.....                                                                            | 53        |
| 3.                 | Configuration C .....                                                                           | 58        |
| 4.                 | Configuration D .....                                                                           | 64        |
| <b>B.</b>          | <b>CONCLUSIONS .....</b>                                                                        | <b>67</b> |
| <b>C.</b>          | <b>FUTURE WORK.....</b>                                                                         | <b>68</b> |
| <b>APPENDIX A.</b> | <b>ALGORITHM IMPLEMENTED IN GAMS CODE FOR<br/>NETWORK CONFIGURATION A WITH TWO ATTACKS.....</b> | <b>71</b> |
| <b>APPENDIX B.</b> | <b>RESULTING GAMS OUTPUT FILE FOR NETWORK<br/>CONFIGURATION A WITH TWO ATTACKS .....</b>        | <b>81</b> |
|                    | <b>LIST OF REFERENCES .....</b>                                                                 | <b>91</b> |
|                    | <b>INITIAL DISTRIBUTION LIST .....</b>                                                          | <b>97</b> |

## LIST OF FIGURES

|            |                                                                                                                                                                                                                                                 |    |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Figure 1.  | Pictorial representation of the potential applications of underwater acoustic communications (From Schrope 2000).....                                                                                                                           | 3  |
| Figure 2.  | Illustration of the FORCEnet concept (From Rice unpublished Seaweb presentation).....                                                                                                                                                           | 4  |
| Figure 3.  | A deployable autonomous distributed system (DADS) supported by a Seaweb network (From Rice 2000). ....                                                                                                                                          | 7  |
| Figure 4.  | Overview of the basic Seaweb concept (From Grimmer 2009).....                                                                                                                                                                                   | 8  |
| Figure 5.  | The function of the Seaweb server is to connect the submerged network with manned command centers (From Fletcher et al., 2003 and Rice et al. 2001). ....                                                                                       | 10 |
| Figure 6.  | The Seaweb half-duplex handshake protocol (From Rice 2005).....                                                                                                                                                                                 | 11 |
| Figure 7.  | The organization process of the Seaweb network (From Rice 2000). ....                                                                                                                                                                           | 12 |
| Figure 8.  | Buzzards Bay, Massachusetts was the test site for Seaweb '98, '99, and 2000 (From Rice 2000). ....                                                                                                                                              | 14 |
| Figure 9.  | Illustration of the teleseismic link between a submerged submarine and an autonomous off board device (From Rice 2000). ....                                                                                                                    | 17 |
| Figure 10. | Illustration of the Sublink 2000 setup (From Rice 2000). ....                                                                                                                                                                                   | 18 |
| Figure 11. | During Fleet Battle Experiment – India in June 2001, a 14-node Seaweb network undersea grid was installed on the Loma Shelf adjacent to San Diego. Mobile positions near the nodes are indicated by the submarine icon (Rice et al. 2001). .... | 20 |
| Figure 12. | In February, the Seaweb 2003 Q272 Seaweb network in the Eastern Gulf of Mexico included three AUVs, six repeater nodes, and two gateway buoys (From Bachmeyer et al. 2004). ....                                                                | 21 |
| Figure 13. | Seaweb 2004 with 40 nodes. Figure on the left shows the planned deployment, while the right hand figure shows the final position following hurricanes and trawling (From Rice and Green 2008). ....                                             | 22 |
| Figure 14. | The May 2005 Seaweb ARIES (Acoustic Radio Interactive Exploratory Server) Experiment in Monterey Bay (From Ouimet, Hahn, and Rice 2005). ....                                                                                                   | 23 |
| Figure 15. | Conceptual operations among a UUV, surface ship, Directional Acoustic Transponder (DAT), and Smart Marker (From Green 2007). ....                                                                                                               | 24 |
| Figure 16. | The collaboration of many universities and state and federal agencies came together in the implementation of San Francisco Bayweb in May 2009 (From Ramp et. al. 2009). ....                                                                    | 25 |
| Figure 17. | Reliable acoustic paths from a deep source to shallow receivers (From Urlick 1983). ....                                                                                                                                                        | 26 |
| Figure 18. | Ray diagram of transmission in the deep sound channel (DSC) for a source on the axis (From Urlick 1983). ....                                                                                                                                   | 28 |
| Figure 19. | Computer generated ray diagram of the DSC for a source near the axis. Reflected rays are omitted (From Urlick 1983). ....                                                                                                                       | 29 |
| Figure 20. | Worldwide DSC axis depths in meters (From Munk and Forbes 1989)....                                                                                                                                                                             | 29 |

|            |                                                                                                                                 |    |
|------------|---------------------------------------------------------------------------------------------------------------------------------|----|
| Figure 21. | Deep Seaweb concept illustration (From Rice unpublished Deep Seaweb presentation).....                                          | 30 |
| Figure 22. | Worldwide ocean depths in meters (From Amante and Eakins 2009). ....                                                            | 32 |
| Figure 23. | Acoustic modem composition used for Thompson’s DSC analysis (From Thompson 2010). ....                                          | 33 |
| Figure 24. | Optimal node placement without any attacks for configuration A (with 5 repeater nodes). ....                                    | 49 |
| Figure 25. | Optimal node placement with two attacks for configuration A (with 6 repeater nodes and no s nodes blocked).....                 | 50 |
| Figure 26. | Optimal node placement with four attacks for configuration A (with 25 repeater nodes and one s node blocked). ....              | 51 |
| Figure 27. | Optimal node placement with six attacks for configuration A (with 25 repeater nodes and two s nodes blocked).....               | 52 |
| Figure 28. | Optimal node placement with seven attacks for configuration A (with 5 repeater nodes and all flow blocked in the network). .... | 53 |
| Figure 29. | Optimal node placement without any attacks for configuration B (with 7 repeater nodes). ....                                    | 54 |
| Figure 30. | Optimal node placement with two attacks for configuration B (with 13 repeater nodes and no s nodes blocked).....                | 55 |
| Figure 31. | Optimal node placement with four attacks for configuration B (with 13 repeater nodes and no s nodes blocked).....               | 56 |
| Figure 32. | Optimal node placement with six attacks for configuration B (with 21 repeater nodes and two s nodes blocked).....               | 57 |
| Figure 33. | Optimal node placement with seven attacks for configuration B (with 7 repeater nodes and all flow blocked the network). ....    | 58 |
| Figure 34. | Optimal node placement without any attacks for configuration C (with 2 repeater nodes). ....                                    | 59 |
| Figure 35. | Optimal node placement with two attacks for configuration C (with 7 repeater nodes and no s nodes blocked).....                 | 60 |
| Figure 36. | Optimal node placement with four attacks for configuration C (with 8 repeater nodes and no s nodes blocked).....                | 61 |
| Figure 37. | Optimal node placement with six attacks for configuration C (with 14 repeater nodes and no s nodes blocked).....                | 62 |
| Figure 38. | Optimal node placement with eight attacks for configuration C (with 15 repeater nodes and one s node blocked). ....             | 63 |
| Figure 39. | Optimal node placement with nine attacks for configuration C (with 2 repeater nodes and all flow blocked in the network). ....  | 64 |
| Figure 40. | Optimal node placement without any attacks for configuration D (with 7 repeater nodes). ....                                    | 65 |
| Figure 41. | Optimal node placement with two attacks for configuration D (with 20 repeater nodes and no s nodes blocked).....                | 66 |
| Figure 42. | Optimal node placement with four attacks for configuration D (with 7 repeater nodes and all flow blocked in the network). ....  | 67 |

## LIST OF TABLES

|          |                                                                           |    |
|----------|---------------------------------------------------------------------------|----|
| Table 1. | Numerical values for data used in the GAMS code.....                      | 47 |
| Table 2. | Labeling key for the network configurations in Figures 24 through 42. ... | 48 |
| Table 3. | Configuration A for placement of $s$ and $t$ nodes. ....                  | 48 |
| Table 4. | Configuration B for placement of $s$ and $t$ nodes. ....                  | 53 |
| Table 5. | Configuration C for placement of $s$ and $t$ nodes. ....                  | 58 |
| Table 6. | Configuration D for placement of $s$ and $t$ nodes. ....                  | 64 |
| Table 7. | Number of attacks required to completely block the flow in the network.   | 68 |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS AND ABBREVIATIONS

|       |                                                                                                                                   |
|-------|-----------------------------------------------------------------------------------------------------------------------------------|
| AD    | attacker-defender                                                                                                                 |
| ARIES | Acoustic Radio Interactive Exploratory Server                                                                                     |
| AUV   | Autonomous Underwater Vehicles                                                                                                    |
| C4ISR | Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance                                   |
| CDMA  | code-division multiple-access                                                                                                     |
| CDPD  | cellular digital packet data                                                                                                      |
| CPLEX | IBM High-performance mathematical programming solver for linear programming, mixed integer programming, and quadratic programming |
| COTS  | commercial of-the-shelf                                                                                                           |
| CSD   | communications at speed and depth                                                                                                 |
| CTS   | clear-to-send                                                                                                                     |
| DAD   | defender-attacker-defender                                                                                                        |
| DADS  | deployable autonomous distributed system                                                                                          |
| DAT   | Directional Acoustic Transponder                                                                                                  |
| DILP  | Dual-Integer Linear Program                                                                                                       |
| DRDC  | Defence Research and Development Canada                                                                                           |
| DSC   | deep sound channel                                                                                                                |
| DSP   | digital signal processor                                                                                                          |
| DSSS  | direct-sequence spread spectrum                                                                                                   |
| FDMA  | frequency-division multiple-access                                                                                                |
| FHSS  | frequency-hopped spread spectrum                                                                                                  |
| FRONT | Front-Resolving Observation Network with Telemetry                                                                                |
| GAMS  | General Algebraic Modeling System                                                                                                 |

|       |                                            |
|-------|--------------------------------------------|
| ISP   | Internet Service Provider                  |
| LRP   | location routing problem                   |
| MAC   | media-access-control                       |
| MAI   | multi-access interference                  |
| MIMO  | multiple-input–multiple-output             |
| MFSK  | M-ary frequency-shift-keying modulation    |
| MPSK  | M-ary phase-shift-keying modulation        |
| OFDM  | orthogonal-frequency-division-multiplexing |
| ONR   | Office of Naval Research                   |
| OPNET | optimized network engineering tool         |
| PD    | periscope depth                            |
| $r$   | repeater node                              |
| RACOM | radio acoustic communication               |
| RAP   | reliable acoustic path                     |
| RTS   | request-to-send                            |
| $s$   | access point node                          |
| SNR   | signal-to-noise ratio                      |
| SOFAR | sound fixing and ranging                   |
| $t$   | gateway node                               |
| TDMA  | time-division multiple-access              |
| UAN   | underwater acoustic networking             |
| UAV   | unmanned aerial vehicle                    |
| USV   | unmanned surface vehicle                   |
| UUV   | unmanned underwater vehicle                |

## EXECUTIVE SUMMARY

Communication among our forces is a fundamental requirement for national defense. There have been vast resources dedicated to improving, fortifying, encrypting, and expanding the communication resources available to the warfighters of all communities and military branches. Elaborate networks of satellites and aircraft allow the ground troops, airborne troops, and surface sailors to maintain two-way communications with the chain of command. Even the forces below the surface of the ocean have methods of ensuring that they have fairly recent information from the chain of command. Even with the time latency involved, it is still sufficient to maintain the big picture and carry out the mission.

The current method of obtaining this information involves either raising a mast while at periscope depth or surfaced or deploying a receiver and transmitter or transceiver while submerged. These options place restrictions on the submarine that inhibit the submarine's ability to carry out mission tasking. Finding methods for submarines to maintain two-way communications at speed and depth (CSD) has been a high priority for the United States Navy to better capitalize on the strengths of this great asset. One of the available options for CSD is utilizing a Deep Seaweb network for acoustic underwater communications. The Deep Seaweb network has the potential to be a crucial link in the FORCEnet concept that is shaping the way information is shared among all the players in current and future military operations.

Seaweb has been successfully employed in more than fifty sea trials. One of the aspects that is still being developed is utilizing the Seaweb technology in the deep sound channel (DSC) to allow greater spacing between acoustic modems and allow the technology to be utilized in the open ocean with submarines and other underwater vehicles.

We first develop a network design model that takes a given set of access points and gateway nodes and places a fixed number of modems to minimize the number of undelivered packets from the access points. As a secondary objective, the model

minimizes the total number of links used in transmissions from access points to any gateway node, to create an efficient network. This basic model does not account for potential attacks, but because it considers both the design of the network and the operation of the network (through flow variables that model the route taken by messages from each access point), it provides a basis for a tri-level optimization model, called a *defender-attacker-defender* (DAD) model, which determines a network design that is resilient to the worst-case attack that could be mounted against that design.

This thesis executes the algorithm on four different initial network configurations to compare the resiliency of various network topographies and analyzes three attack scenarios for each network configuration: no attacks, two attacks, and enough attacks to completely block all flow in the network. The resulting network design with no attacks provides the basis for the effect of the attacks on each configuration. Networks that have separation among the destination or gateway nodes with at least some of the access point or source nodes near the middle of the area are more resilient. Also, when the destination nodes are not co-located, or at least have some geometric separation, such as opposite sides of grid, it requires more attacks to completely block the flow through the network.

Our models generalize the concept of  $k$ -connectivity used in the designs of communication networks in that they can still provide network designs that retain some functionality, even if some of the sources are disconnected from the destinations. We find that the designs provided by our model and algorithm make sense, but that some of these designs can be quite costly in terms of the number of repeaters required to provide the desired level of resilience. Finally, the algorithms can take quite a while to solve larger versions of these problems, and there is much work to be done in making these algorithms (and possibly models) more efficient.

## ACKNOWLEDGMENTS

I would like to publicly acknowledge my Heavenly Father's hand in my life and thank Him for all that He has done to help me complete this thesis. He helped me get through the classes and the many projects leading up to this point. I truly would not have been able to complete this thesis on my own, for I know that "with God, all things are possible" Matthew 19:26, and that He promises that we "should be diligent, that thereby [we] might win the prize," Mosiah 4:27. I am eternally grateful that the Lord has helped me to grow so much and reach this pinnacle in my academic career. It is definitely true that behind every good man is an even better woman, and in my case, two. While I will not claim to be perfect, I try my best to be a good man, but it is only possible because my best friends in the world and in the eternities, my wife, Melanie, and my daughter, Abigail, have always supported and encouraged me despite my faults and follies. My wife always manages to overlook my faults and treat me like the man she and the Lord know that I can be. My daughter manages to always bring a smile to my face and remind me why it is all worth it. Whenever I return home, she runs to give me a big hug, yelling, "Daddy's home!" Most of the credit for this thesis and for the man that I have become goes to the Lord and to these two awesome women.

I am extremely grateful to my thesis advisor, W. Matthew Carlyle, and my thesis co-advisor, Joseph A. Rice. They were able to help me complete this thesis despite their very busy research and travel schedules. They made time for me even though deployments placed us in separate parts of the country and even halfway around the world. They also collaborated well between the Operations Research and Physics departments. I am thankful for their willingness to share their knowledge and experience. They provided guidance on the best way to limit the scope of this thesis to keep it manageable. I am thankful for the backup and support of my second reader, COL Robert E. Burks, and for the time that he took to lend his expertise in editing my thesis and providing mentorship both academically and professionally. I would also like to thank Lisa Puzon for all her help and support in completing the administrative requirements for all the classes and this thesis.

I would like to thank the many professionals at Johns Hopkins University Applied Physics Laboratory for the jump start that they provided as they hosted me during my experience tour while I was conducting my thesis research. Specifically, I would like to acknowledge John Tochko, William Kroshl, Larry Green, Chris Watkins, Matt Vonada, Maria Hoffacker, Shirley Musgrove, and Charlene Roelecke.

There were other professionals who were very helpful in assisting me in narrowing down the topic of this thesis, including Bob Headrick, Ocean Acoustics Program Director at the Office of Naval Research Division 322; as well as CAPT Steve Perry, the branch head for Undersea Warfare Acquisition and Modernization (OPNAV N97); and CAPT Chris Anklam, the branch head for Information Dominance (OPNAV N81F); both from the Office of the Chief of Naval Operations.

I would like to thank some of the many people who encouraged my love for learning throughout my life. My parents, David and Mayleen, supported me through my childhood and adult education. Gary Turner strengthened my love for math, chemistry, and physics. Linda Turner and Carolyn Southerlin continually challenged me in English and always expected my best writing for every essay or assignment. Brian Felsch helped me understand the biological sciences.

# **I. INTRODUCTION**

## **A. BACKGROUND**

Communication among our forces is a fundamental requirement for national defense. Over the last several decades, it has become possible for all ground troop members to carry handheld radios that enable the accurate and timely flow of information both up and down the chain of command. This has proven to be advantageous, making it possible for every land unit to maintain near instantaneous communications with headquarters. The aviators have sophisticated equipment to ensure that they have timely information regarding target locations, rules of engagement, and situational awareness. Those sailors on the sea surface have sophisticated equipment to maintain two-way communications with the chain of command. Elaborate networks of satellites and aircraft tie all these forces together.

There is one facet of our communications network that is not as robust as the others: the link to submerged submarines. Even though our forces below the surface of the ocean have methods of ensuring they have fairly recent information from the chain of command, there is still some time latency involved. Although it is not up to the minute, it is generally only a few hours old and is sufficient to maintain the big picture and carry out the mission. The importance of submarines is emphasized in *A Cooperative Strategy for 21st Century Seapower* and the *Naval Operations Concept* for 2006 and 2010. Given the importance of communications, it is imperative to ensure that this vital link to our submarine troops is fortified, improved, and encrypted to ensure that sensitive information does not fall into the wrong hands and lead to our disadvantage both on and off the battlefield. Communication with submarines without compromising their inherent stealth and ability to effectively carry out the mission remains a challenge. Finding methods for a submarine to maintain real-time, two-way communications at speed and depth (CSD) has been a high priority for the United States Navy in recent years to better capitalize on the strengths of this important asset.

The current options for CSD involve strict speed and depth limitations because the submarine must extend a receiver and transmitter or a transceiver. This can be done by 1) raising a mast while at periscope depth (PD) or surfaced, or 2) deploying a receiver and transmitter or a transceiver from the submarine while submerged. The first option places the submarine at increased risk while at periscope depth and while surfaced greatly compromises the stealth of the submarine and their ability to carry out the mission. The second option involves strict speed and depth restrictions to deploy a receiver and transmitter or a transceiver. The device can then be useful for transmitting information only while it remains tethered to the submarine, which limits the submarine in speed and depth as long as the device remains connected. An alternative means of communication without these constraints would empower submarines to better carry out mission tasking.

There are several advanced methods of CSD that are in the research and development phase. One such method is using lasers to establish two-way communication between the submarine and an airborne platform. The disadvantage of this method is that either the submarine is required to be in a given area for an extended length of time so the message can be systematically broadcast over the specified area and the submarine can then send any outgoing information or it must come to PD to indicate its position. The submarine could also remain at PD and receive and transmit information by radio frequency. It could take advantage of the higher bandwidth available from the laser, which would require a shorter time at PD.

Another CSD option is long-range acoustic communications. There are several possibilities for this option. One of them uses towed arrays, source moorings, and moored vertical-line-array receivers, but the towed array limits the maneuverability of the submarine and the low frequency limits the communications bandwidth and interferes with sonar contacts. It is also possible to use long-range extremely low frequency acoustic transmitters. This method is only one-way and, due to the high power required to transmit great distances, the transmitters must be very large with either a short battery life or shore based which limits the application when the submarine ranges too far from land. Each of these methods imposes various restrictions on the submarine.

Utilizing a Deep Seaweb network for acoustic communications is another possibility for two-way communications with the submarine that does not have the same limitations as the current options. This method could utilize the larger bandwidth of radio frequencies or lasers for the gateway buoys.

## B. POSSIBLE APPLICATIONS OF SEAWEB

There are many possible applications for underwater acoustic communications. Schrope in *Business 2.0* illustrates one of these concepts in Figure 1.

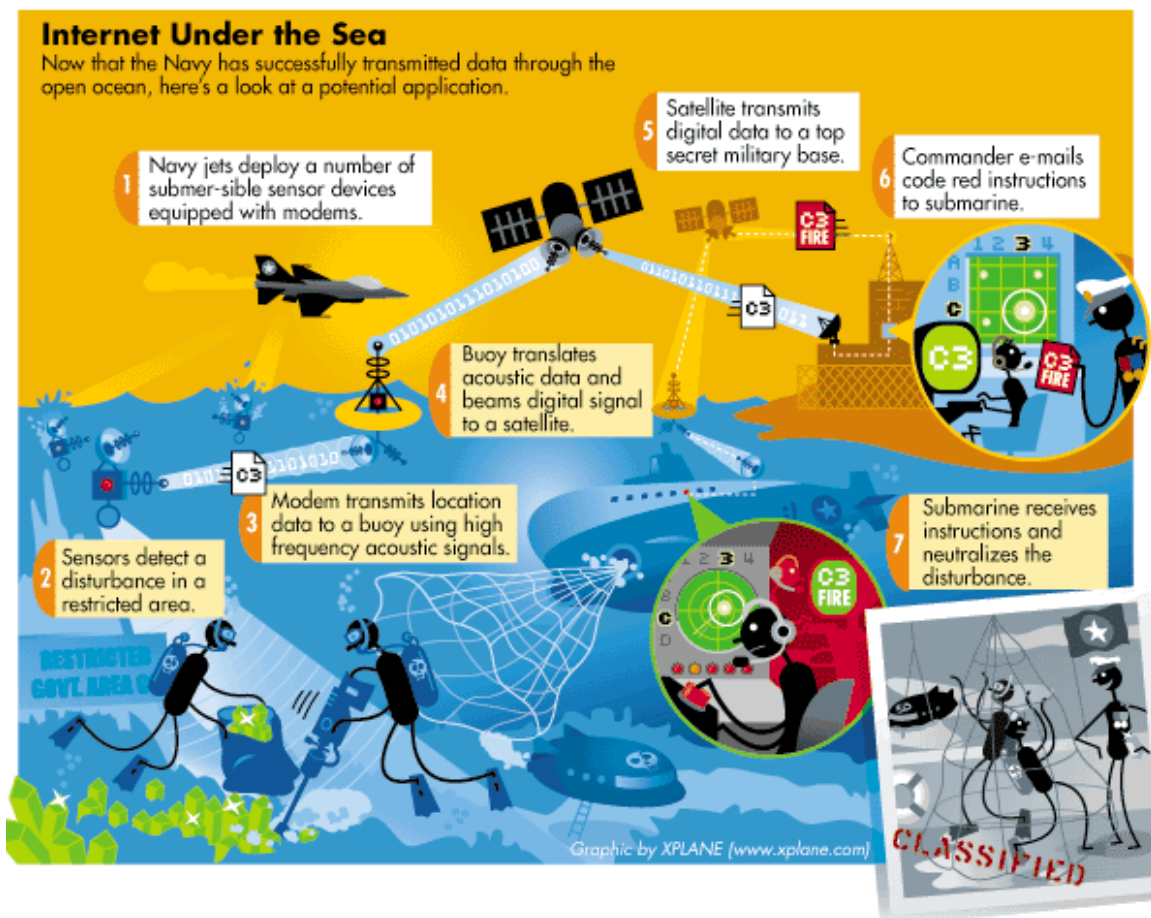


Figure 1. Pictorial representation of the potential applications of underwater acoustic communications (From Schrope 2000).

Another application is the FORCEnet concept. Both Ackerman (2004) and Browne (2004) discussed the significance and the challenges facing the Navy in

developing this concept. This complex endeavor has been the focus of the Navy's network-centric warfare thrust for more than a decade now. This concept, illustrated in Figure 2, ties together all the warfare communities allowing them to share information as close to real time as possible. Utilizing this more timely information flow empowers the military forces of all communities and branches to work together in a manner that would otherwise be impossible.

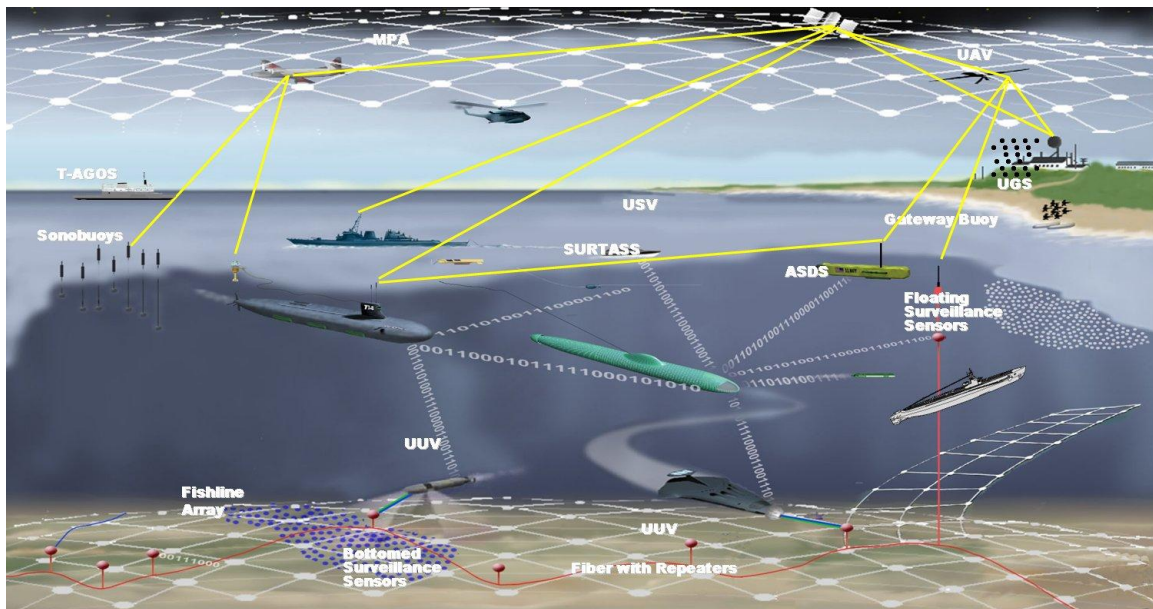


Figure 2. Illustration of the FORCEnet concept  
(From Rice unpublished Seaweb presentation).

### C. PAST RESEARCH

There has been significant research done on the multiple facets of underwater acoustic communications. Biediger (2010) explored the environmental considerations for passive detection of maritime targets. Kriewaldt (2006) analyzed the communications performance of a wide-area network application of Seaweb. Goh (2010) analyzed various network protocols of the underwater local area network known as “Seastar.” Ong (2008) analyzed the initialization process of spontaneously deployed versions of Seaweb. Zinkhon (2009) utilized a node localization algorithm to estimate the relative locations of all nodes in an ad hoc Seaweb placement. Green, Rice, and Merriam (1998) explored the

aspects involved in the physical design of the modems used in the Seaweb networks. McGirr et al. (1999) highlighted some of the key aspects involved in the network design and analysis of the deployable autonomous distributed system (DADS).

Grimmett (2007) analyzed the message routing criteria for underwater acoustic communications networks and utilized Dijkstra's algorithm to solve for hypothetical network configurations. Li et al. (2009) presented a multiple-input-multiple-output (MIMO) system design that applies spatial multiplexing with orthogonal-frequency-division-multiplexing (OFDM) signals. Nicholas (2009) explored the challenges of quickly and optimally designing a wireless mesh network. Shankar (2008) explored the challenges of operating and jamming wireless mesh networks. Sanchez (2010) described one of the processes used by Internet Service Providers (ISPs) when designing and maintaining internet networks. Bohner (2003) used a distributed underwater acoustic networking (UAN) protocol for ad hoc deployment of stationary and mobile nodes across a relatively wide area. Sözer, Stojanovic, and Proakis (2000a) discussed using an optimized network engineering tool (OPNET) modeler to design and test an underwater acoustic ad hoc network. Proakis et al. (2003) discussed several design considerations for shallow water acoustic networks to maximize throughput and reliability with minimum power consumption.

Belenguer et al. (2006) applied a branch and cut method to the location routing problem (LRP). Barreto (2007) implemented cluster analysis to minimize the routing and location costs of a LRP. Berger, Coullard, and Daskin (2007) utilized a set-partitioning-based formulation of an uncapacitated location-routing model with distance constraints. Brown, Carlyle, and Wood applied defender-attacker-defender (DAD) optimization to terror risk management and mitigation in 2008 in appendix E of the *Department of Homeland Security's Bioterrorist Risk Assessment: A Call for Change*. Alderson et al. (2011) developed a DAD sequential game model for infrastructure systems that improves an infrastructure's resilience to attacks from an intelligent adversary. Brown et al. (2006) applied bi-level and tri-level optimization models to fortify critical infrastructures against terrorist attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

## II. PHYSICS BACKGROUND AND SUMMARY

### A. ACOUSTIC UNDERSEA NETWORKS

The requirement for wide-area undersea surveillance in littoral waters using a deployable autonomous distributed system (DADS), such as shown in Figure 3, has motivated the development of Seaweb (Rice and Green 2008). The littoral surveillance application typically involves water depths up to 300 meters and node separations up to 5 kilometers with data packets of about 1,000 information bits (McGirr et al. 1999).

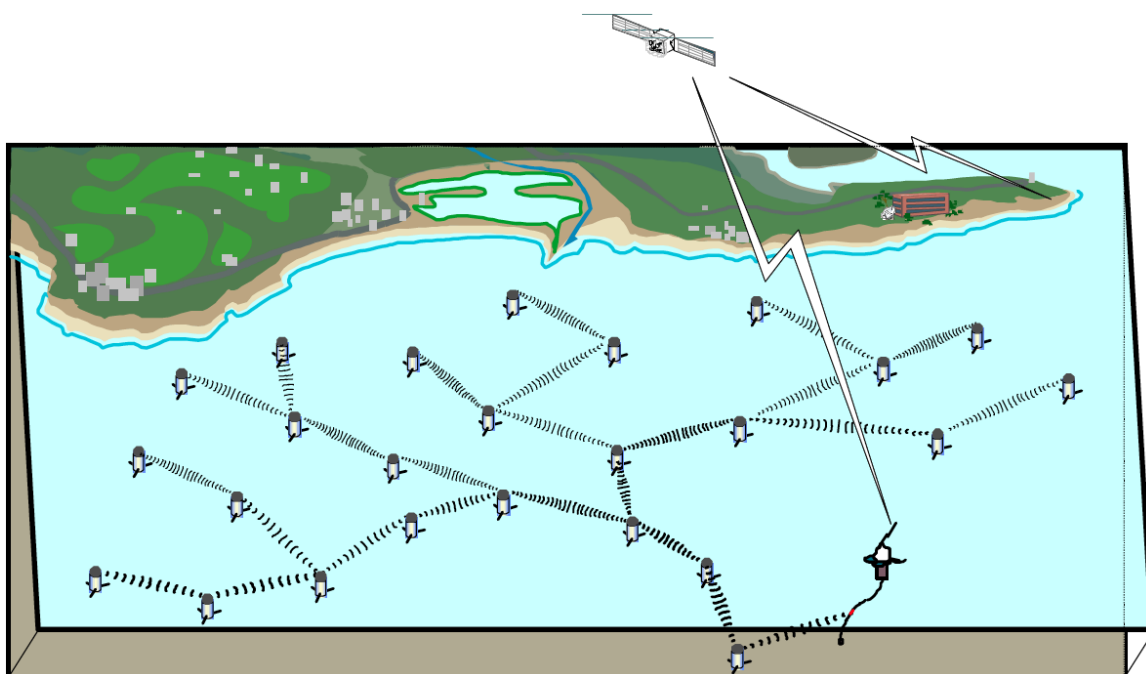


Figure 3. A deployable autonomous distributed system (DADS) supported by a Seaweb network (From Rice 2000).

There are several aspects of the water environment that constrain the performance of an underwater acoustic communications network: the relatively slow speed of sound through water, multipath propagation, ambient noise, limited spectral bandwidth, and ambient noise (Rice and Green 2008). Nevertheless, Seaweb has been shown to be a viable option for CSD.

## B. SEAWEB

Seaweb has evolved into an underwater acoustic network that can be used for communications, maritime surveillance, oceanographic monitoring, underwater positioning, and many other purposes as depicted in Figure 4. Battery-powered nodes in the Seaweb network can potentially be launched from various platforms such as submarines, ships, aircraft, unmanned underwater vehicles (UUVs), or unmanned aerial vehicles (UAVs), allowing great flexibility in deploying an appropriate combination of node types and concentration for any given mission and environment.

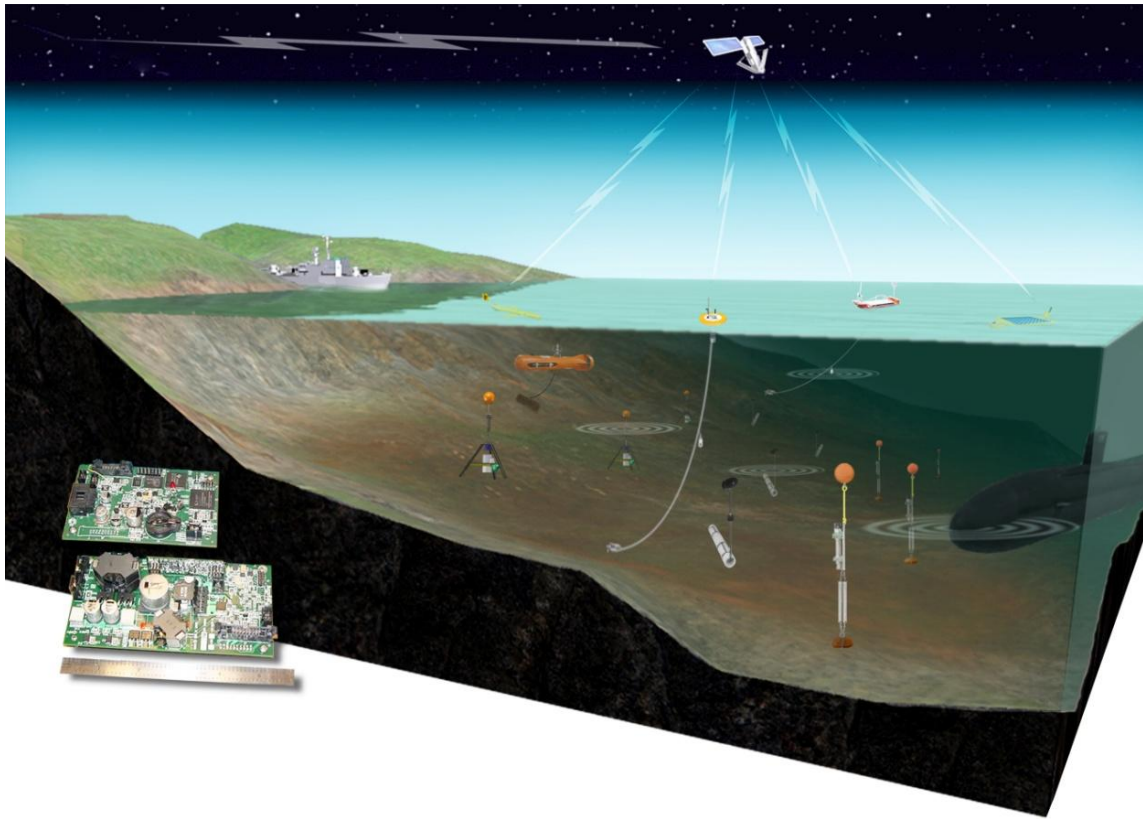


Figure 4. Overview of the basic Seaweb concept (From Grimmer 2009).

The capability of two autonomous underwater vehicles (AUVs) to maintain two-way communications was demonstrated in 1993 by a field study conducted in Barrington, New Hampshire (Chappell et al. 1994). Seaweb built upon that result and expanded it to an underwater acoustic network. Rice summarized the Seaweb basic concept of

operation as, “Telesonar wireless acoustic links [that] interconnect distributed undersea assets, potentially integrating them as a unified resource and extending ‘net-centric’ operations into the undersea environment” (2000). Seaweb is the real world application of undersea wireless networks (Sözer, Stojanovic, and Proakis 2000b) to include fixed and mobile nodes, intelligent master nodes, and manned command centers. It also provides a good coordinating infrastructure for Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance (C4ISR) for any mission in an ocean environment.

### **1. Seaweb Components**

Seaweb has several basic components: *backbone*, *peripherals*, *gateways*, and *servers*. The *backbone* is a set of autonomous, stationary nodes (*e.g.*, deployable surveillance sensors, sea mines, relay stations, etc.). The *peripherals* are the mobile nodes (*e.g.*, unmanned underwater vehicles (UUVs) to include swimmers and crawlers) and specialized nodes (*e.g.*, bi-static sonar projectors). The *gateways* connect the various command centers whether submerged, afloat, airborne, or ashore. For Seaweb, these gateways are telesonar nodes to link the submerged acoustic network to other airborne, terrestrial, and satellite networks. The *servers* are co-located with the manned command centers and act as an interface to the submerged acoustic network as shown in Figure 5. The server keeps an archive of all inbound data packets while allowing client stations read-only access over the internet. Only one “super” server reconfigures and controls the network as needed (Fletcher et al. 2003 and Rice et al. 2001).

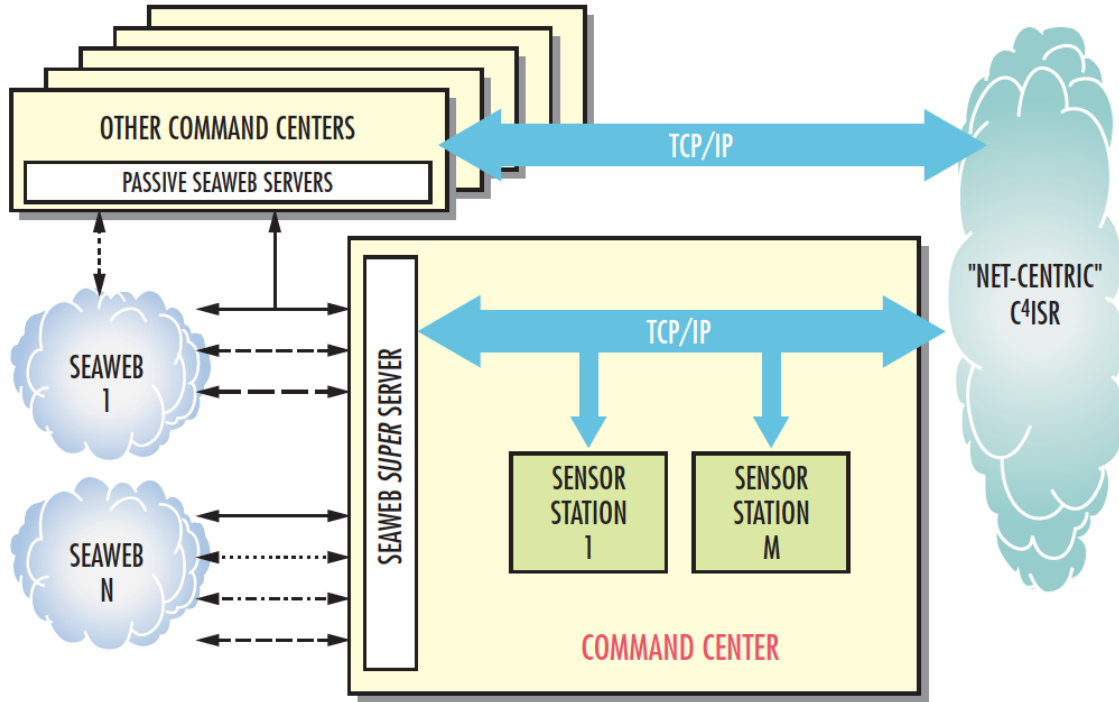


Figure 5. The function of the Seaweb server is to connect the submerged network with manned command centers (From Fletcher et al., 2003 and Rice et al. 2001).

The architecture of Seaweb is hierarchical with three fundamental layers of interest: the physical layer, the media-access-control (MAC) layer, and the network layer. These communication layers provide a functionality that can support higher application-specific layers (Rice 2000).

Adaptive telesonar links are established asynchronously using a half-duplex handshaking protocol depicted in Figure 6. The initiating node, A, transmits a request-to-send (RTS) signal using a frequency-hopped spread spectrum (FHSS) series or a direct-sequence spread spectrum (DSSS) pseudo-random carrier specific to the receiver node, B. The initiating node could also issue a RTS when broadcasting or linking to unknown nodes. Upon receiving the RTS, node B comes out of a low-power sleep mode, demodulates the signal, and processes the signal to estimate the channel scattering function and signal excess. Node B then acknowledges the RTS by sending a FHSS or DSSS clear-to-send (CTS) signal to node A specifying the data-packet modulation parameters based on the existing channel conditions. After this concise RTS/CTS

handshake, node A transmits the data packet(s) taking full advantage of the optimal bit-rate, modulation, coding, and source level (Rice 2005).

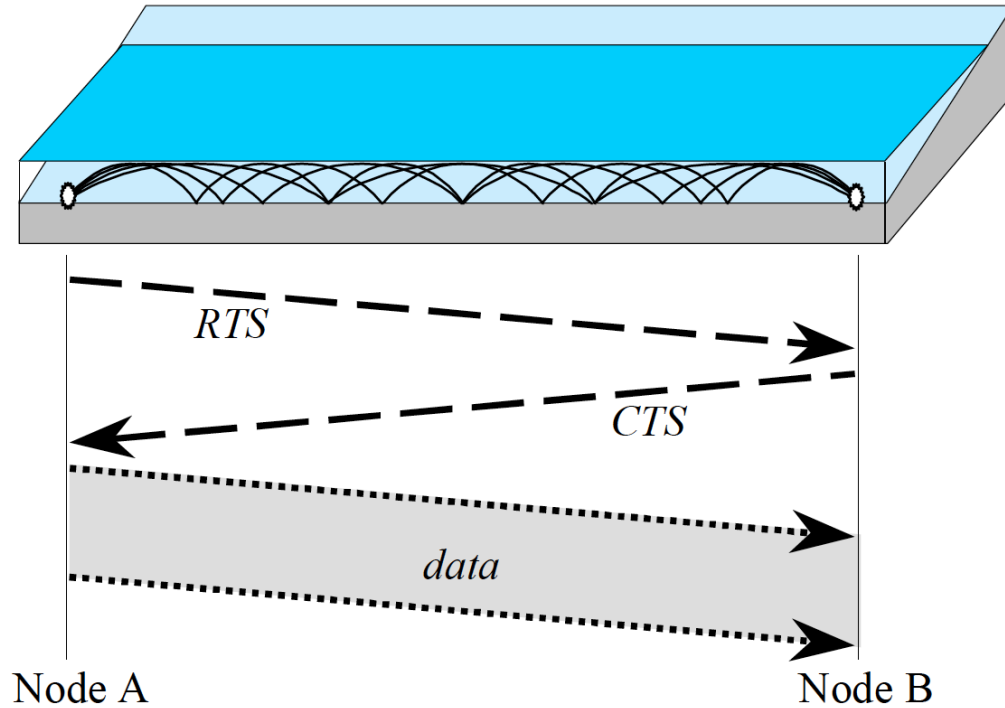


Figure 6. The Seaweb half-duplex handshake protocol (From Rice 2005).

An understanding of the physical layer is reached through measuring existing transmission channel conditions and numerical propagation models. Combining this with digital signal processor (DSP) modulators and demodulators allows the exploitation of the unique characteristics of the underwater channel while directional transducers improve modem performance (Rice 2000).

The MAC layer's purpose is to support secure, low-power, point-to-point connectivity. The handshaking protocol just described is well suited to wireless half-duplex networking with slowly propagating channels while providing addressing, ranging, channel estimation, adaptive modulation, and power control. It is necessary for the telesonar links to adapt to a changing environment while allowing for bi-directional asymmetry. Asynchronous multiple-access to the physical channel can be provided through spread-spectrum modulation using code-division multiple-access (CDMA), time-division multiple-

access (TDMA), or frequency-division multiple-access (FDMA) methods. The Seaweb network is then configured and maintained through the master nodes to allow network adaptation following node failure, addition of new nodes, and incorporation of mobile nodes. As the telesonar links are established, range measurement, range-rate measurement, and clock-synchronization are obtained which allows network initialization, navigation, and optimization. This process is described in Figure 7 (Rice 2000).

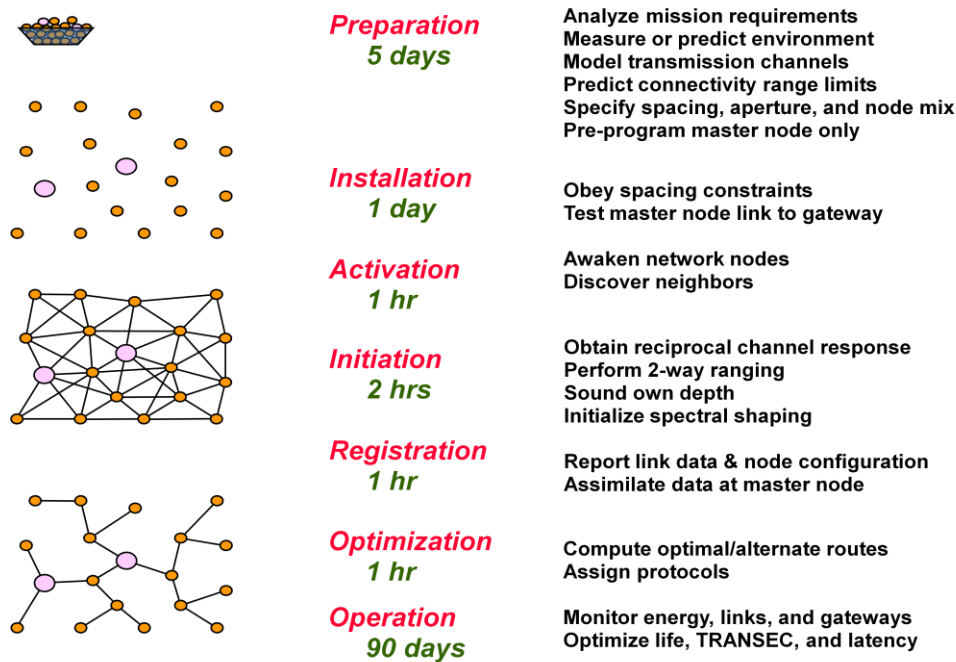


Figure 7. The organization process of the Seaweb network (From Rice 2000).

An optimized network engineering tool (OPNET) is used to simulate the Seaweb using basic ocean acoustic propagation assumptions allowing various network arrangements and protocols to be explored and refined in the laboratory (Raysin et al. 1999) while controlled sea trials improve telesonar signaling technologies (McDonald et al. 1999).

Seaweb then combines the results from this research with the resources of extended ocean experiments. The annual Seaweb experiments have been able to verify system analysis and promote essential technologies to ensure that Seaweb continues to evolve toward higher reliability and increased functionality. The goal of these

experiments is to provide a means of implementing and testing telesonar modems in networks using various modulations and networking algorithms. As improvements are noted and implemented, the ultimate goal can be reached: an acoustic network that is self-configuring with links that automatically adjust to the existing environmental conditions by properly selecting the optimal transit parameters (Rice 2000).

## **2. Seaweb Implementations**

Seaweb technology was used in the May Sublink 2000, the April ForeFRONT-2 and June FRONT-2, both during the same year (Codiga et al. 2000). This extended use allowed collection of valuable long-term performance data. Buzzards Bay, Massachusetts, shown in Figure 8, was the site for the annual Seaweb experiment for the first three years, 1998, 1999, and 2000. This site was chosen since it is within line-of-sight radio contact with Datasonics and Benthos in western Cape Cod (Rice 2000).

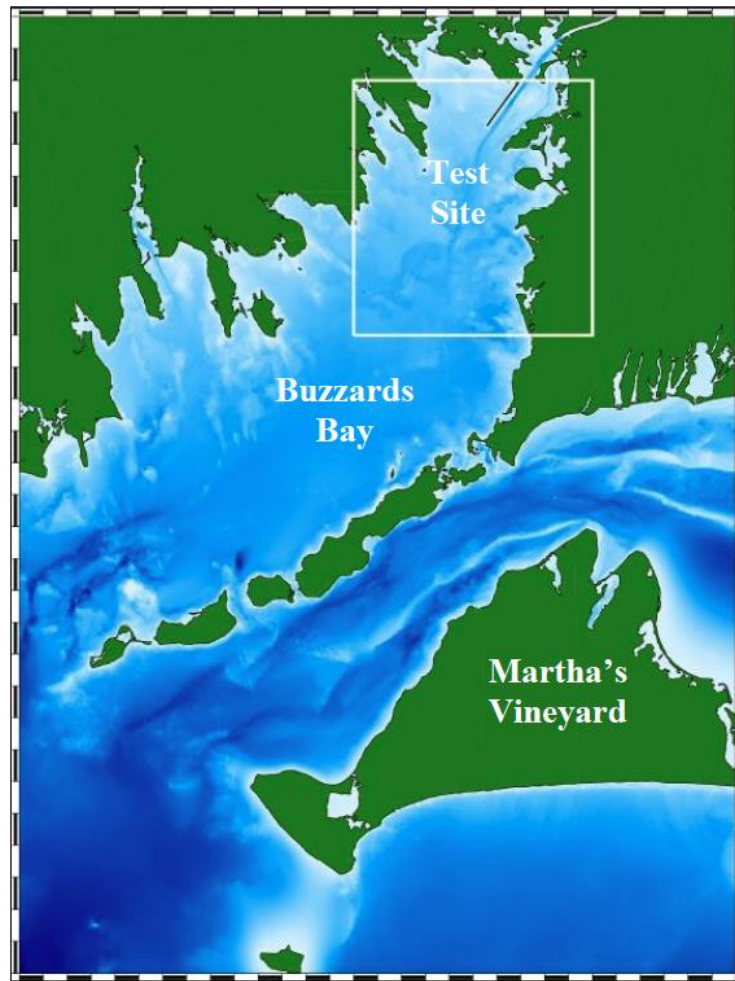


Figure 8. Buzzards Bay, Massachusetts was the test site for Seaweb '98, '99, and 2000 (From Rice 2000).

There are several important results from Seaweb '98. One of the most important is that the network consistently provided high quality data. Only approximately 2% of the data packets delivered to the command centers had uncorrected bit errors, which came from the intentional collisions at the master node. There were several important network concepts illustrated by Seaweb '98: 1) the ability to store and forward data packets, 2) transmit retries and automatic repeat request, 3) packet routing, and 4) mitigated minimize multi-access interference (MAI) through FDMA node cell-like grouping. Several application DADS concepts were also illustrated: 1) networked underwater sensors, 2) wide-area coverage, 3) acoustic/radio interface, 4) robustness in a shallow-water environment, 5) robustness during shipping noise, 6) use of sleep modes for low-

power node operation, 7) economic feasibility, and 8) remote control. Seaweb '98 also highlighted the difference between acoustic and conventional networks: Limited power, low bandwidth, and long propagation times (Rice 2000).

Seaweb '99 continued the advancement of undersea wireless networks. All links in the network used a simple telesonar handshake protocol allowing automatic packet-collision resolution through transmitter retries or receiver repeat requests. The multi-access strategy used a variation of FDMA, which was an important step toward self-configuration and precedes the use of secure CDMA spread-spectrum unique codes assigned to each node during initialization. Node-to-node ranging was simplified. One of the most important aspects of Seaweb '99 was the implementation of a Seaweb server, run on a laptop computer, to continually monitor, display, and log network status. The server also bridged the connection between a Bell Atlantic cellular digital packet data (CDPD) gateway node over the internet and a radio gateway link to establish a gateway-to-gateway route through the server. The server was able to remotely reconfigure network routing, which is one important step closer to self-configuration and dynamic network control.

There were several implementations of Seaweb technology between Seaweb '99 and Seaweb 2000: the ForeFRONT-1 (Front-Resolving Observation Network with Telemetry) (November 1999), FRONT-1 (December 1999), ForeFRONT-2 (April 2000), Sublink 2000 (May 2000), and FRONT-2 (June 2000) experiments. These greatly aided the firmware transition from the ATM875 modem, which was used in Seawebs '98 and '99, to the ATM885, which was used in Seaweb 2000 and has a more powerful DSP and more memory (Rice 2000).

Seaweb 2000 firmware used the foundation of a structured protocol to map the network and MAC layers onto the physical layer based on channel conditions. It used seven utility packet types while OPNET simulations were used to explore expanding that number. The initial handshake utilized the RTS/CTS combination, forming a basis for adjusting the data modulation for channel conditions. Data packets are sent following the RTS/CTS interchange. Seaweb 2000 used a hybrid CDMA/TDMA approach vice the FDMA to help avoid MAI. It also implemented two parallel Seaweb networks, the one at

the command center is airborne and the other one in Buzzards Bay is water-borne, allowing troubleshooting firmware and code change testing prior to at-sea downloads. All modems now logged the data in an internal buffer allowing the study of individual nodes following sea trials. The modem firmware used additional channel-estimation diagnostics (e.g., SNR, multipath spread, Doppler spread, range rate, etc.), demodulation statistics (e.g., bit-error rate, automatic gain control, intermediate decoding results, power level, etc.), and networking (e.g., data packet source, data packet sink, routing path, etc.) (Rice 2000).

The data logging allows a modem to archive the data packets. This means that a node could be designated as a sink node and collect all packets from the network until requested by a gateway, which could be a ship arriving on station. An internal watchdog timer provides a means to automatically reboot a modem if required. SignalEx, an applied telesonar research effort, was hosted by Seaweb 2000 with shared resources and empirical test control. Several experimental network tests explored acoustic navigation methods for node localization, cost functions for optimized network routing, and statistics for network traffic analysis. Seaweb 2000 products were implemented in FRONT-3. Overall, Seaweb 2000 made major contributions toward a self-configuring, wireless, undersea acoustic network (Rice 2000).

### **C.     SUBLINK**

The associated Sublink experiments incorporated a submarine as a mobile node in the Seaweb networks. Sublinks '98 and '99 explored acoustic communications with the research submarine *USS Dolphin* (AGSS 555), telesonar test beds, gateway buoys, stationary autonomous bottom nodes, and the *R/V Acoustic Explorer*. These experiments demonstrated two-way communications with a moving submarine utilizing developmental telesonar technology (Rice 2000).

These experiments also measured communications figures of merit as *Dolphin* varied her distance from telesonar test beds, depth, speed, and telesonar modem settings. Onboard the *Dolphin*, a COTS underwater telephone, EDO 5400, was integrated with the organic WQC-2 HF transducers located on the sail, keel, and foredeck. Seaweb acoustic

modem electronics were integrated within the EDO 5400 chassis. The Seaweb operator station was adjacent to the sonar room with a serial connection to the EDO 5400. The Seaweb station included a Seaweb server and a data recorder. This station allowed wireless communications with autonomous network nodes as illustrated in Figure 9 (Rice 2000).

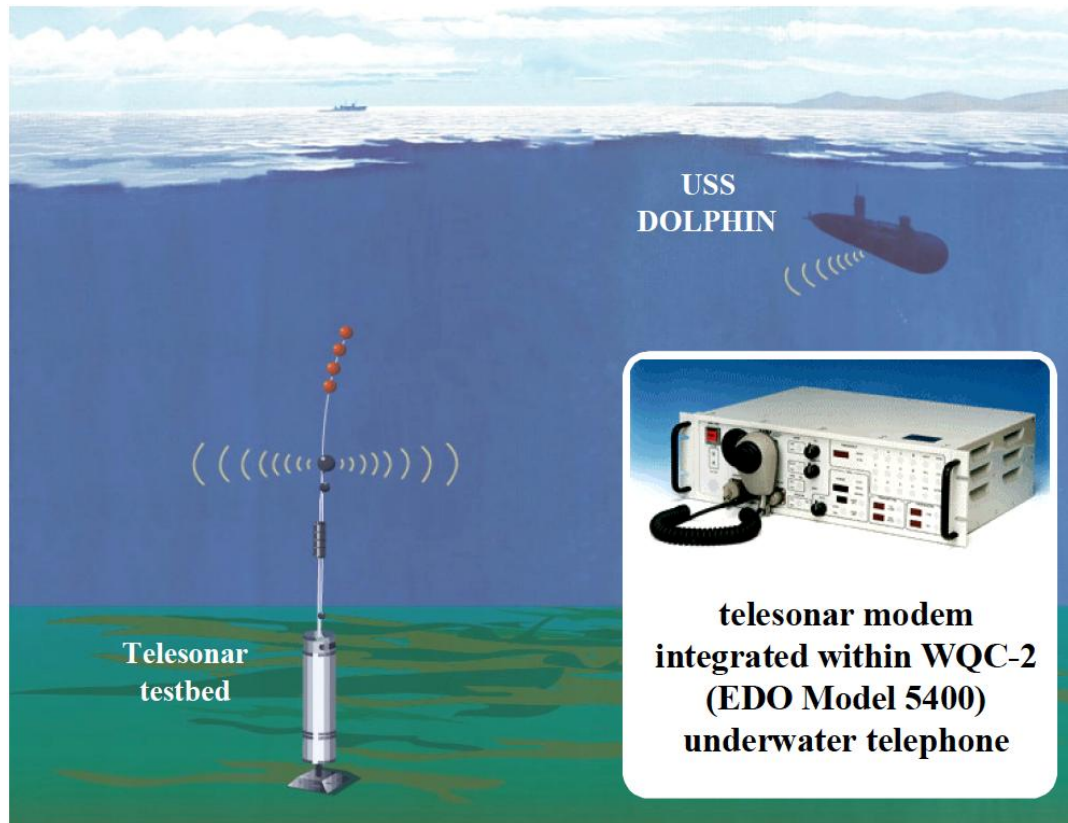


Figure 9. Illustration of the telesonar link between a submerged submarine and an autonomous off board device (From Rice 2000).

Sublinks '98 and '99 were staged on the Loma Shelf, 10 km west-southwest of Pt. Loma, San Diego, in 150 to 250 m water. Both experiments used the ATM875 modem and all acoustic communications were within the 8 to 10.5 kHz band to ensure compatibility with the WQC-2. *Acoustic Explorer* was the afloat command center that supported the telesonar test bed operations. It was moored south of the test beds to monitor *Dolphin's* transmissions using an over-the-side transducer coupled with a deck modem. *Dolphin's* sonar acted as an acoustic gateway while the Seaweb server interfaced with her command center. The server interpreted the outgoing messages and

commands, converted them to ASCII data packets, added the necessary headers and routing information, and directed the transmissions to a destination node. The server also interpreted, time stamped, and logged incoming messages while providing a graphic user interface (Rice 2000).

Sublink 2000 tested acoustic communication among *Dolphin*, seafloor based telesonar test beds, a moored RACOM-3 (radio acoustic communications) gateway buoy, telesonar listening nodes, and nodes hung over the side of the moored *Acoustic Explorer* as illustrated in Figure 10 (Rice 2000).

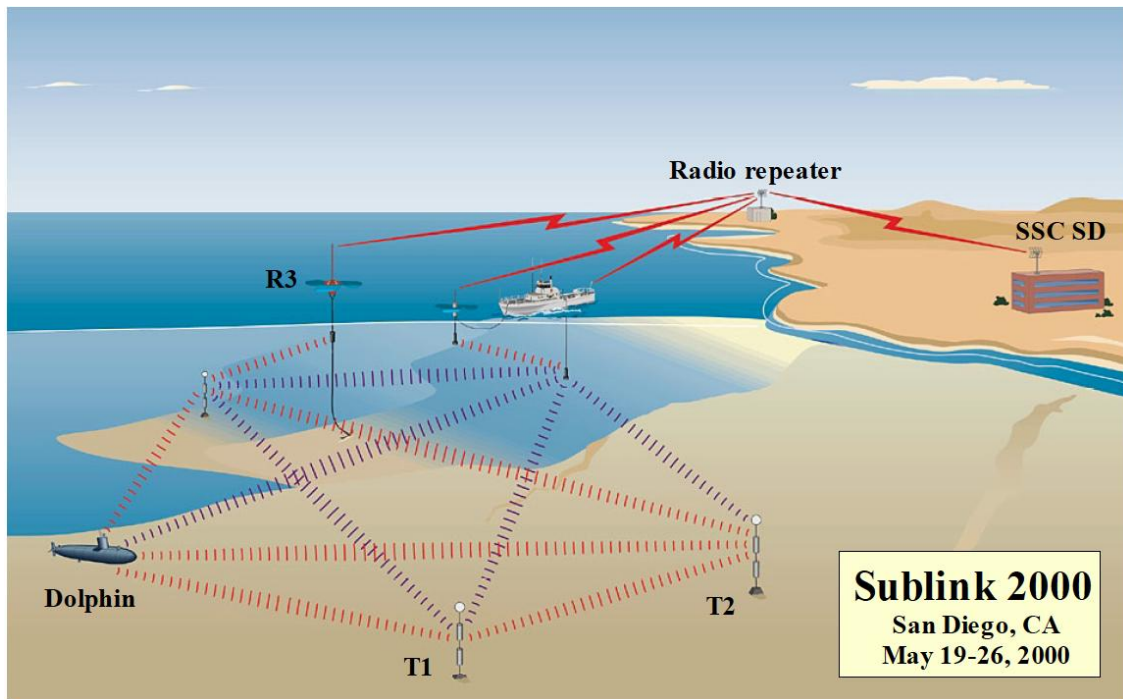


Figure 10. Illustration of the Sublink 2000 setup (From Rice 2000).

A shore-based radio repeater provided internet links for the gateways at the RACOM buoy and the *Acoustic Explorer*. This experiment tested the links between all network node combinations and varied the signaling and channel geometries using the ATM885 telesonar modem (Rice 2000).

Some of the highlights of this experiment are as follows. Aboard *Dolphin*, the ATM885, the EDO 5400, and the WQC-2 were successfully integrated. Telesonar

communications from *Dolphin* to the testbed were established at ranges up to 10 km but the same links from the telesonar testbeds to the *Dolphin* were not as reliable due to relatively lower SNR from lower source levels and higher receiver noise levels. The TDMA signaling schedule was executed flawlessly. SignalEx transmissions were performed using a variety of waveform suites. SignalEx and ATT9 modulation suites were successful between two testbeds with 7 km separation and between testbeds and *Dolphin* at speeds up to 5 knots. Emails from *Dolphin* were delivered to the Office of Naval Research, Submarine Development Squadron Five, and the family of a young sailor while submerged and transiting by utilizing telesonar transmissions, the RACOM gateway buoy, and the Seaweb server (Rice 2000).

In June 2001, during Fleet Battle Experiment – India, a submarine navigated a 14-node Seaweb network with two RACOM buoys on the Loma Shelf near San Diego, CA as illustrated in Figure 11. During this exercise an email was sent from a submerged submarine to an ashore command center (Rice et al. 2001). This particular Seaweb implementation was analyzed by Hartfield in 2003 in his master’s thesis.

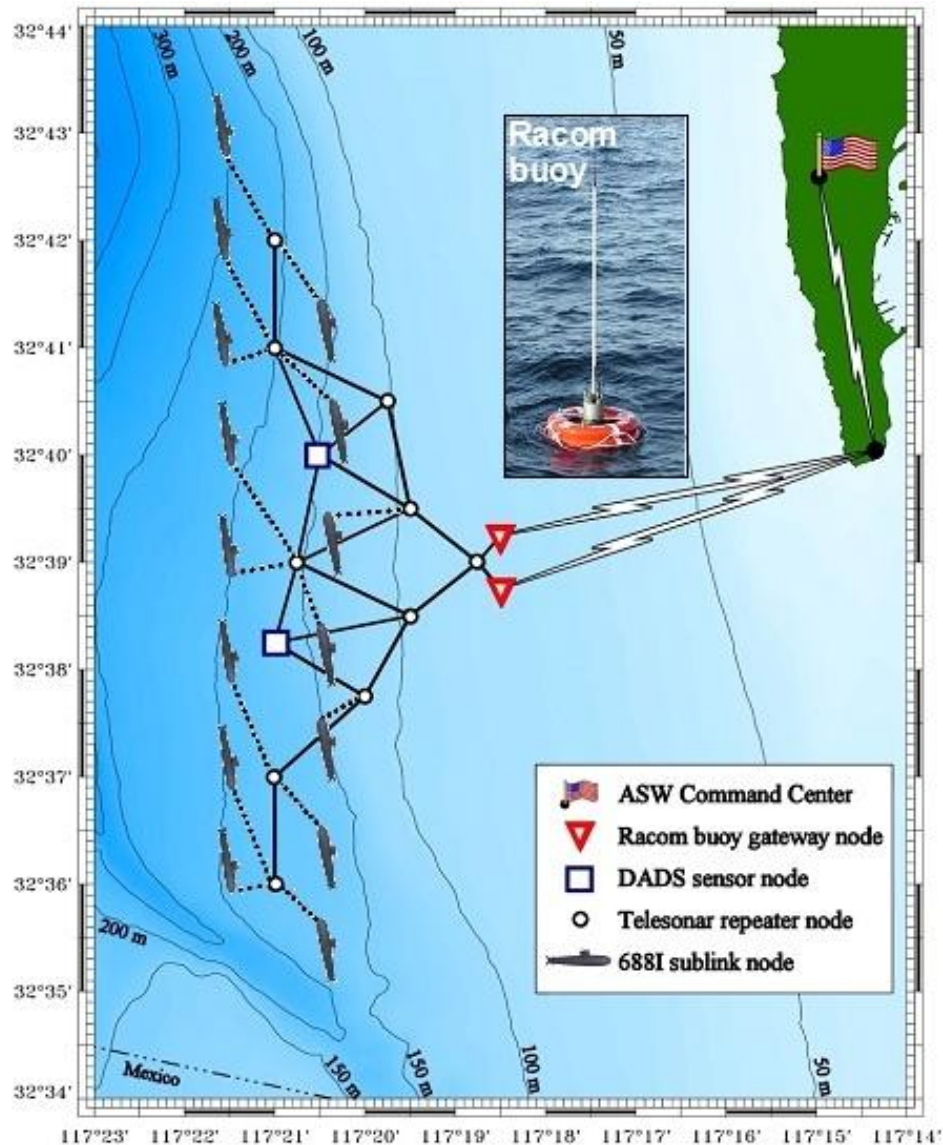


Figure 11. During Fleet Battle Experiment – India in June 2001, a 14-node Seaweb network undersea grid was installed on the Loma Shelf adjacent to San Diego. Mobile positions near the nodes are indicated by the submarine icon (Rice et al. 2001).

In February 2003, Seaweb 2003 was conducted when the Q272 Seaweb network was successfully deployed in an experiment conducted with Defence Research and Development Canada (DRDC) in the Eastern Gulf of Mexico with three Autonomous Underwater Vehicles (AUVs), six repeater nodes, and two gateway nodes as shown in Figure 12. In this experiment, gliders were fitted with telesonar modems and utilized as

mobile nodes. These gliders were manufactured with radio communication equipment, which made them effective mobile gateway nodes without the vulnerability of moored gateway buoys (Bachmeyer et al. 2004).

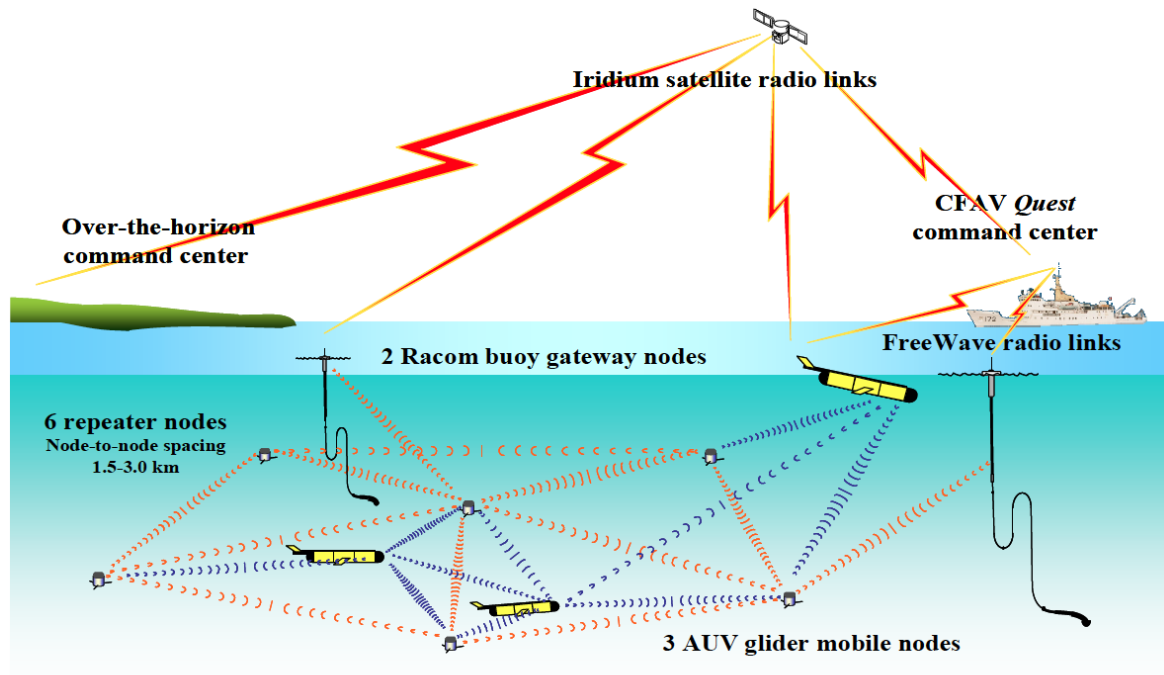


Figure 12. In February, the Seaweb 2003 Q272 Seaweb network in the Eastern Gulf of Mexico included three AUVs, six repeater nodes, and two gateway buoys (From Bachmeyer et al. 2004).

In Seaweb 2004, an experiment with 40 nodes was conducted where the reliability of underwater communications was shown as connectivity was maintained despite two hurricanes and severe trawling (Kriewaldt 2006). The initial location of the nodes is shown on the left and the final location is shown on the right of Figure 13.

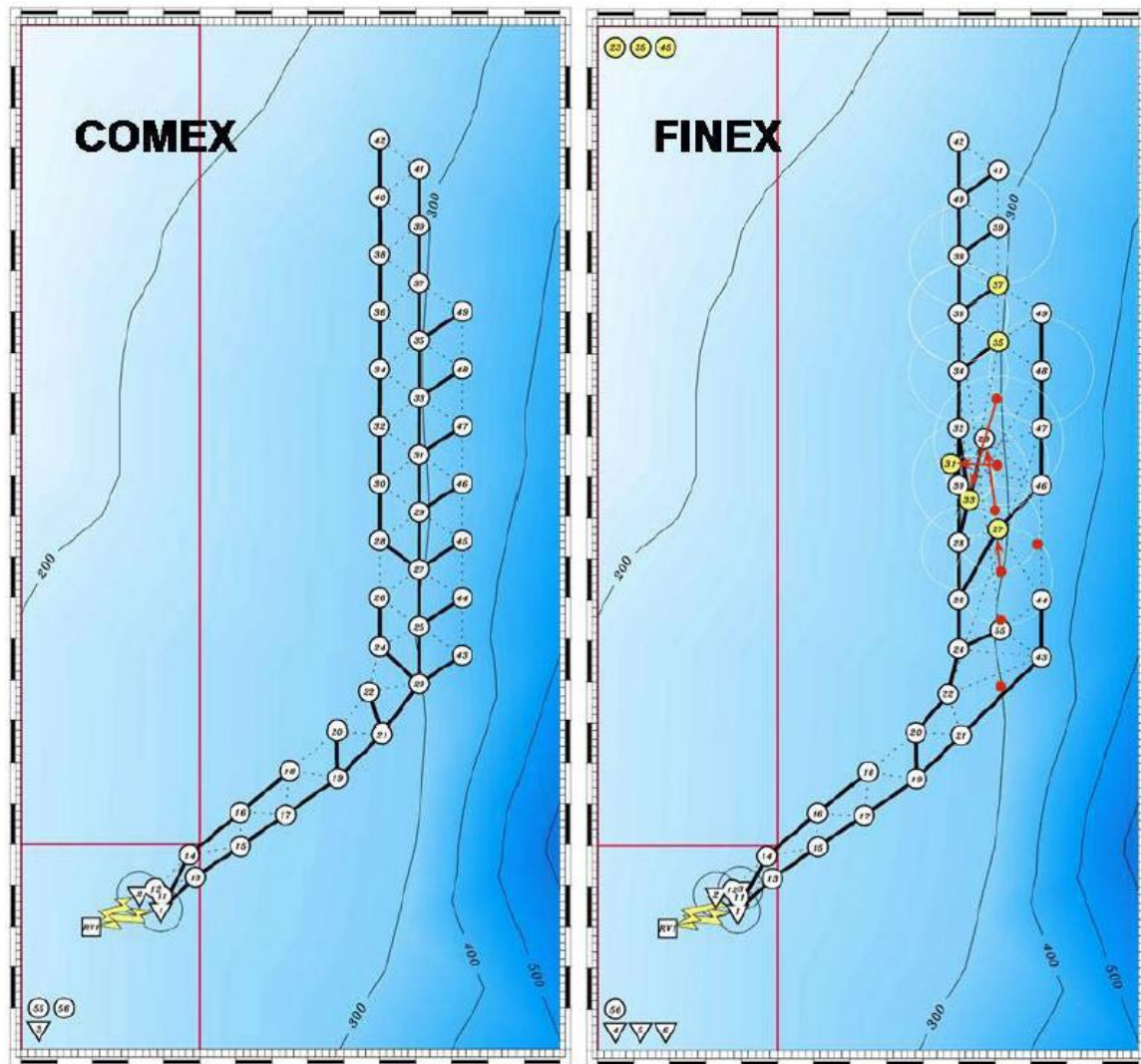


Figure 13. Seaweb 2004 with 40 nodes. Figure on the left shows the planned deployment, while the right hand figure shows the final position following hurricanes and trawling (From Rice and Green 2008).

In May 2005, the node-to-node acoustic ranging capability of Seaweb networked modems as a mechanism for tracking a UUV mobile node relative to a fixed undersea grid was tested in the ARIES Experiment (Acoustic Radio Interactive Exploratory Server) in Monterey Bay shown in Figure 14. When the UUV is submerged, tracking was accomplished by triangulation from the fixed nodes. When surfaced, Seaweb tracking quality was compared to GPS position. This comparison produced reliable results and showed the viability of the Seaweb network (Ouimet, Hahn, and Rice 2005).

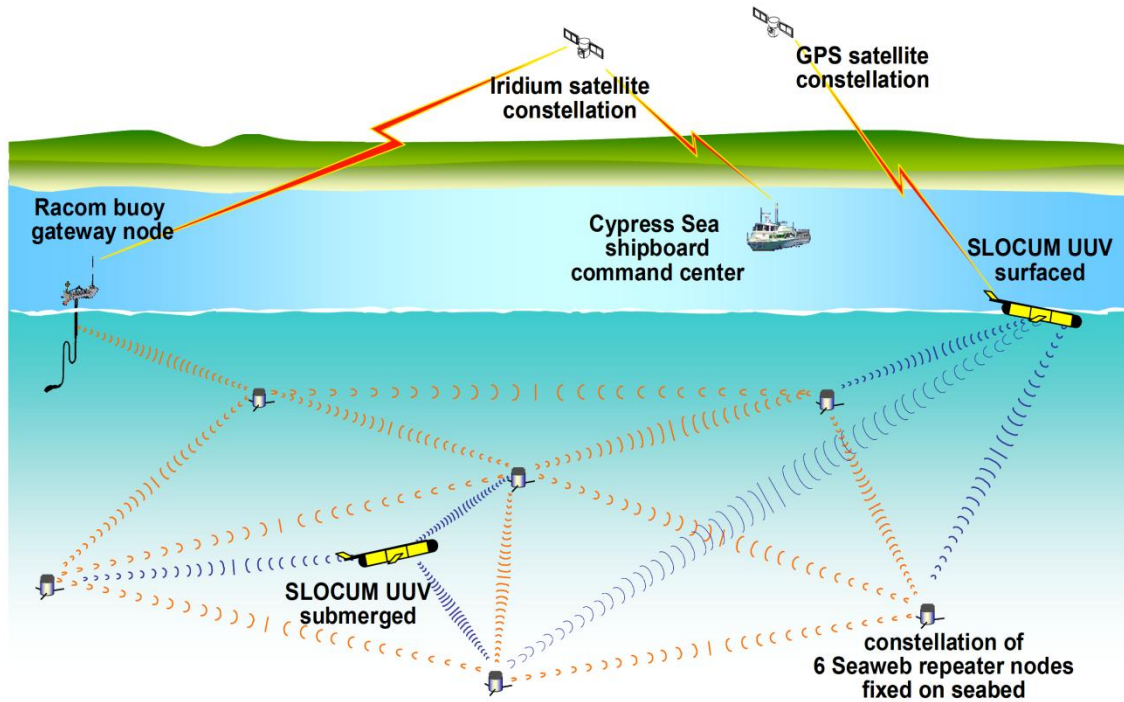


Figure 14. The May 2005 Seaweb ARIES (Acoustic Radio Interactive Exploratory Server) Experiment in Monterey Bay (From Ouimet, Hahn, and Rice 2005).

The general application of the Seaweb infrastructure is well adapted for the use of modem-based navigation aids. This concept allows the use of the acoustic modems to pass to a UUV its geoposition while also providing full connectivity to the outside world. The combination of acoustic communications and modem-based navigation aids is illustrated in Figure 15, which shows a UUV (or a surface ship) simultaneously reacquiring a Smart Marker and being directed by the Directional Acoustic Transponder (DAT) (Green 2007).

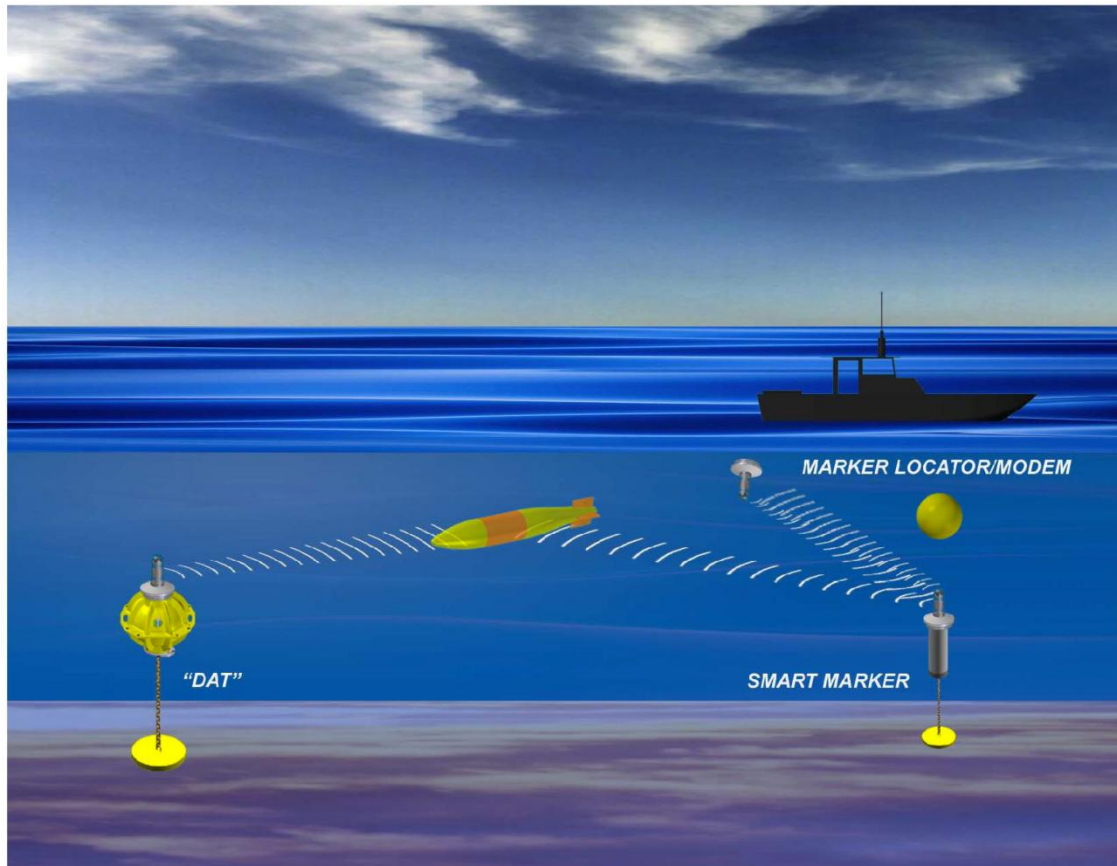


Figure 15. Conceptual operations among a UUV, surface ship, Directional Acoustic Transponder (DAT), and Smart Marker (From Green 2007).

In May 2009, the Seaweb network was implemented in the San Francisco Bay. This pilot experiment demonstrated a practical application of real-time underwater acoustic networks. Despite the difficult environment, the network was successfully deployed and for two weeks was able to gather current and other environmental data that were valuable in understanding the unique environment in the bay. However, the live networking piece of the experiment was not successful and this is where the research in optimally employing these networks is so valuable to allow the full use of the information and advantage that can be gained through these underwater acoustic networks. Figure 16 shows the implementation of San Francisco Bayweb 2009 (Ramp et. al. 2009).

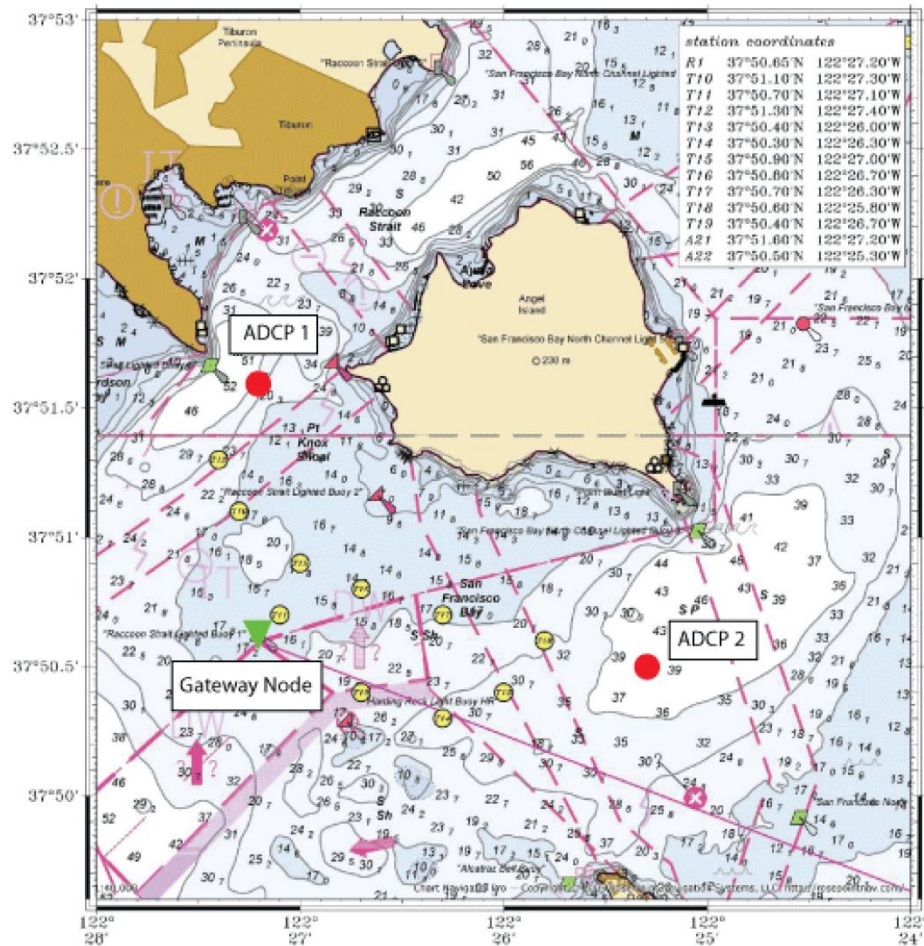


Figure 16. The collaboration of many universities and state and federal agencies came together in the implementation of San Francisco Bayweb in May 2009 (From Ramp et. al. 2009).

The Seaweb network has been successfully deployed in over 50 sea trials. (Ramp et al. 2009) Other implementations include FRONT-3 from March to June 2001, Seaweb 2001, FRONT-4 from January to June 2002, Seaweb 2002, Seaweb 2005 UUV experiments in July 2005 in Monterey Bay and December 2005 in St Andrews Bay, Seaweb 2005, Seaweb 2008, Unet 2006, 2007, 2008, NGAS 2008, 2009, 2010, 2011, 2012, and MISSION 2012 in Singapore Strait.

#### D. DEEP SEAWEB

Seaweb operations can be extended to the deep ocean by exploiting the characteristics of the deep ocean, specifically the Deep Sound Channel (DSC) and

reliable acoustic path (RAP) phenomena. These concepts are explored in detail in Scott Thompson's thesis, "Sound Propagation Considerations for a Deep Ocean Acoustic Network" in December 2009 and are summarized here.

### 1. Reliable Acoustic Path

Of the several paths available, frequently one will be more dominant due to minimum transmission losses (Urick 1983). An example of these dominant paths is known as reliable acoustic path (RAP). This phenomenon is exploited by using the direct path between deep source and shallow receiver, or vice versa. These moderate ranges are achieved because the sound travels over specific paths that are not sensitive to near-surface effects or losses from reflection as in "bottom-bounce" propagation. Example RAPs are shown in Figure 17 (Urick 1983).

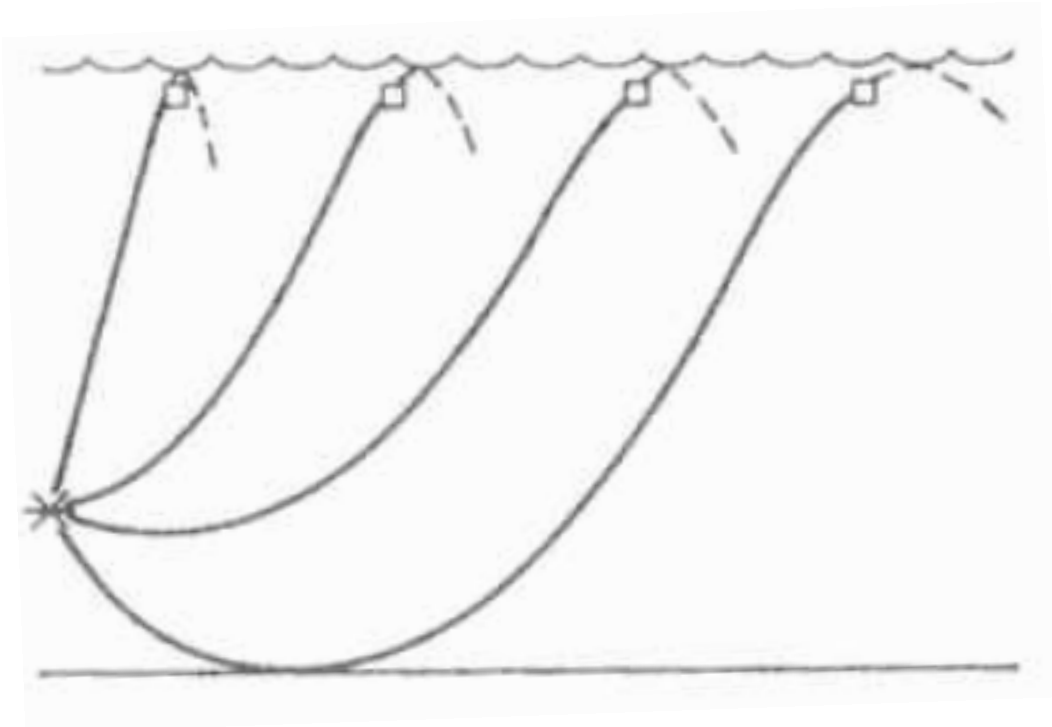


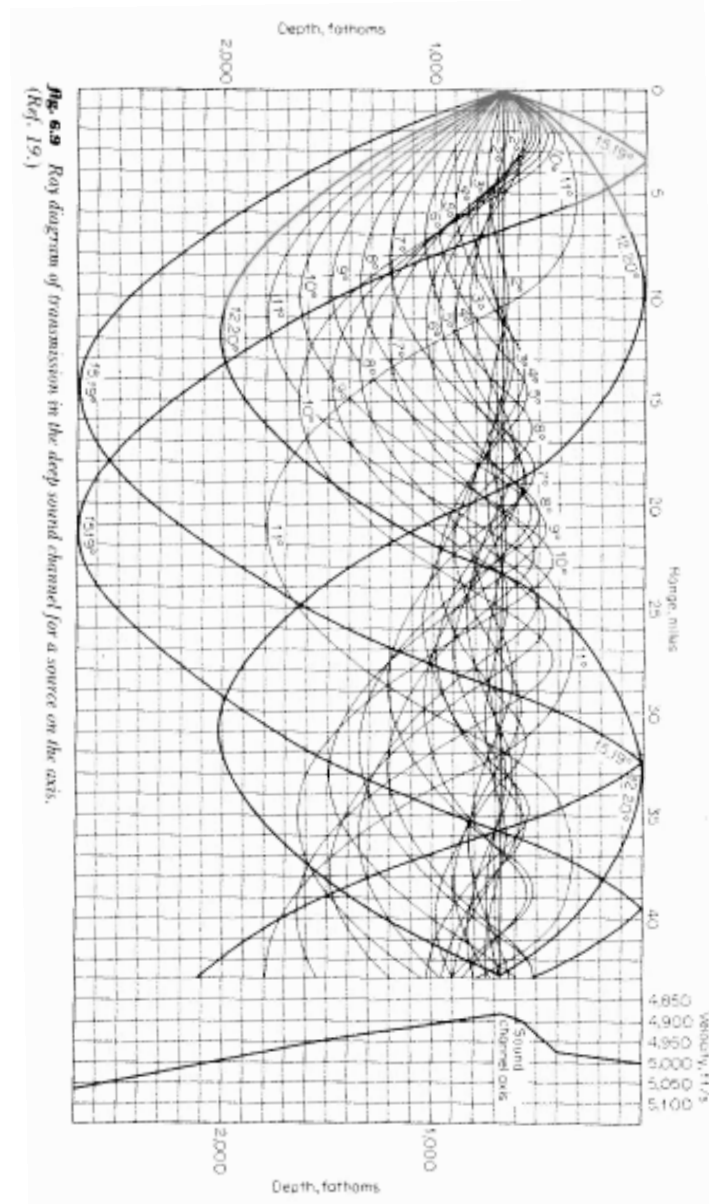
Figure 17. Reliable acoustic paths from a deep source to shallow receivers  
(From Urick 1983).

## **2. Deep Sound Channel**

This phenomenon is the result of the sound-speed profile of the deep ocean. Sound speed is minimum at a specific depth depending largely on the latitude. Refraction focuses the sound waves in the ocean according to Snell's Law, bending them toward the depth of the minimum velocity. When an acoustic source is located at or near the depth of minimum velocity, the sound waves are trapped in the deep sound channel (DSC) and propagate to great distances. The axis of the DSC is the depth at which the minimum velocity occurs (Urick 1983).

Following World War II, Ewing and Worzel explored the characteristics of the DSC. The DSC was utilized in the SOFAR (sound fixing and ranging) system to rescue aviators that went down at sea. The aviator could drop a small explosive charge and the acoustic signal could be received thousands of miles away. Using receipts at two or more stations provided a cross-fix of the location of detonation. Ewing and Worzel published a ray diagram like that in Figure 18 that was originally drawn by hand for a sound source at 4,000 ft that clearly indicates a zone at 32 1/2 miles where the sound waves from several propagation paths converge to produce a convergence zone. These ray traces are now computer created as shown in Figure 19 (Urick 1983).

Because the path that each sound wave travels can vary so much, there is significant distortion of acoustic signals transmitted in the DSC. As an example, an experiment in 1963 using 4-pound explosive sources dropped from an aircraft and detonated at the DSC axis in Bermuda demonstrated how much distortion can be introduced by sound traveling along the DSC. Even though the explosive pulse was initially very short, the received acoustic signal 1,000 miles away was spread to 9.4 seconds. (Urick 1983) Several modulation techniques can handle the multipath propagation: frequency hopping, multi-channel M-ary frequency-shift keyed (MFSK), and M-ary phase-shift-keyed (MPSK) to name a few (Kilfoyle and Baggeroer Jan 2000).



**Fig. 6.9** Ray diagram of transmission in the deep sound channel for a source on the axis.  
(Ref. 19.)

Figure 18. Ray diagram of transmission in the deep sound channel (DSC) for a source on the axis (From Urick 1983).

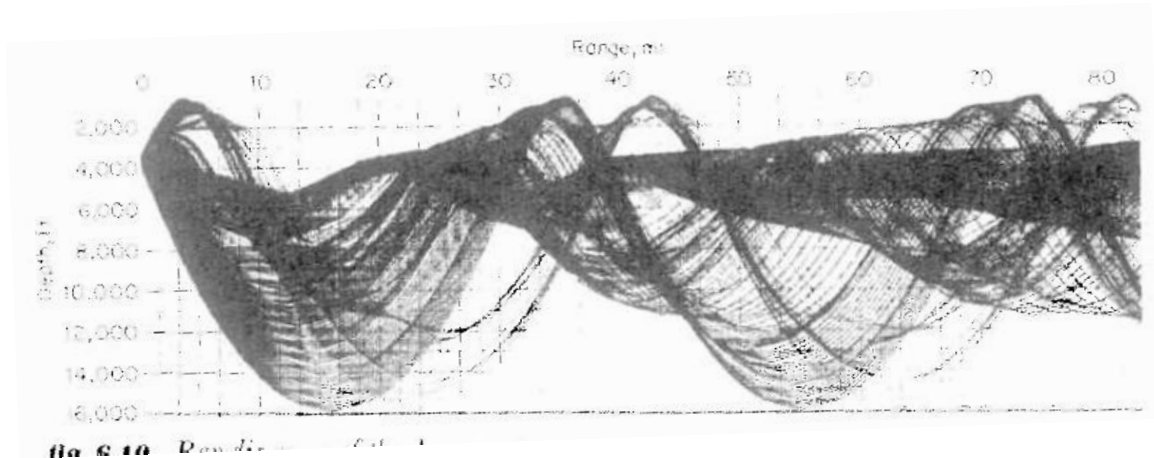


Figure 19. Computer generated ray diagram of the DSC for a source near the axis.  
Reflected rays are omitted (From Urick 1983).

Another advantage of utilizing the DSC is its nearly global availability as shown in Figure 20, a worldwide map showing DSC axis depths. The DSC axis is around 1000 meters deep (3,280 feet) in the midlatitudes but can be very near the surface near polar regions (Munk and Forbes 1989).

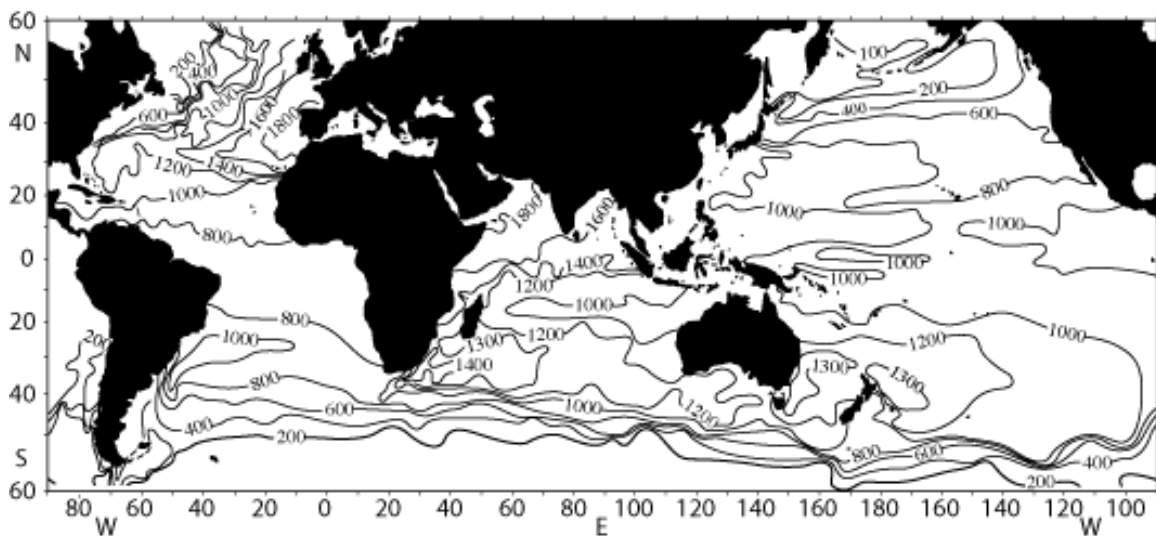


Figure 20. Worldwide DSC axis depths in meters (From Munk and Forbes 1989).

### 3. Deep Seaweb Concept

The Deep Seaweb concept is similar to that of Seaweb but it exploits the DSC as shown in Figure 21 to provide longer links and greater area coverage.

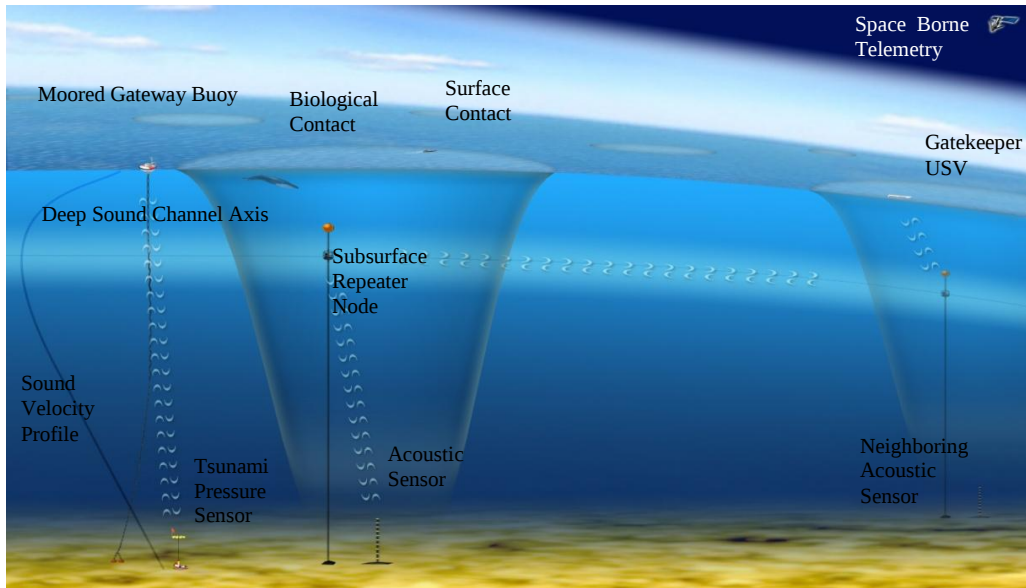


Figure 21. Deep Seaweb concept illustration (From Rice unpublished Deep Seaweb presentation).

The DSC is deep enough to avoid being a hazard to navigation. The DSC can also provide fairly stealthy channels of communication between submerged, surface, and air assets. It is possible for submarines to participate in the communication network with messaging over long distances and connections to command centers via a gateway node at a more secure or more remote location.

The gateway node could be an unmanned surface vehicle (USV), a moored surface or subsurface buoy that is linked to an airborne asset via lasers or radio frequency, a cabled seafloor modem, or a manned surface vessel. Paul Blodgett analyzed the use of lasers to communicate with submarines in his thesis, “Submarine Laser Communication Options and the Impact of Light Refraction at the Air-Sea Interface” in September 2009. Lasers could be used to communicate with a subsurface gateway node

in a distributed undersea Seaweb infrastructure instead of linking directly with the submarine.

There are several factors that need to be considered when exploring the use of a moored gateway buoy. One important factor is the effect of ocean currents on the long tether that anchors the acoustic modem and transducer to the sea floor. Scott Thompson explored this aspect in detail in his thesis “Displacement of tethered hydro-acoustic modems by uniform horizontal currents” in December 2009.

Another important factor to consider is longevity since these buoys are battery powered. There are several options that could increase the operational time buoys and acoustic modems are able to remain in service. There have been great advances in developing regimens to conserve battery power by utilizing low power states and more efficient electronic components that have greatly increased the service life. To compliment these advances, there are several options that could be used to recharge the batteries on station rather than replace them, which would be very expensive in time and resources for modems and buoys deployed in the deep ocean. One option is to utilize a microbial fuel cell. On April 22, 2010, for an Earth Day event at the Pentagon, the Office of Naval Research (ONR) showcased such a microbial fuel cell that converts “naturally occurring fuels and oxidants in the marine environment into electricity, offering a clean, efficient and reliable alternative to batteries and other environmentally harmful fuels” (Office of Naval Research 2010). ONR Program Manager Dr. Linda Chrisey made the following observations:

Think of it as a battery that runs on mud. They are sustainable, environmentally friendly and don't involve hazardous reactants like a regular battery might because they use the natural carbon in the marine environment. For example, we are working on a 4-foot long autonomous underwater vehicle that will settle on the seafloor and recharge its batteries using this fuel cell approach. We are already able to power many types of sensors using microbial fuel cells. (Office of Naval Research 2010)

Another option is to have a solar panel with a buoyancy controlled feature that would allow periodic recharging. It is also possible to harness the energy available in the ocean currents to run a small generator for recharging. While each of these options has

its advantages, the microbial fuel cell seems to be very promising and it was named as one of TIME magazine's "Top 50 Inventions for 2009" (Office of Naval Research 2010).

The standard Deep Seaweb acoustic modems are the same as those used for Seaweb, commercially available Teledyne Benthos acoustic modems that operate in the 9-14 kHz band. Although the ocean floor depth is around 8,000 meters (26,246 feet) in some places, 4,000 meters (13,123 feet) is a typical ocean depth as shown in Figure 22 (Amante and Eakins 2009). Using a typical DSC axis depth of 1,000 meters (3,280 feet), the cable that anchors the transducer and acoustic modem will be approximately 3,000 meter (9,842 feet) long. The acoustic modem setup that Thompson analyzed in detail in both theses is shown in Figure 23.

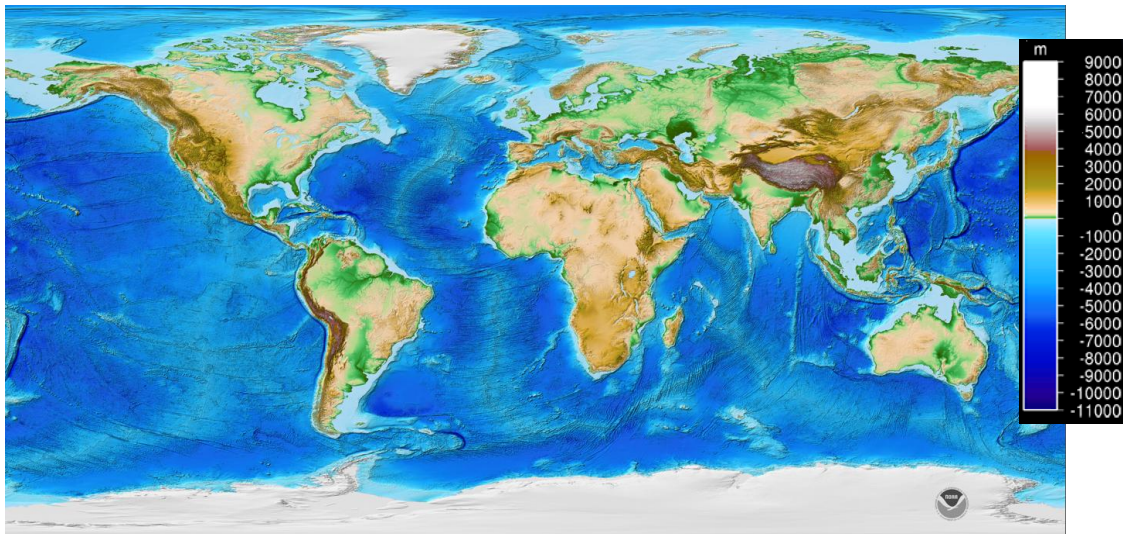


Figure 22. Worldwide ocean depths in meters (From Amante and Eakins 2009).

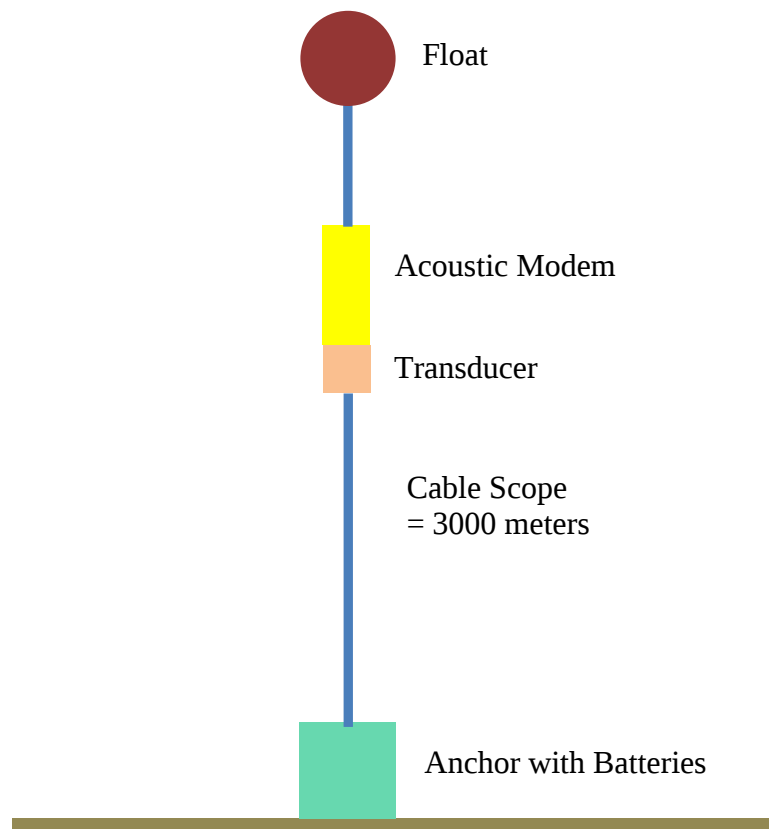


Figure 23. Acoustic modem composition used for Thompson's DSC analysis (From Thompson 2010).

THIS PAGE INTENTIONALLY LEFT BLANK

### III. NETWORK MODEL FORMULATION

#### A. DESIGNING A RESILIENT NETWORK

##### 1. Network Setup

The wireless Seaweb underwater network can be set up in any geometric arrangement, as indicated in the various applications mentioned in chapter II. In order to create a finite representation that can be optimized, we decided to use a small square area measuring 75 km x 75 km (40.5 nm x 40.5 nm) in a generic patch of ocean that has a typical sound velocity profile. We divide the area into a 5km x 5km (2.7nm x 2.7nm) grid, placing an acoustic modem only at a *node*, defined as the center of one of the 225 square patches defined by the grid. Each grid square diagonal is 7.07 km (3.8 nm). The number of gateway nodes and access point nodes in any scenario is fixed and each is placed at a predetermined location. A fixed number of repeater nodes are available for placement at other, unoccupied nodes. Each acoustic modem has a maximum effective range of about 25 km, (13.5 nm); if two modems are placed within range of each other a connection can be established between them, and we represent this possibility as an *arc* between two nodes whose Euclidean distance is less than or equal to the maximum effective range.

We also assume that each node in the network is a potential *attack* location, at which an adversary can detonate ordnance (e.g., a depth charge). We assume that the detonation corresponding to such an attack will damage nearby modems and render them unusable. Any damage radius can be used; for the purposes of our study, we assume that an attack at any node disables modems placed at any of the eight adjacent (orthogonally and diagonally) nodes.

The goal of our model is to determine locations for repeaters so that each access point is connected to at least one gateway node through a sequence of modems within range of each other. We do this by establishing a unit of communications traffic at each access point, and having the model place repeaters at nodes to minimize the number of undeliverable units of traffic, where traffic will be routed along arcs that connect nodes occupied by repeaters.

This network design must consider a set of possible attacks by a rational, malicious adversary, the *attacker*, who chooses a set of nodes to attack and whose goal is the exact opposite of that of the network designer, who we call the *defender*: to maximize the costs (including penalties) of delivering messages from each of the access points to any gateway node. We define the set of feasible attacks for the attacker through a simple budget constraint limiting the number of nodes he can attack. However, this can be generalized to any set of constraints we wish to place on the attacker's operations, based on our estimation of his capability to launch simultaneous attacks against our network.

We present the following monolithic tri-level optimization problem, which we refer to as a *defender-attacker-defender (DAD)* model, for optimizing the design of a communications network that is resilient to attack. Although such problems cannot be solved directly, we develop a decomposition algorithm and several related problem formulations that we use to determine optimal solutions to this problem.

## 2. Sets and Indices

$i \in N$  potential sites for relays (alias  $j$ ) or attacks (alias  $i', j'$ ) or source nodes (alias  $k$ )

$(i, j) \in A$  potential communication arcs; pairs of sites that are within range of each other {alias  $(j, i)$ }

$S \subset N$  access points (source nodes) for messages

$T \subset N \setminus S$  gateway (exit) nodes for the network

$V_i \subset N$  set of nodes that affect node  $i$  when attacked

## 3. Data

$q$  penalty for each undelivered packet

$p$  penalty on each packet sent across an attacked arc

$max\_repeaters$  maximum number of repeaters to emplace (including access points and gateways)

$max\_attacks$  maximum number of attacks

#### 4. Variables [type]

$E_k$  undelivered messages remaining at any source node  $k$  [nonnegative]

$X_{i'}$  1 if node  $i'$  is attacked. [binary]

$Y_{ij}^k$  messages originating from source node  $k$  sent across  $(i,j)$  [nonnegative]

$F_i^k$  messages from a source node  $k$  undelivered to any gateway node  $t$  [nonnegative]

$R_i$  1 if modem emplaced at node  $i$ , includes access points, gateway nodes, and relay nodes [binary]

#### 5. Formulation SUBNET\_DAD:

$$\min_R \max_X \min_{Y,E,F} \sum_{k \in S} qE_k + \sum_{(i,j) \in A} (1 + \sum_{i' \in V_i} pX_{i'} + \sum_{j' \in V_j} pX_{j'}) \sum_{k \in S} Y_{ij}^k \quad (T1)$$

$$\text{s.t.} \quad \sum_{j:(i,j) \in A} Y_{ij}^k - \sum_{j:(j,i) \in A} Y_{ij}^k = \begin{cases} 1 - E_k & i = k \\ 0 & i \in (N - k) \setminus T \quad \forall i \in N, k \in S \\ -F_i^k & i \in T \end{cases} \quad (T2)$$

$$\sum_{j:(i,j) \in A} Y_{ij}^k \leq R_i \quad \forall i \in N \setminus (S \cup T), k \in S \quad (T3)$$

$$\sum_{i \in N} R_i \leq max\_repeaters \quad (T4)$$

$$\sum_{i' \in N} X_{i'} \leq max\_attacks \quad (T5)$$

$$Y_{ij}^k \geq 0 \quad \forall (i,j) \in A, k \in S \quad (T6)$$

$$X_{i'} \in \{0,1\} \quad \forall i' \in N \quad (T7)$$

$$R_i \in \{0,1\} \quad \forall i \in N \quad (T8)$$

#### 6. Discussion

The objective function (T1) assesses a penalty of  $q$  units per undelivered message from each source node and calculates the total number of hops taken by the delivered messages to get to their destination; it also includes a penalty of  $p$  units for each attacked

arc traversed by a message. Constraints (T2) maintain balance of flow at each node  $i$  for each individual message tagged by its source node,  $k$ . There is one constraint (T3) for every pair of  $k$  and  $R_i$  that requires a repeater be placed at the (non-source, non-gateway) tail node of any arc that transmits messages; in practice the  $R$  variables are fixed for source and gateway nodes, so the corresponding control constraints are not required in any of the formulations. Constraints (T4) and (T5) place a ceiling on the total number of repeater nodes and max number of attacks, respectively. Constraint (T6) establishes each individual message flow as a nonnegative variable. Constraints (T7) and (T8) establish each  $X_{i,j}$  and  $R_i$  as a binary variable.

For an actual laydown in a known geographic area, nodes can be located anywhere in that area and a sound propagation model can be run for each pair of nodes to determine connectivity: if modems placed at two nodes could establish a viable communications channel, then the arc between these two points is added to the set  $A$ . In our simple grid example, the set  $A$  of potential communication arcs is calculated using a constant, *sidelen*, that determines the distance between adjacent cells, in nm, and a constant, *maxdist*, that gives the maximum range in nm between repeaters that communicate with each other. The propagation model provides the basis for that maximum range.

In a scenario with multiple gateway nodes, we connect each gateway node to one “central gateway node” with zero cost, invulnerable arcs (i.e., for such an arc  $(i,j)$ , both  $V_i$  and  $V_j$  are empty) so even though the actual gateway nodes will be modeled  $t \in T \subseteq N$ , the code incorporates the “central gateway node” as  $t \in N$ . This allows a message originating at an access node to exit the system at any one of the gateway nodes.

## B. SOLVING SUBNET\_DAD WITH DECOMPOSITION

In order to solve SUBNET\_DAD, we propose a decomposition algorithm in which the subproblem solves for the optimal attack against any fixed network design, and the master problem builds a design that is resilient to each attack seen so far. We first formulate the attacker subproblem, which is simply SUBNET\_DAD with the design variables,  $R$ , fixed, and is therefore a two-level optimization problem we refer to as an

*attacker-defender (AD)* model. In this model, we define a fixed design through a new set of parameters representing a fixed design, use those parameters in place of the  $R$  variables, modify the objective (T1) and constraints (T3), and drop constraints (T4) and (T8):

### 1. New Data

$\bar{R}_i$       1 if modem emplaced at node  $i$ , 0 otherwise (a fixed design) [binary]

### 2. Formulation SUBNET\_AD:

$$\max_X \min_{Y, E, F} \sum_{k \in S} qE_k + \sum_{(i,j) \in A} (1 + \sum_{i' \in V_i} pX_{i'} + \sum_{j' \in V_j} pX_{j'}) \sum_{k \in S} Y_{ij}^k \quad (T1')$$

$$\text{s.t.} \quad \sum_{j:(i,j) \in A} Y_{ij}^k - \sum_{j:(j,i) \in A} Y_{ij}^k = \begin{cases} 1 - E_k & i = k \\ 0 & i \in (N - k) \setminus T \quad \forall i \in N, k \in S \\ -F_i^k & i \in T \end{cases} \quad (T2)$$

$$\sum_{j:(i,j) \in A} Y_{ij}^k \leq \bar{R}_i \quad \forall i \in N \setminus (S \cup T), k \in S \quad (T3')$$

$$\sum_{i' \in N} X_{i'} \leq \max\_attacks \quad (T5)$$

$$Y_{ij}^k \geq 0 \quad \forall (i, j) \in A, k \in S \quad (T6)$$

$$X_{i'} \in \{0, 1\} \quad \forall i' \in N \quad (T7)$$

### 3. Discussion

This formulation still cannot be solved directly, but a simple, standard reformulation converts it to an integer programming problem. For fixed values of both the  $R$  and  $X$  variables, the resulting optimization problem is an amalgamation of several minimum-cost network flow problems, one per source node, that models the routing (or non-routing, as appropriate) of each message through the existing, attacked network. In this case constraints (T2), (T3'), and (T6) define the feasible region for the operator's flow problem. For a fixed design,  $\bar{R}$ , and a fixed attack plan,  $\bar{X}$ , the network operator faces the following message routing problem:

#### 4. New Data

$\bar{X}_i$ , 1 if node  $i$  ' attacked, 0 otherwise (a fixed attack plan) [binary]

#### 5. Formulation SUBNET\_ROUTING:

$$\min_{Y,E,F} \sum_{k \in S} qE_k + \sum_{(i,j) \in A} (1 + \sum_{i' \in V_i} p\bar{X}_{i'} + \sum_{j' \in V_j} p\bar{X}_{j'}) \sum_{k \in S} Y_{ij}^k \quad (\text{T1"})$$

$$\text{s.t.} \quad \sum_{j:(i,j) \in A} Y_{ij}^k - \sum_{j:(j,i) \in A} Y_{ij}^k = \begin{cases} 1 - E_k & i = k \\ 0 & i \in (N - k) \setminus T \quad \forall i \in N, k \in S \quad [\pi_{ik}] \\ -F_i^k & i \in T \end{cases} \quad (\text{T2})$$

$$\sum_{j:(i,j) \in A} Y_{ij}^k \leq \bar{R}_i \quad \forall i \in N \setminus (S \cup T), k \in S \quad [\mu_{ik}] \quad (\text{T3'})$$

$$Y_{ij}^k \geq 0 \quad \forall (i,j) \in A, k \in S \quad (\text{T6})$$

#### 6. Discussion

This is a linear programming problem, and we have indicated dual variable names for each constraint. The objective (T1'') is now a pure minimization in the flow and artificial variables. We have dropped constraints (T5) and (T7), as the attack is fixed, and the rest of the model is the same as before.

We are now in a position to take the dual of this routing formulation, and then replace the attack parameters with decision variables to yield a pure maximization integer programming problem:

## 7. Formulation SUBNET\_AD\_DUALILP:

$$\max_{X, \pi, \mu} \sum_{k \in S} \pi_{kk} - \sum_{\substack{i \in N \\ k \in S}} \bar{R}_i \mu_{ik} \quad (D1)$$

$$\text{s.t.} \quad \pi_{ik} - \pi_{jk} - \mu_{ik} - \sum_{i' \in V_i} pX_{i'} - \sum_{j' \in V_j} pX_{j'} \leq 1 \quad \forall (i, j) \in A, k \in S \quad (D2)$$

$$\pi_{kk} - \mu_{kk} \leq q \quad \forall k \in S \quad (D3)$$

$$\pi_{ik} - \mu_{ik} \leq 0 \quad \forall i \in T, k \in S \quad (D4)$$

$$\sum_{i' \in N} X_{i'} \leq \max\_attacks \quad (D5)$$

$$X_{i'} \in \{0, 1\} \quad \forall i' \in N \quad (D6)$$

$$\mu_{ik} \geq 0 \quad \forall i \in N, k \in S \quad (D7)$$

## 8. Discussion

The DAD objective function takes the input from the objective function for the Operator Model then provides input to the solution to cut  $d$  of the DAD Model (D1) provides optimum solution of the DAD Model. Constraint (D2) maintains balance of flow at each node, where each access point,  $s$ , has one unit of supply, and must connect to at least one gateway node,  $t$ . Constraints (D3) and (D4) require that repeaters be placed at both endpoints of any arc that is used for communication. Constraint (D5) places a ceiling on maximum number of attacks. Constraints (D6) establish each  $X_{i'}$  as a binary variable. Constraints (D7) establish each  $\mu_{ik}$  as a nonnegative variable.

For any fixed design, this model can be solved with commercial, off-the-shelf optimization software such as GAMS (General Algebraic Modeling System) (GAMS, 2013) and CPLEX Optimizer (IBM, 2013). SUBNET\_AD\_DUALILP serves as the subproblem for our decomposition algorithm, and with it in place, we now provide the master problem formulation.

## C. MASTER PROBLEM FORMULATION

Our master problem includes design decision variables,  $R$ , from the original formulation, and keeps track of the attack found by the subproblem at each iteration,  $d$ .

For each of these attacks, it maintains a separate set of flow and artificial variables, indexed by the iteration, so that it can determine the optimal routing response to each attack. It is a network design problem in which the design chosen is evaluated against each of a finite set of attacks, and therefore determines the design that is resilient to the worst-case attack out of all the attacks it has seen so far.

### 1. Sets and Indices

$d$  iteration index for DAD model

### 2. Data

$\bar{X}_i^d$  1 if node  $i$  ' attacked in iteration  $d$ , 0 otherwise

$D$  number of iterations

### 3. Variables [type]

$Z_{DAD}$  DAD master problem objective function value [free]

$ED_k^d$  undelivered messages remaining at any access point node  $s$  in response to attack from iteration  $d$  [nonnegative]

$YD_{ij}^{kd}$  messages sent across  $(i,j)$  in response to attack from iteration  $d$  [nonnegative]

$FD_i^d$  messages undelivered to any gateway node  $i$  in response to attack from iteration  $d$  [nonnegative]

#### 4. Model Formulation

$$\min_{R, YD, ED, FD} Z_{DAD} \quad (M0)$$

$$Z_{DAD} \geq \sum_{k \in S} \left( qED_k^d + \sum_{(i,j) \in A} \left( 1 + \sum_{i' \in V_i} p\bar{X}_{i'}^d + \sum_{j' \in V_j} p\bar{X}_{j'}^d \right) YD_{ij}^{kd} \right) \quad \forall d \leq D \quad (M1)$$

$$\sum_{j: (i,j) \in A} YD_{ij}^{kd} - \sum_{j: (j,i) \in A} YD_{ji}^{kd} = \begin{cases} 1 - ED_k^d & i = k \\ 0 & i \in (N - k) \setminus T \\ -FD_i^{kd} & i \in T \end{cases} \quad \forall i \in N, k \in S, d \leq D \quad (M2)$$

$$\sum_{j: (i,j) \in A} YD_{ij}^{kd} \leq R_j \quad \forall i \in N \setminus (S \cup T), k \in S, d \leq D \quad (M3)$$

$$\sum_{i \in N} R_i \leq \text{max\_repeaters} \quad (M4)$$

$$YD_{ij}^{kd} \geq 0 \quad \forall (i, j) \in A, k \in S, d \leq D \quad (M6)$$

$$R_i \in \{0, 1\} \quad \forall i \in N \quad (M8)$$

#### 5. Discussion

The DAD master problem objective (M0) represents the operating cost resulting from the worst-case attack. Each cut constraint (M1) provides a lower bound on the worst-case cost based on a particular attack plan,  $\bar{X}^d$ , and the associated flows  $YD^{kd}$  representing the operator's optimal re-routing of that message in response to that attack plan. Constraints (M2) enforce balance of flow for each node and each message, for each attack plan. Constraints (M3) require a repeater node be established at the tail node of any arc that carries flow, for each attack plan. Constraint (M4) limits the total number of repeaters used in the network design. Constraints (M6) establish each  $YD_{ij}^{kd}$  as a nonnegative variable. Constraints (M8) establish each  $R_i$  as a binary variable.

When solving SUBNET\_DAD using Benders decomposition, we can encounter a repeated attack from the subproblem (since the subproblem itself is an integer linear program, the optimal attack in response to a given suboptimal defense might be one we've seen before), which immediately leads to cycling and a failure to converge. To prevent this, we create a version of the SUBNET\_DUALILP subproblem with an additional set of constraints:

$$\sum_{(i',d) \in \bar{X}_i^d} X_{i'} \leq \max\_attacks - 1 \quad (\text{D8})$$

These constraints use the iteration index,  $d$ , defined in the master problem, and, when solving the subproblem at iteration  $D$ , they make use of the stored attack plans  $\bar{X}_i^d$  from the previous iterations,  $1 \leq d < D$ . The constraints (D8) require that the current attack *not* target at least one node that was targeted in each of the prior attacks. We refer to this version as SUBNET\_DUALILP\_UNIQUE.

#### D. ALGORITHM

Using the models just described, the following algorithm solves for the optimal placement of repeaters at nodes, and, as a by-product, an optimal attack for that specific network configuration.

##### 1. Variables used in the algorithm not previously defined [type]

|                 |                                                    |
|-----------------|----------------------------------------------------|
| $R_i^{best}$    | incumbent defense                                  |
| $\bar{R}$       | current defense to use in the AD subproblem        |
| $X_{i'}^{best}$ | attack corresponding to the incumbent defense      |
| $ub\_DAD$       | upper bound for DAD model [nonnegative]            |
| $lb\_DAD$       | lower bound for DAD model [nonnegative]            |
| $epsilon\_DAD$  | relative tolerance for the DAD model [nonnegative] |

##### 2. Algorithm SUBNET\_DECOMP

Solve SUBNET\_DESIGN for  $R, Y, E, F, Z_{DAD}$

$lb\_DAD = Z_{DAD}$

$ub\_DAD = +\infty$

$\bar{R} = R, R^{best} = \bar{R}, X^{best} = \mathbf{0}$

$D = 1$

While  $ub\_DAD - lb\_DAD > epsilon\_DAD * lb\_DAD$

Solve SUBNET\_DUALILP for  $X, \pi, \mu, Z_{AD}$

If  $ub\_DAD > Z_{AD}$   
     Update  $ub\_DAD = Z_{AD}$   
     Update incumbent defense,  $R^{best} = \bar{R}$   
     Record attack corresponding to incumbent defense,  $X_i^{best}$   
 If not first iteration (i.e.,  $D > 1$ )  
     Compare  $X$  to each  $X^d, 1 \leq d < D$   
     If  $X = X^d$  for some  $d$   
         Solve SUBNET\_DUALILP\_UNIQUE for  $X, \pi, \mu, Z_{AD}$   
     Record next (unique) attack:  $X^D = X$   
     Solve SUBNET\_DAD\_MASTER for  $R, YD, ED, FD, Z_{DAD}$   
     If  $lb\_DAD < Z_{DAD}$   
         Update  $lb\_DAD = Z_{DAD}$   
     Update current design  $\bar{R} = R$   
      $D = D + 1$   
 Solve SUBNET\_ROUTING (with  $R = R^{best}, X = X^{best}$ ) to recover  $Y, E, F$

### 3. Discussion

Algorithm SUBNET\_DECOMP uses the standard structure of Benders decomposition with a modified subproblem (here, SUBNET\_DUALILP\_UNIQUE) that guarantees a unique, if suboptimal, attack plan, given a list of prior attack plans previously enumerated. Although this modified subproblem does not generate valid bounds (and therefore cannot be used to update the incumbent), it does guarantee that every possible attack plan that uses all available attacks will eventually be enumerated. If the subproblem becomes infeasible due to these constraints, then we must have enumerated all possible attacks and therefore the incumbent solution is optimal. Each suboptimal attack generates a valid cut for the master problem, and will eventually provide enough guidance (possibly through an exhaustive enumeration of all possible cuts) to converge.

THIS PAGE INTENTIONALLY LEFT BLANK

## IV. RESULTS, CONCLUSIONS, AND FUTURE WORK

### A. RESULTS

This analysis is based on the small 15 by 15 node network with the access point nodes,  $s$ , and the gateway nodes,  $t$ , in predetermined locations as mentioned in chapter III. The location of the repeater nodes,  $r$ , are determined by initially solving the network design problem. This network is indexed by row and column and numbered from left to right and top to bottom. To further examine the effect of access point and gateway node placement, four configurations, A through D, were used. The location of each node will be referenced by row and column in this format (row, column). For instance, a node in row 5, column 10 will be written as (5, 10).

For this 15 by 15 network, the numerical values used in the GAMS code are summarized in Table 1.

Table 1. Numerical values for data used in the GAMS code.

| Data Term        | Definition                                                                    | Value for this 15 by 15 network |
|------------------|-------------------------------------------------------------------------------|---------------------------------|
| $q$              | penalty for each undelivered packet                                           | 12                              |
| $p$              | penalty on each packet sent across an attacked arc                            | 13                              |
| $max\_repeaters$ | maximum number of repeaters to emplace (including access points and gateways) | up to 30                        |
| $max\_attacks$   | maximum number of attacks                                                     | varied from 2 to 9              |
| $epsilon\_DAD$   | relative tolerance for the DAD model                                          | varied from 0.15 to 2           |

Recall that each attack has an area effect which disables the attacked node and all adjacent nodes. Introducing the possibility of two attacks will show some common effects regardless of the placement of access point and gateway nodes. Further analysis is done on each configuration to determine the number of attacks required to completely

block all flow in the network. The value of *epsilon\_DAD* was varied in order for the model to converge on a solution for some of the configurations.

The optimal placement of repeater nodes with and without two attacks for each configuration is shown in Figures 24 through 42, where the nodes are labeled according to Table 2. The various configurations of access point nodes and gateway nodes are summarized in Tables 3 through 6.

Table 2. Labeling key for the network configurations in Figures 24 through 42.

|                                                                                    |                                                                 |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| S                                                                                  | access point node                                               |
| T                                                                                  | gateway node                                                    |
| R                                                                                  | repeater node                                                   |
| X                                                                                  | attacked node                                                   |
| R X                                                                                | attacked repeater node                                          |
|  | node disabled from the area effect of an adjacent attacked node |

### 1. Configuration A

Table 3. Configuration A for placement of *s* and *t* nodes.

| Node Type | Site | Row | Column |
|-----------|------|-----|--------|
| <i>s</i>  | n016 | 2   | 1      |
| <i>s</i>  | n113 | 8   | 8      |
| <i>s</i>  | n211 | 15  | 1      |
| <i>t</i>  | n015 | 1   | 15     |
| <i>t</i>  | n225 | 15  | 15     |

The initial solution to the network routing problem with 5 repeater nodes and without any attacks for configuration A is shown in Figure 24.

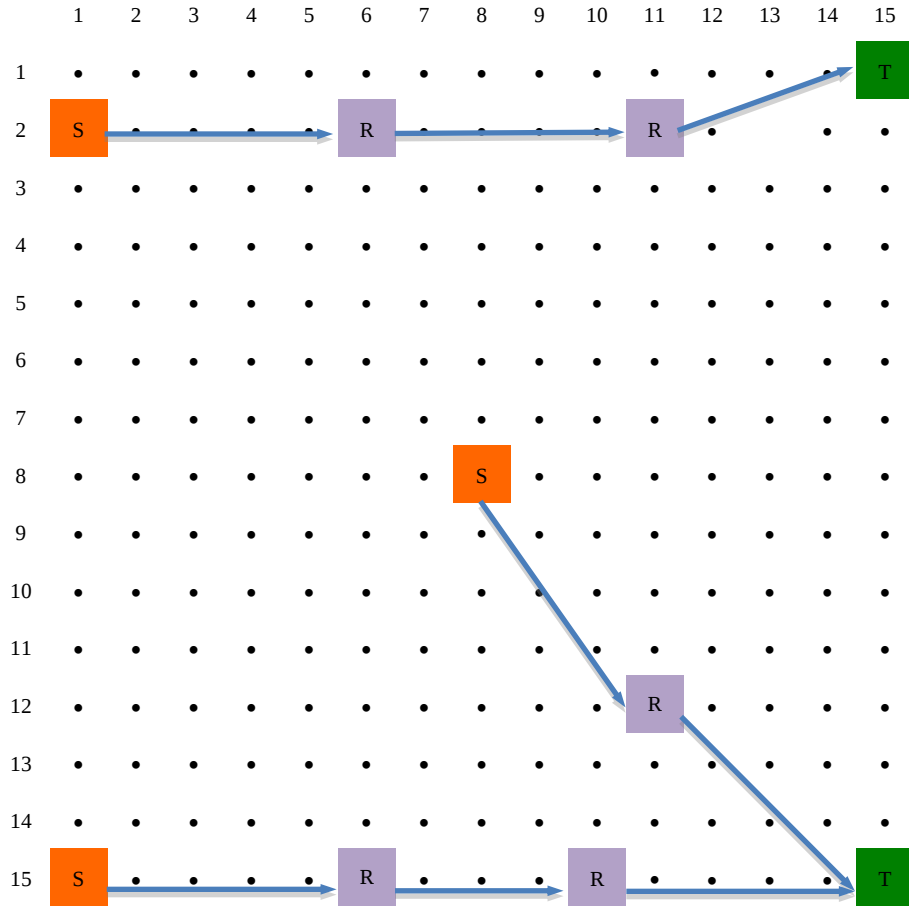


Figure 24. Optimal node placement without any attacks for configuration A (with 5 repeater nodes).

With two attacks, the attacker can completely isolate the  $t$  node in (1, 15). The repeater nodes in (5, 12) and (11, 12) are disabled but the flow that would go through these nodes is redirected and all  $s$  nodes are still connected to at least one  $t$  node. Figure 25 illustrates the resulting network configuration with 6 repeater nodes.

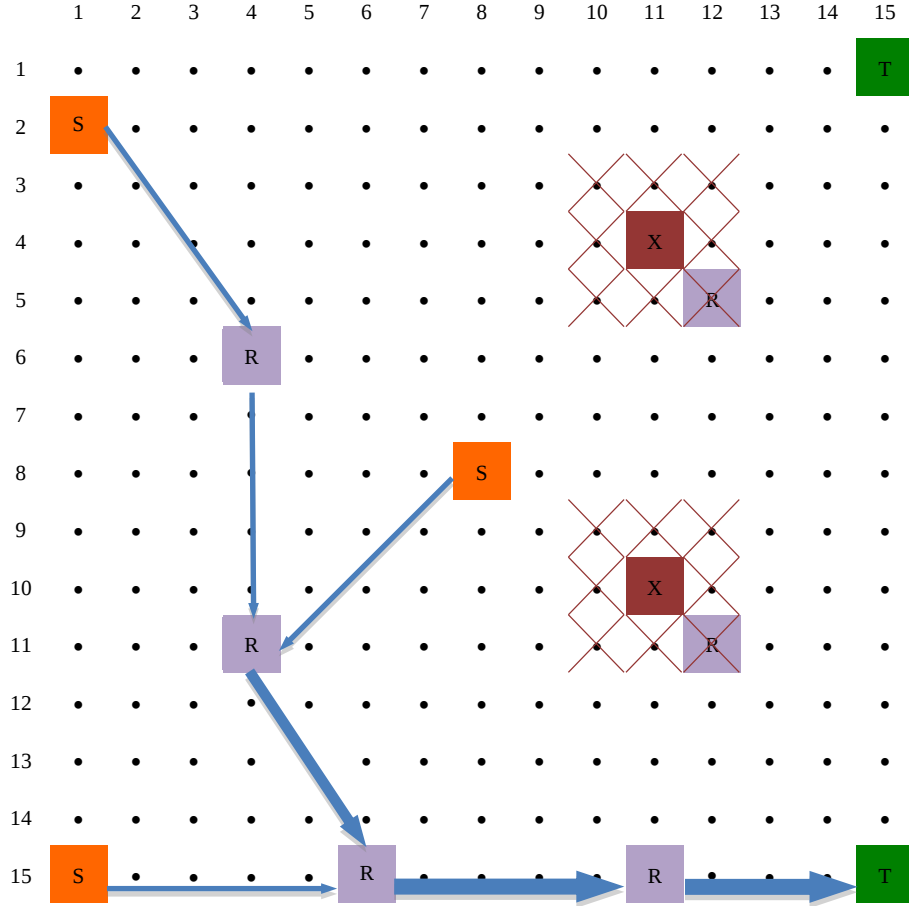


Figure 25. Optimal node placement with two attacks for configuration A (with 6 repeater nodes and no  $s$  nodes blocked).

With four attacks, the attacker can completely isolate the  $t$  node in (1, 15) and block all flow from the  $s$  node in (2, 1). Even though there are multiple disabled repeater nodes, the flow from the  $s$  nodes in (15, 1) and (8, 8) is rerouted to the  $t$  node in (15, 15). If the repeater at (6, 4) had been placed at (7, 3) then if all else remained the same, the  $s$  node at (2, 1) would have a link to the  $t$  node in (15, 15). However, if the repeater node had been placed at (7, 3) instead of (6, 4), the algorithm would have placed the attacks differently and evaluated the resulting solution to be less optimal than the final solution. Figure 26 illustrates the resulting network configuration with 25 repeater nodes and one  $s$  node blocked.

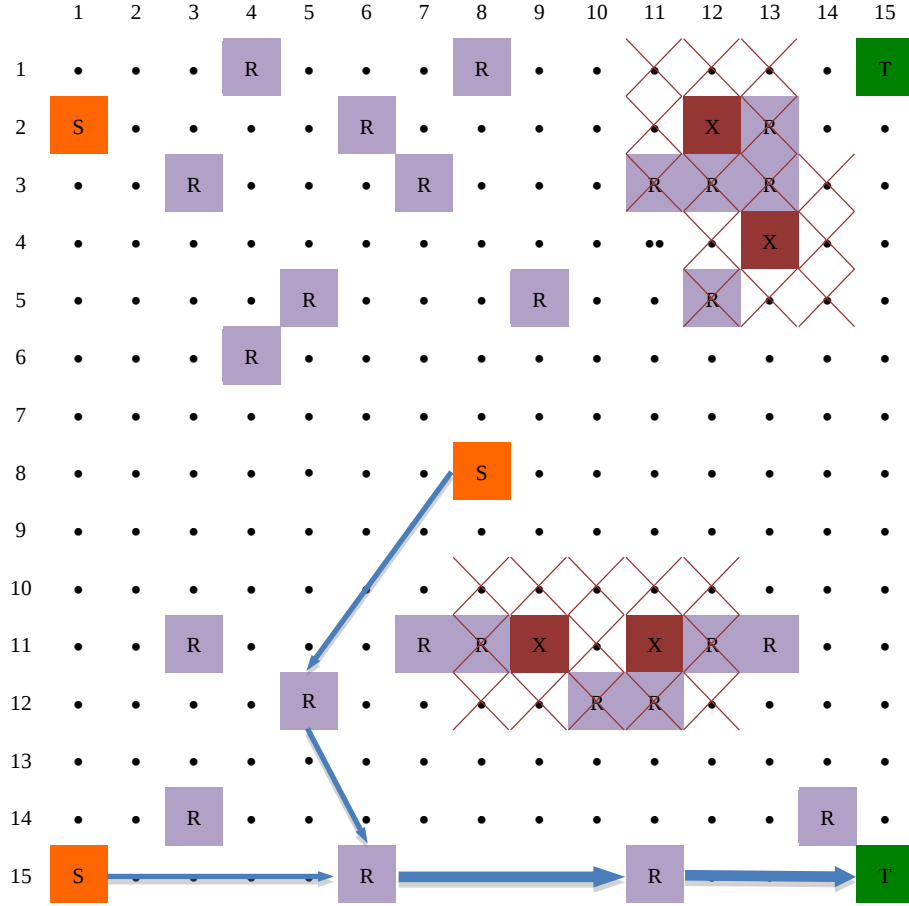


Figure 26. Optimal node placement with four attacks for configuration A (with 25 repeater nodes and one s node blocked).

With six attacks, the attacker can completely isolate the  $t$  node in (15, 15) and block all flow from the  $s$  nodes in (2, 1) and (15, 1). Despite multiple disabled repeater nodes, the flow from the  $s$  nodes in (8, 8) is rerouted to the  $t$  node in (1, 15). One of the attacks is on the repeater node in (4, 11). Figure 27 illustrates the resulting network configuration A with 25 repeater nodes and two  $s$  nodes blocked.

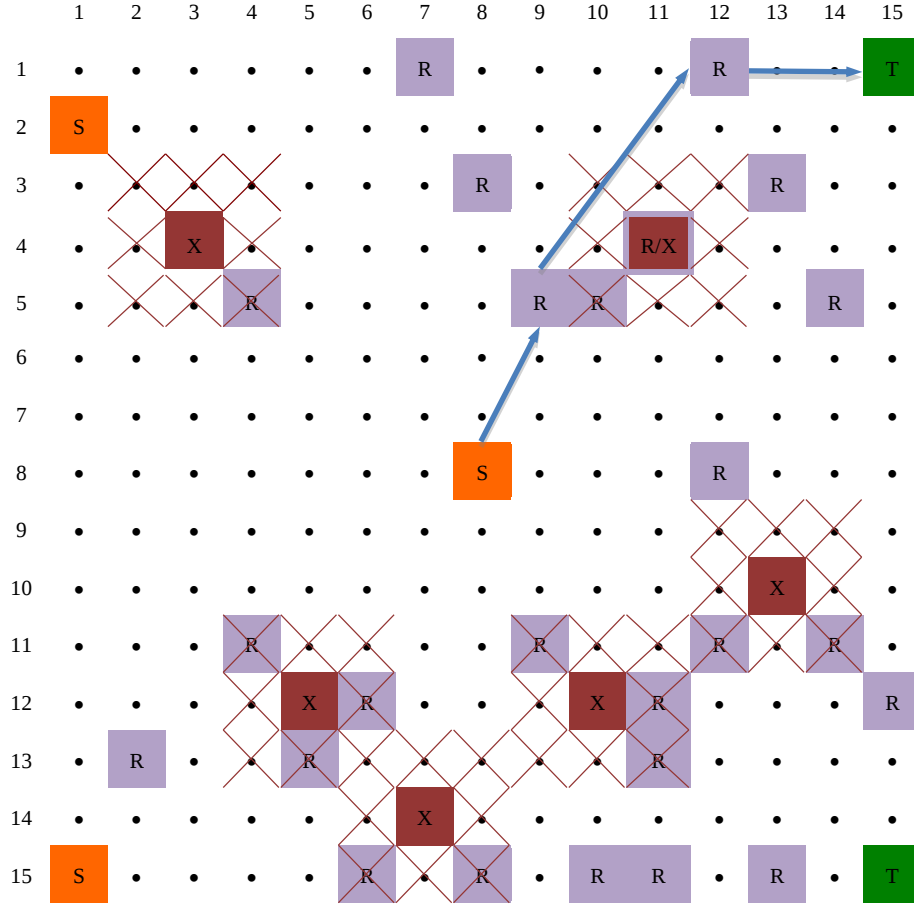


Figure 27. Optimal node placement with six attacks for configuration A (with 25 repeater nodes and two s nodes blocked).

With seven attacks, the attacker can completely isolate both  $t$  nodes and block all flow from all  $s$  nodes. One of the attacks is on the repeater node in (12, 11). Figure 28 illustrates the resulting network configuration with 5 repeater nodes and all flow blocked in the network. Although it may appear that the addition of only a few nodes near the  $t$  node at (15, 15) could provide conductivity in the network, the full story comes in the effect of increasing the maximum number of attacks from 6 in Figure 27 to 7 in Figure 28. The addition of one more attack blocks the only remaining flow in the network from the  $s$  node at (8, 8) ensuring that there is no solution that provides connectivity even if all 25 repeater nodes were used. This is reflected when the algorithm places minimum repeater nodes and groups the attacks. The only way to provide flow in the network is to increase the number of repeater nodes available. When there are sufficient attacks to

block all flow in the network, the algorithm provides similar solutions for configurations B, C, and D.

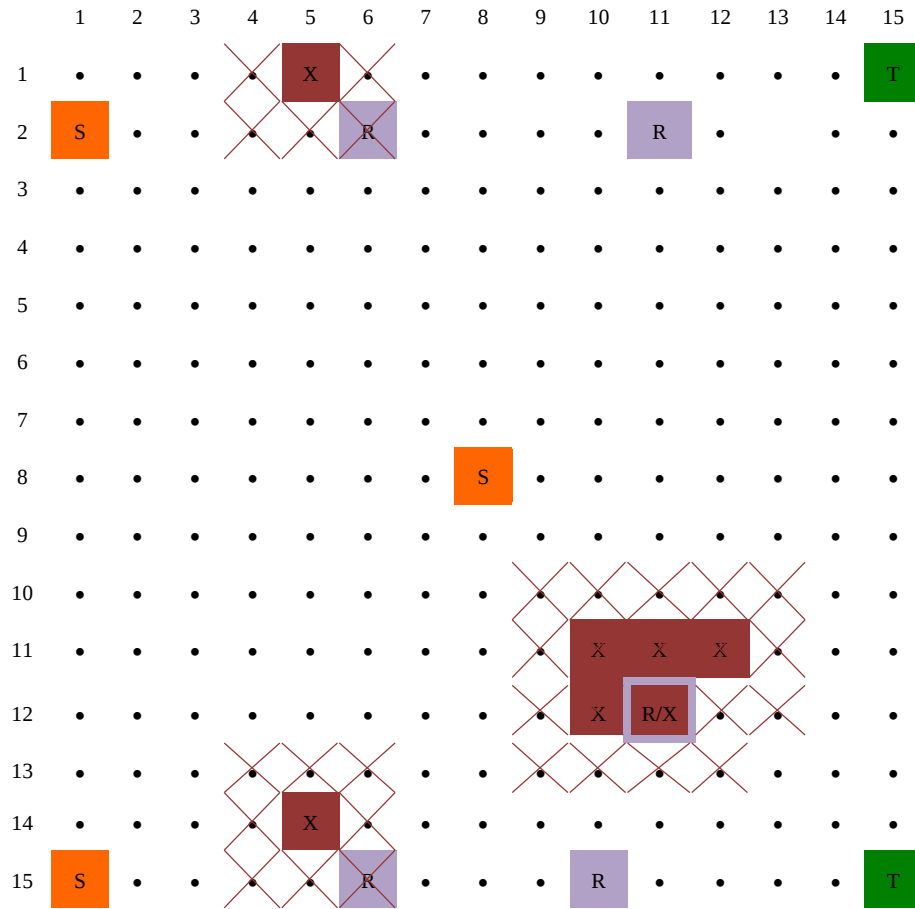


Figure 28. Optimal node placement with seven attacks for configuration A (with 5 repeater nodes and all flow blocked in the network).

## 2. Configuration B

Table 4. Configuration B for placement of  $s$  and  $t$  nodes.

| Node Type | Site | Row | Column |
|-----------|------|-----|--------|
| $s$       | n015 | 1   | 15     |
| $s$       | n113 | 8   | 8      |
| $s$       | n211 | 15  | 1      |
| $t$       | n001 | 1   | 1      |
| $t$       | n225 | 15  | 15     |

The initial solution to the network routing problem without any attacks for configuration B is shown in Figure 29 with 7 repeater nodes.

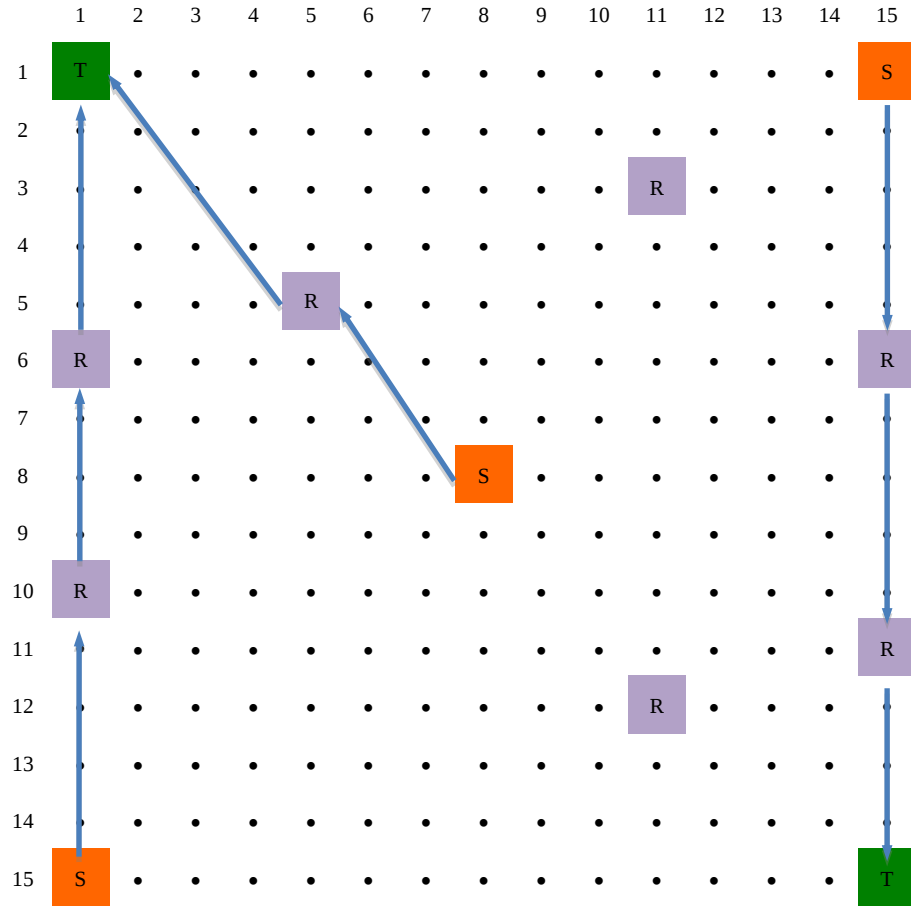


Figure 29. Optimal node placement without any attacks for configuration B (with 7 repeater nodes).

With two attacks, the attacker can completely isolate the  $t$  node in (1, 15). The repeater nodes in (4, 5), (5, 4), and (11, 12) are disabled. The flow from the  $s$  nodes in (1, 15) and (8, 8) are redirected so all  $s$  nodes are still connected to at least one  $t$  node. Figure 30 illustrates the resulting network configuration with 13 repeater nodes and no  $s$  nodes blocked when there were 15 repeater nodes available. Since all  $s$  nodes are connected, the additional 2 repeater nodes are not necessary to provide flow in the network.

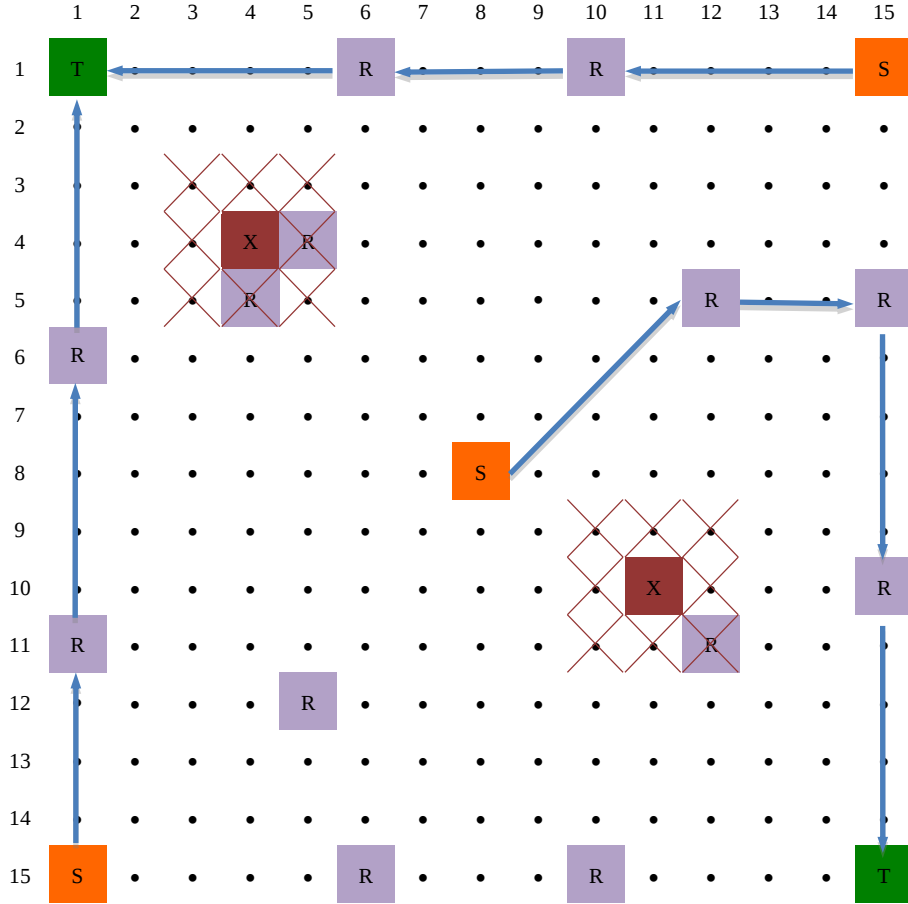


Figure 30. Optimal node placement with two attacks for configuration B (with 13 repeater nodes and no s nodes blocked).

With four attacks, the attacker is able to completely isolate the  $t$  node in (15, 15) and block all flow from  $s$  node in (1, 15). Even though there are multiple disabled repeater nodes, the flow from  $s$  nodes in (8, 8) and (1, 15) is rerouted so that they are still connected to one  $t$  node. Figure 31 illustrates the resulting network configuration with 13 repeater nodes and no  $s$  nodes blocked when there were 15 repeater nodes available. Since all  $s$  nodes are connected, the additional 2 repeater nodes are not necessary to provide flow in the network.

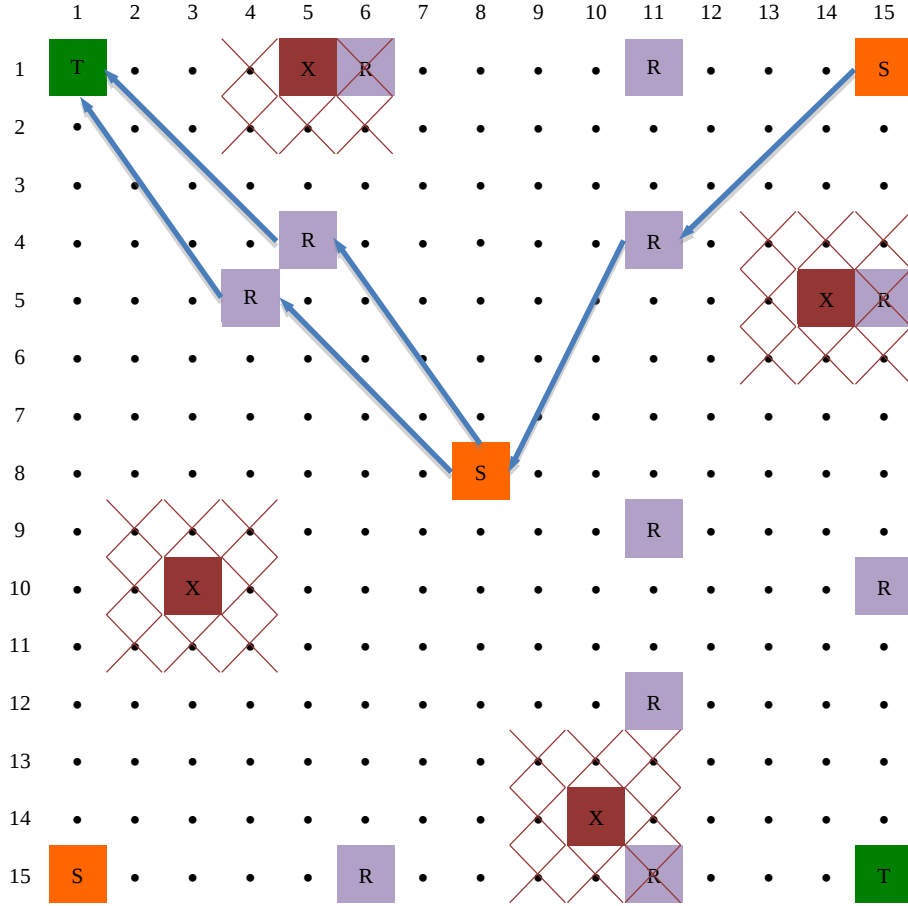


Figure 31. Optimal node placement with four attacks for configuration B (with 13 repeater nodes and no  $s$  nodes blocked).

With six attacks, the attacker is able to completely isolate the  $t$  node in (1, 1) and block all flow from the  $s$  nodes in (1, 15) and (8, 8). Even though there are multiple disabled repeater nodes, the flow from the  $s$  node in (1, 15) is rerouted so that it is still connected to one  $t$  node. One of the attacks is on the repeater node in (6, 1). Figure 32 illustrates the resulting network configuration with 21 repeater nodes and two  $s$  nodes blocked. Here since the  $s$  nodes at (15, 1) and (8, 8) are completely blocked, flow in the network would not improve even if all 25 repeater nodes were used.

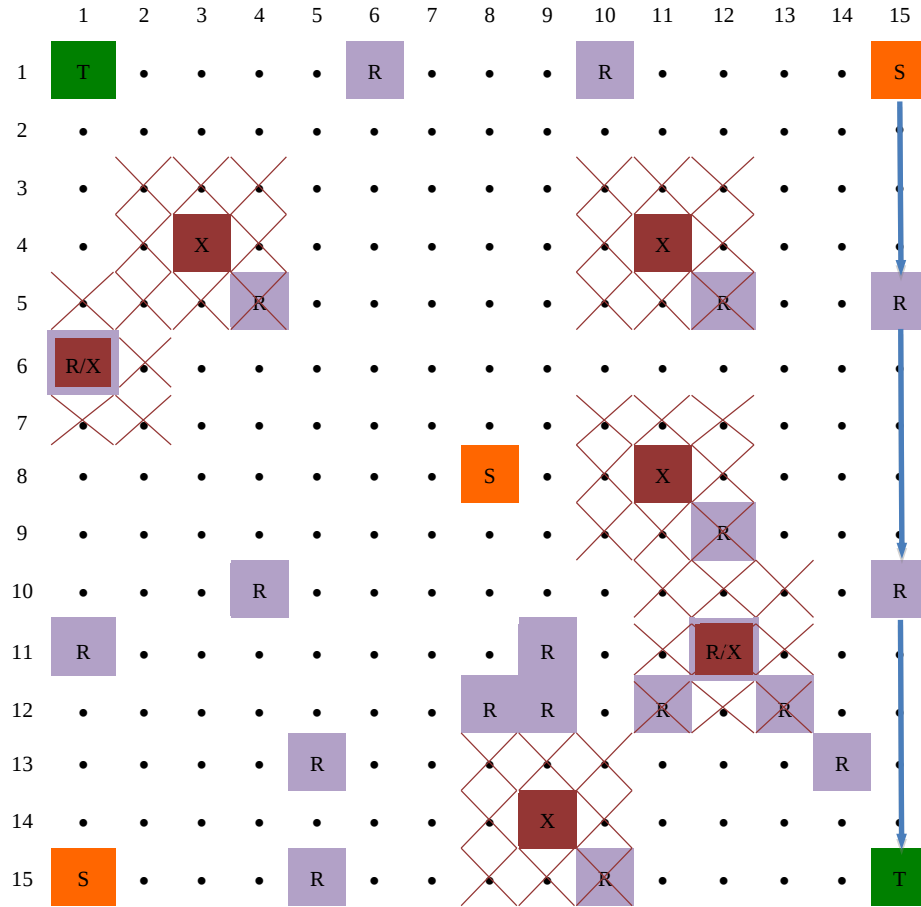


Figure 32. Optimal node placement with six attacks for configuration B (with 21 repeater nodes and two s nodes blocked).

With seven attacks, the attacker can completely isolate both  $t$  nodes and block all flow from all  $s$  nodes. Figure 33 illustrates the resulting network configuration with 7 repeater nodes and all flow blocked the network even though up to 25 repeater nodes were available. This is the same result and discussion as in configuration A for Figures 27 and 28 where all flow in the network is blocked.

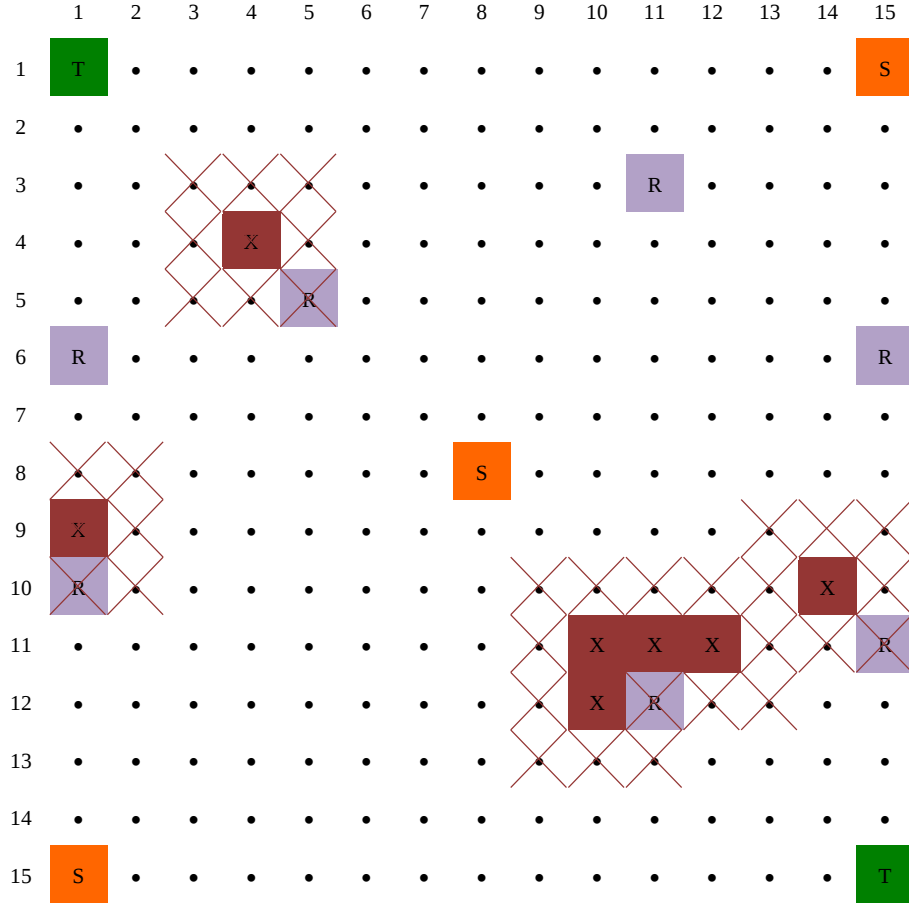


Figure 33. Optimal node placement with seven attacks for configuration B (with 7 repeater nodes and all flow blocked the network).

### 3. Configuration C

Table 5. Configuration C for placement of  $s$  and  $t$  nodes.

| Node Type | Site | Row | Column |
|-----------|------|-----|--------|
| $s$       | n008 | 1   | 8      |
| $s$       | n113 | 8   | 8      |
| $s$       | n218 | 15  | 8      |
| $t$       | n106 | 8   | 1      |
| $t$       | n120 | 8   | 15     |

The initial solution to the network routing problem without any attacks for configuration C is shown in Figure 34 with two repeater nodes.

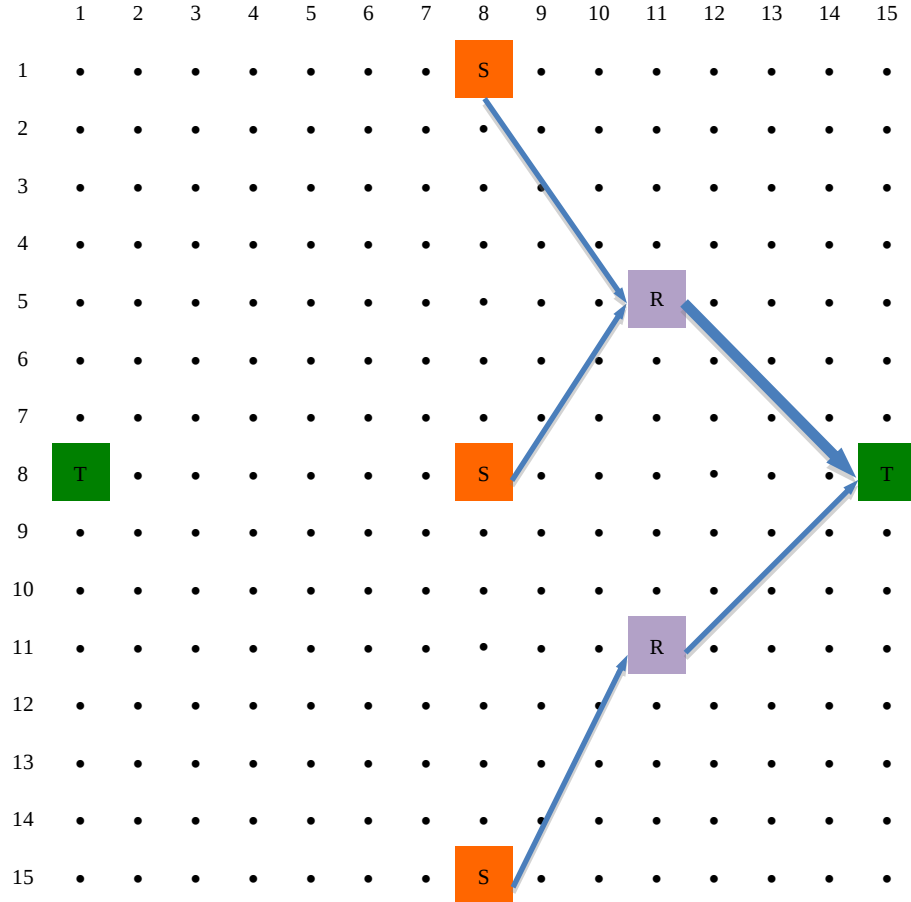


Figure 34. Optimal node placement without any attacks for configuration C (with 2 repeater nodes).

With two attacks, the attacker can only disable the two repeater nodes in (5, 5) and (5, 11). The flow from the  $s$  nodes in (1, 8) and (8, 8) are redirected so all  $s$  nodes are still connected to at least one  $t$  node. Figure 35 illustrates the resulting network configuration with 7 repeater nodes and no  $s$  nodes blocked.

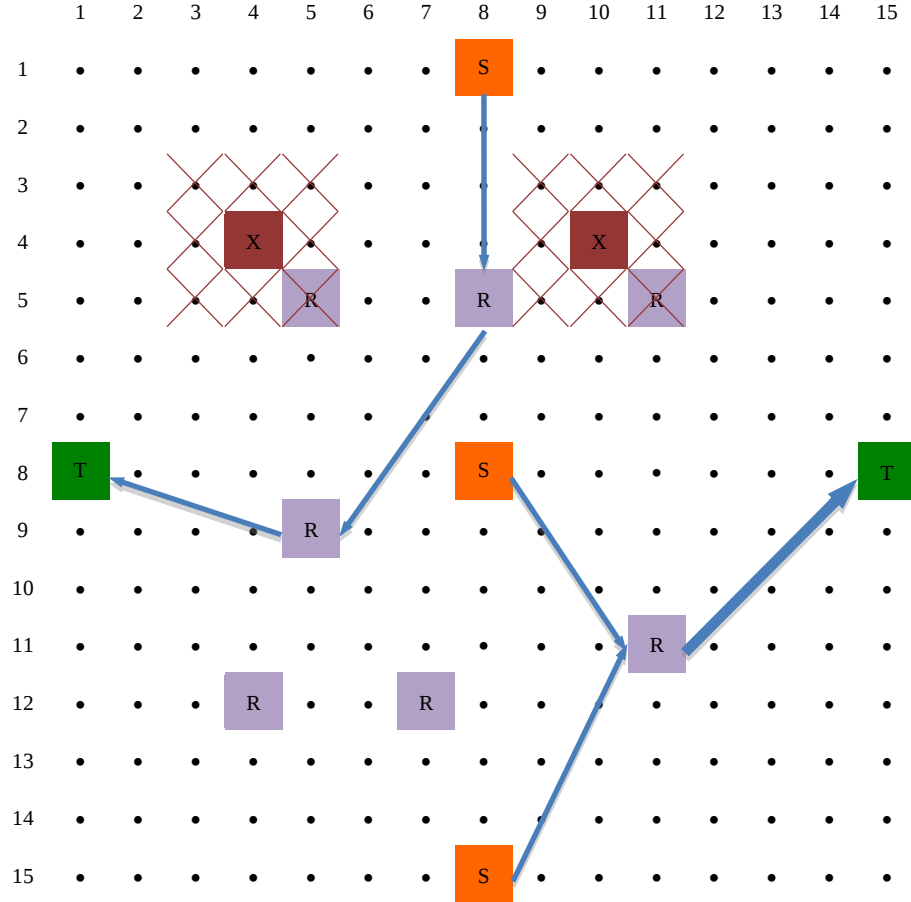


Figure 35. Optimal node placement with two attacks for configuration C (with 7 repeater nodes and no  $s$  nodes blocked).

With four attacks, the attacker can only disable five of the repeater nodes. The flow from the  $s$  nodes in (8, 1) and (8, 8) are redirected and the flow from the  $s$  node in (15, 8) goes through a different repeater node so all of the  $S$  nodes are still connected to at least one  $t$  node. Figure 36 illustrates the resulting network configuration with 8 repeater nodes and no  $s$  nodes blocked when there were 25 repeater nodes available. Since all  $s$  nodes are connected, the additional 17 repeater nodes are not necessary to provide flow in the network.

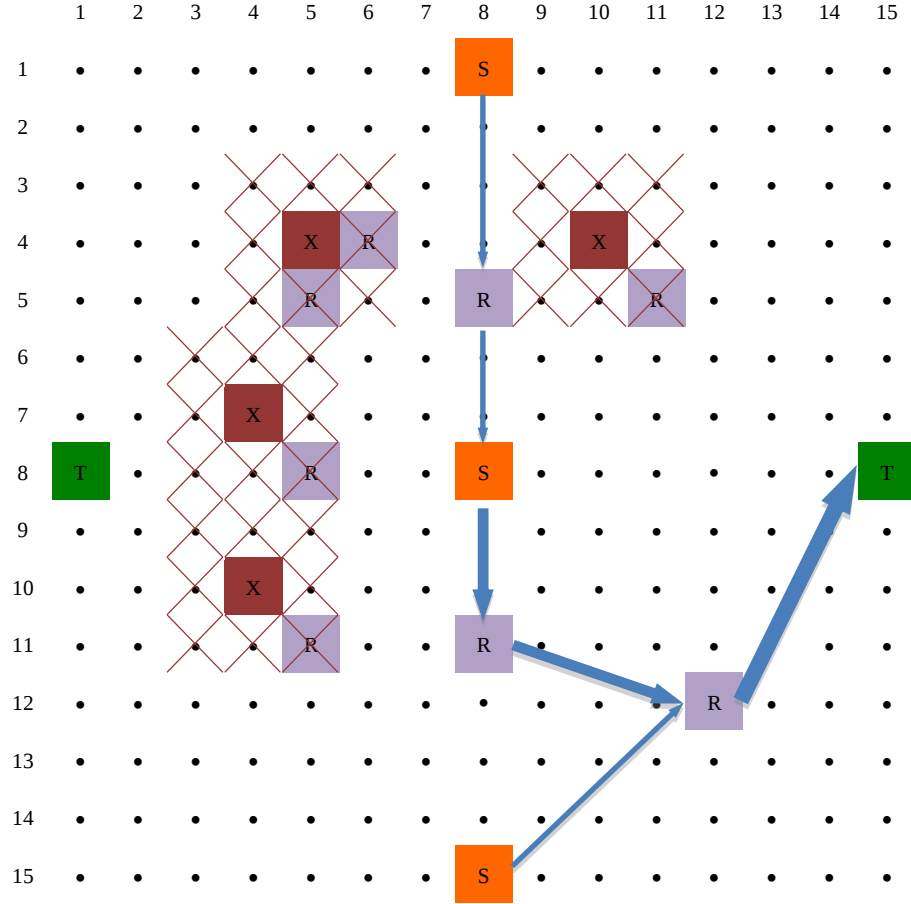


Figure 36. Optimal node placement with four attacks for configuration C (with 8 repeater nodes and no  $s$  nodes blocked).

With six attacks, the attacker can only disable nine of the repeater nodes and the resulting network flow maintains all of the  $s$  nodes connected to at least one  $t$  node. Figure 37 illustrates the resulting network configuration with 14 repeater nodes and no  $s$  nodes blocked when there are 25 repeater nodes available. Since all  $s$  nodes are connected, the additional 11 repeater nodes are not necessary to provide flow in the network.

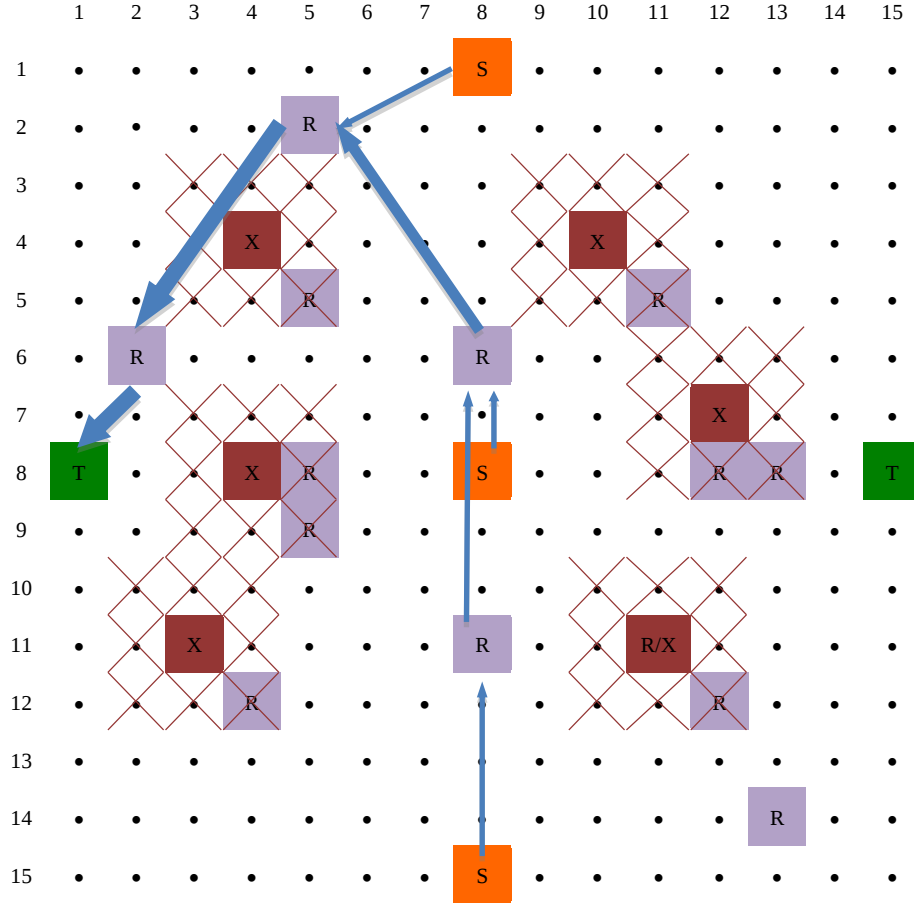


Figure 37. Optimal node placement with six attacks for configuration C (with 14 repeater nodes and no  $s$  nodes blocked).

With eight attacks, the attacker is able to block all flow from the  $s$  nodes in (1, 8) and (8, 8) and isolate the  $t$  node in (8, 1). The flow from the  $s$  node in (15, 8) is redirected so it is still connected to at least one  $t$  node. Two of the attacks are on the repeater nodes in (8, 10) and (11, 11). Figure 38 illustrates the resulting network configuration with 15 repeater nodes and one  $s$  node blocked when there are 25 repeater nodes available. Even if the other 10 repeater nodes were used, the algorithm evaluated the resulting solution would be suboptimal when compared to the final solution.

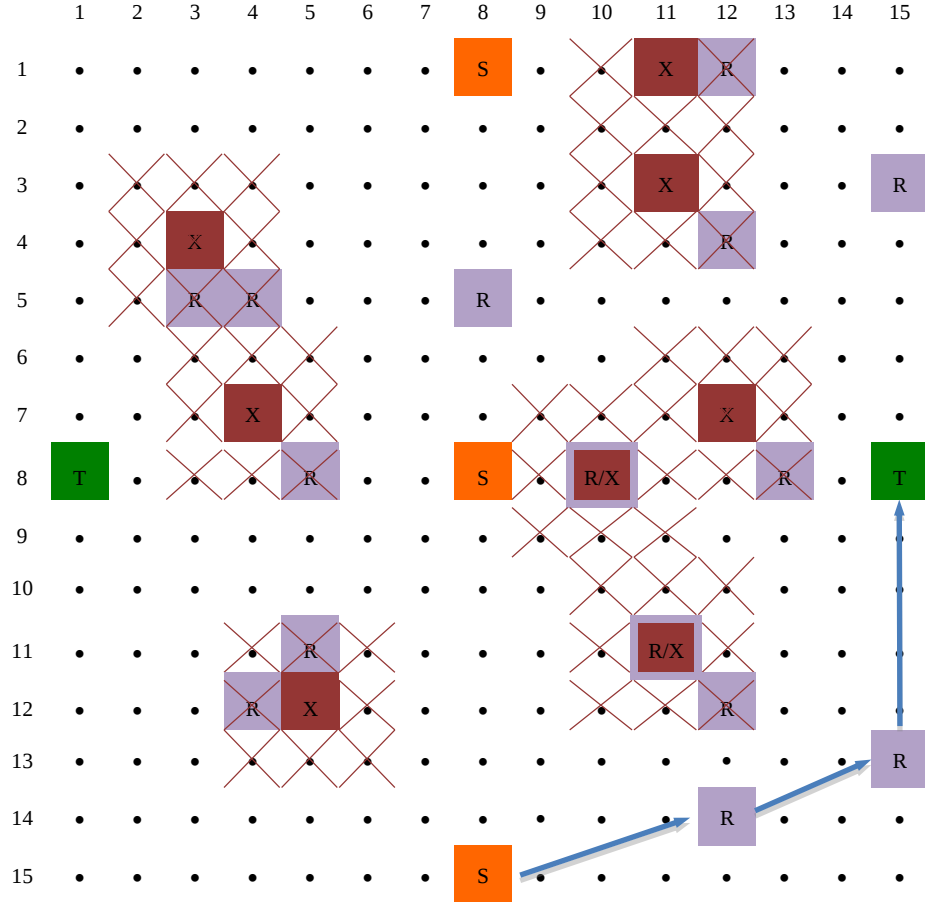


Figure 38. Optimal node placement with eight attacks for configuration C (with 15 repeater nodes and one s node blocked).

With nine attacks, the attacker is able to completely isolate all flow from all  $t$  nodes and block all flow from all the  $s$  nodes. One of the attacks is on the repeater node in (5, 11). Figure 39 illustrates the resulting network configuration with only 2 repeater nodes and all flow blocked in the network when there are 25 repeater nodes available. This is the same result and discussion as in configuration A for Figures 27 and 28 where all flow in the network is blocked.

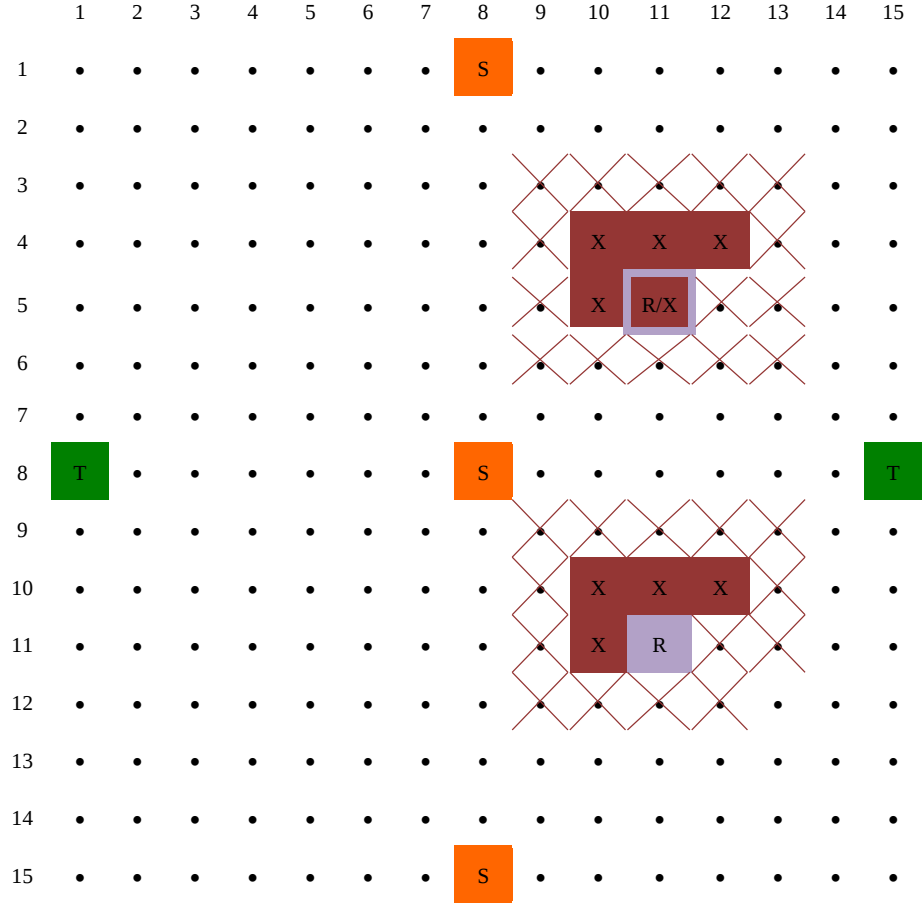


Figure 39. Optimal node placement with nine attacks for configuration C (with 2 repeater nodes and all flow blocked in the network).

#### 4. Configuration D

Table 6. Configuration D for placement of  $s$  and  $t$  nodes.

| Node Type | Site | Row | Column |
|-----------|------|-----|--------|
| $s$       | n211 | 15  | 1      |
| $s$       | n218 | 15  | 8      |
| $s$       | n225 | 15  | 15     |
| $t$       | n004 | 1   | 4      |
| $t$       | n012 | 1   | 12     |

The initial solution to the network routing problem without any attacks for configuration D is shown in Figure 40 with 7 repeater nodes.

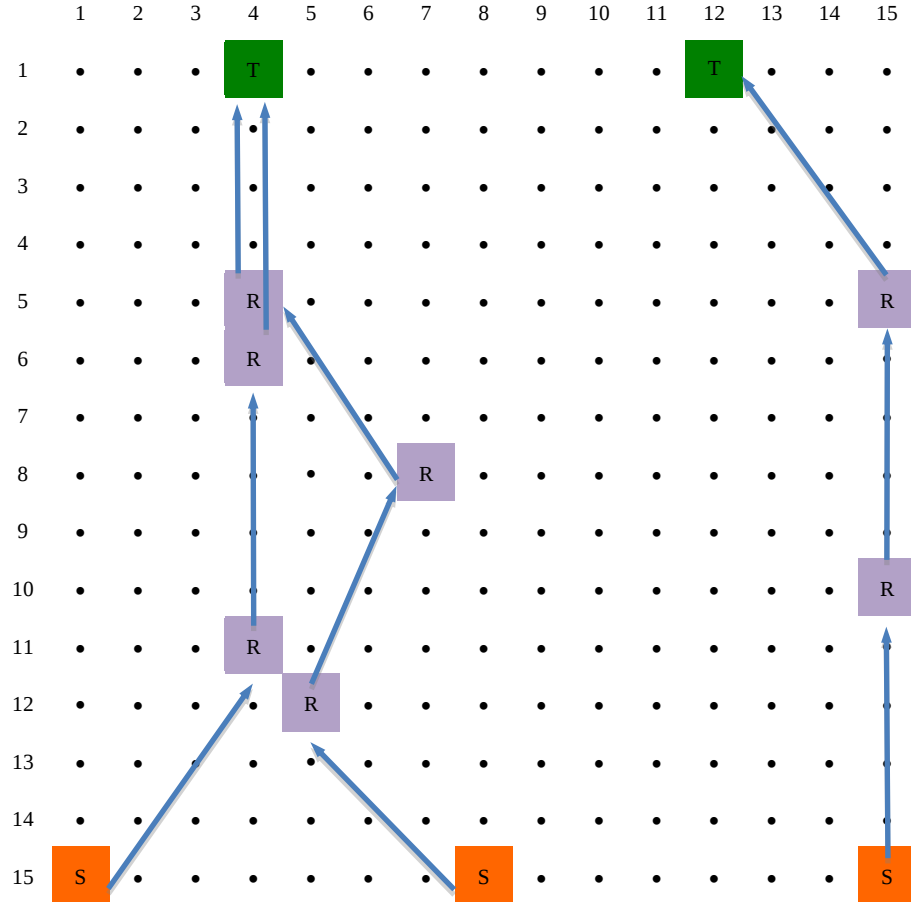


Figure 40. Optimal node placement without any attacks for configuration D (with 7 repeater nodes).

With two attacks, the attacker isolates the  $t$  node in (1, 12). The flow from the  $s$  nodes in (15, 1) and (15, 8) are redirected so all  $s$  nodes are still connected to at least one  $t$  node. Figure 41 illustrates the resulting network configuration with 20 repeater nodes and no  $s$  nodes blocked when there were 25 repeater nodes available. Since all  $s$  nodes are connected, the additional 5 repeater nodes are not necessary to provide flow in the network.

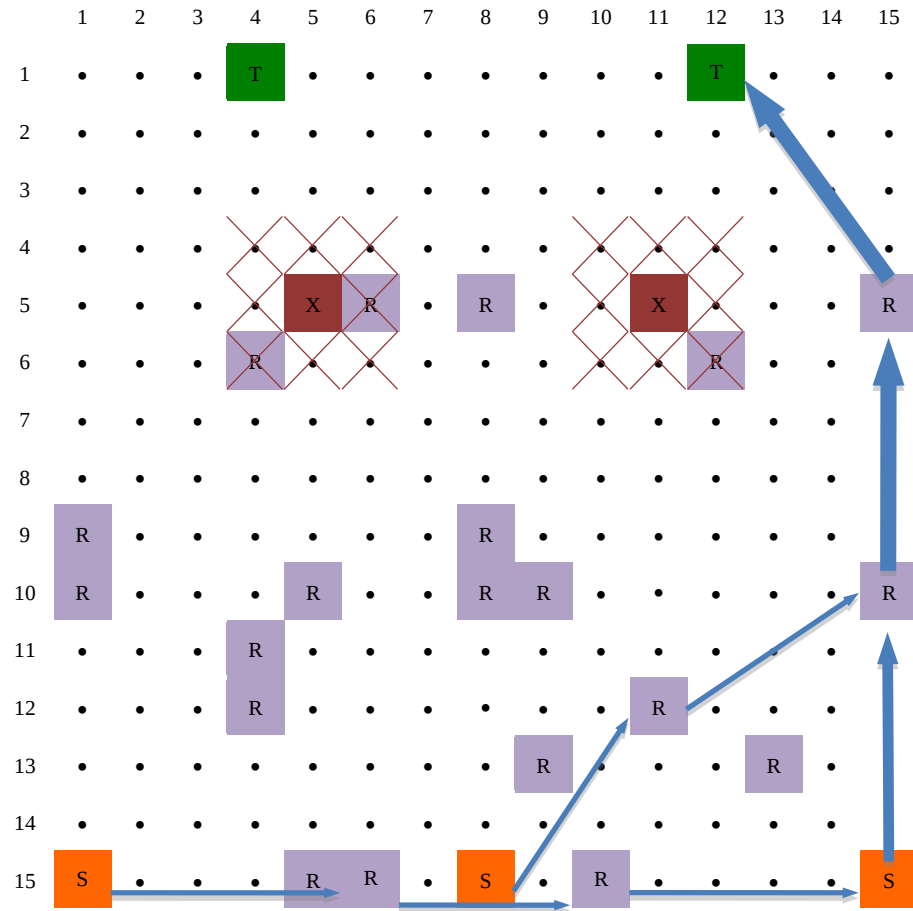


Figure 41. Optimal node placement with two attacks for configuration D (with 20 repeater nodes and no s nodes blocked).

With four attacks, the attacker is able to completely isolate all s nodes. Figure 42 illustrates the resulting network configuration with 7 repeater nodes and all flow blocked in the network even though up to 25 repeater nodes were available. This is the same result and discussion as in configuration A for Figures 27 and 28 where all flow in the network is blocked.

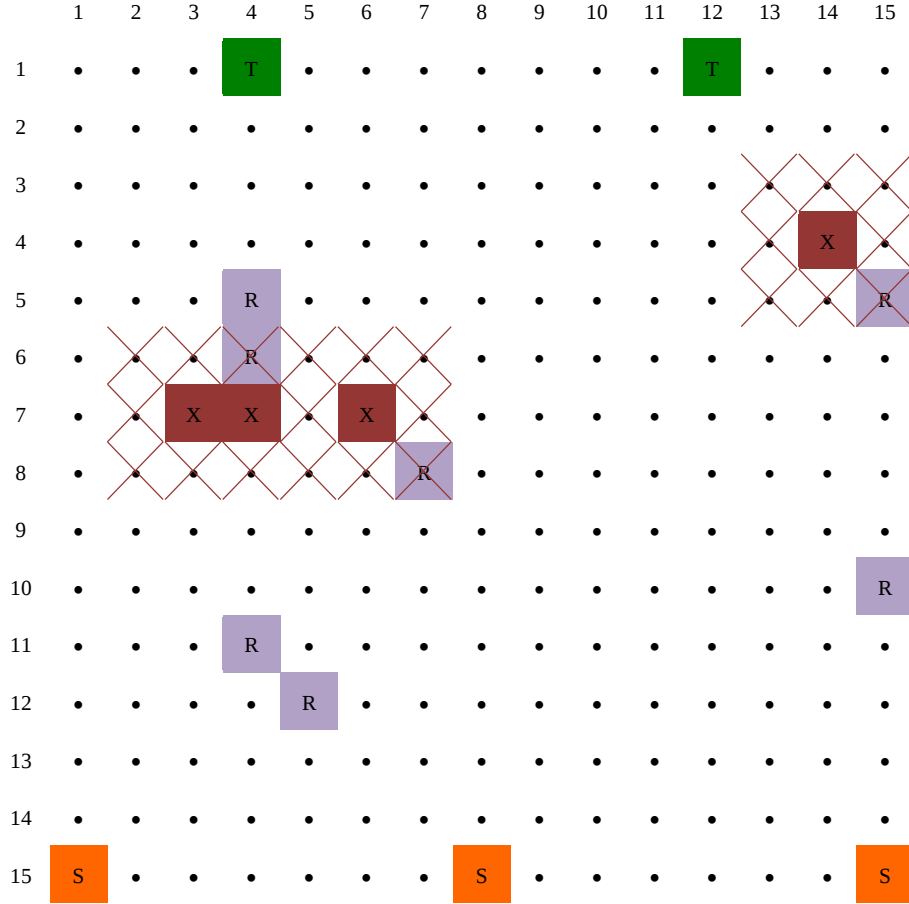


Figure 42. Optimal node placement with four attacks for configuration D (with 7 repeater nodes and all flow blocked in the network).

## B. CONCLUSIONS

While the flow of none of the network configurations are completely blocked by two attacks, by comparing the resulting node placements it is possible to draw some general conclusions. Configurations A and D are more affected by attacks than configurations B and C. The  $t$  nodes in configurations A and D are on the same geometric side whereas the  $t$  nodes for configurations B and C are on opposite sides of the network coverage area. The arrangement for A and D force the flow to only one of the two  $t$  nodes with more units of flow across fewer arcs, making it more vulnerable to further attacks and potentially slowing down the flow of information through the network.

Other conclusions can be drawn from the comparison of the various network configurations when all flow is completely blocked by attacks. The three network configurations A, B, and C that have at least one of the access point nodes,  $s$ , in the middle of the geographic area are much more resilient than network configuration D which has all the  $s$  nodes on the same side of the area. Also, network configuration C is the one with the most (nearly identical) options with all the  $s$  nodes evenly spaced between two parallel sides, is the most resilient network configuration. The number of attacks required to completely block all flow in the network is summarized in Table 7.

Table 7. Number of attacks required to completely block the flow in the network.

| Network Configuration | Number of Attacks |
|-----------------------|-------------------|
| A                     | 7                 |
| B                     | 7                 |
| C                     | 9                 |
| D                     | 4                 |

Overall, this analysis demonstrates two important factors that determine the resiliency of a network against attack or disruption. A network's resilience is related to: 1) the number of possible sources or destinations that are available in that network, and 2) the separation of those sources or destinations. The algorithm developed in this thesis could be crucial in designing an underwater network that is constrained by geography or other environmental factors.

### C. FUTURE WORK

There are several possibilities to further this research in optimizing networks. Currently the gams code can only be used on relatively small networks such as the 15 by 15 network used as a basis for the analysis in this thesis with few  $s$  and  $t$  nodes. This limitation prevents applying it to many practical applications such as public underwater acoustic communications networks, transportation networks, product distribution networks, airline schedules, and communication networks. The code could be modified

to allow the user to enter a starting solution, simplifying the complexity of the calculations and speeding up the execution time of the algorithm.

This work could be carried forward and improved by modifying the gams code to make the penalty terms distance related instead of being tied to the number of nodes travelled from source to destination. This would also make the code easily adapted to larger networks regardless of node spacing or total number of nodes.

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX A. ALGORITHM IMPLEMENTED IN GAMS CODE FOR NETWORK CONFIGURATION A WITH TWO ATTACKS

```
$TITLE SUBNET - Robust design of a submarine communications network using
acoustic modems 130228
```

```
$STITLE Multicommodity network flow formulation, DAD with a dual-ILP
formulation of the AD subproblem
```

```
$INLINECOM { }
```

```
OPTIONS
```

```

    SOLPRINT =      OFF,
    DECIMALS =       1,
    LIMCOL   =       0,
    LIMROW   =       0,
    RESLIM   =      3600, {max seconds}
    ITERLIM  = 99999999, {max iterations}
    OPTCR    =       0.01,
    LP       =      CPLEX,
    MIP      =      CPLEX
;

```

```
FILE out /SUBNET_DAD_KILP.out/;
PUT out;
```

```
PUT 'SUBNET 2.0 130228' / ;
PUTCLOSE out;
```

```

file opt /cplex.opt/ ;
put opt;
put 'startalg 1' / ;
put 'subalg 1' / ;
put 'brdir 1' / ;
put '*mipemphasis 4' / ; {1 for feasibility, or 4 for hidden feasible
solutions}
put 'cuts no' / ;
put 'heurfreq -1' / ;
put '*threads 0' / ;
put '*parallelmode 1' / ;
putclose opt;

```

```

put out;
SETS
    n nodes /
        n001*n225
    /

```

```
{this initial s and t placement is for network configuration A}
```

```

    s(n) /
        n016
        n113
        n211
    /

```

```

t(n) /
    n015
    n225

```

```

/

arc(n,n)
impact(n,n)
d /d00*d99/
;

alias(n,i,j,iprime,jprime,k);
SCALAR
    q {cost for undelivered packet}
    p {cost for delivering a packet over an attacked arc}
    sidelen /5/ {distance between adjacent cells, nm}
    maxdist /25/ {max distance between nodes for a connection to exist}
    max_repeater /11/ {remember to count the access points and the gateway!}
    max_attacks /2/ {set this to 0 when solving for initial placement with no
attacks, varied from 2 to 9 to find the number of attacks to completely block
all flow in a network}
    attack_arc /8/ {the effective radius of an attack, when a node i is attacked
all adjacent nodes are affected}
    card_t
    card_s
    rect_wd /15/
    rect_ht /15/
;
card_t = SUM(t(i),1);
card_s = SUM(s(i),1);

q = CEIL(rect_wd*sidelen/maxdist + rect_ht*sidelen/maxdist);
p = q+1;

VARIABLES
    Z
;
POSITIVE VARIABLES
    E(i)
    F(i,k)
    Y(i,j,k)
;

SCALARS
    d_x
    d_y
    dist
    x_iter
    r_iter
    max_r_iters /30/ {varied up to 75 to obtain convergence, set this to 1 when
solving for initial placement with no attacks}
    lb_DAD
    ub_DAD
    lb_AD
    ub_AD
    is_error
    epsilon_DAD
    epsilon_DAD_M
    epsilon_AD
;

SETS
    xbar(iprime)
    xbard(iprime,d)
    rbar(i)
    xbest(iprime)

```

```

    rbest(i)
;

epsilon_DAD = 0.15; {this was varied to get converge for placements B, C, and
D}
epsilon_AD = 0.01;
epsilon_DAD_M = 0.05;

{determining the arc set}
LOOP((i,j),
    d_x = sidelength*ABS(MOD(ORD(i)-1,rect_wd)-MOD(ORD(j)-1,rect_wd));
    d_y = sidelength*ABS(CEIL(ORD(i)/rect_ht)-CEIL(ORD(j)/rect_ht));
    dist = SQRT(SQR(d_x)+SQR(d_y));
    if( dist<=maxdist,
        arc(i,j) = yes;
    );
);

{determining the subset of attacked nodes}
LOOP((i,iprime),
    d_x = sidelength*ABS(MOD(ORD(i)-1,rect_wd)-MOD(ORD(iprime)-1,rect_wd));
    d_y = sidelength*ABS(CEIL(ORD(i)/rect_ht)-CEIL(ORD(iprime)/rect_ht));
    dist = SQRT(SQR(d_x)+SQR(d_y));
    if( dist<=attack_arc,
        impact(i,iprime) = yes;
    );
);

EQUATIONS
    FLOW_OBJ
    FLOW_BALANCE(i,k)
    CONTROL_FLOW(i,k)
    DESIGN_CONTROL_FLOW(i,k)
    DESIGN_REPEATER_BUDGET
    DUAL_OBJ
    DUAL_Y(i,j,k)
    DUAL_E(k)
    DUAL_F(i,k)
    DUAL_ATTACK_BUDGET
    DUAL_UNIQUE_ATTACK(d)
    DAD_OBJ
    DAD_CUT(k,d)
    DAD_FLOW_BALANCE(i,k,d)
    DAD_CONTROL_FLOW(i,k,d)
    DAD_REPEATER_BUDGET
    DAD_LB
;

FLOW_OBJ..
Z =E= q*SUM(s(i), E(i)) +
        sum((i,j,k)$ (arc(i,j) and s(k)),
            (1 + p*sum(iprime$(impact(i,iprime) and xbar(iprime)),1)
              + p*sum(jprime$(impact(j,jprime) and
xbar(jprime)),1))*Y(i,j,k))
;
FLOW_BALANCE(i,k)$s(k).. {NODEPI(i,k)}
    SUM(arc(i,j), Y(i,j,k)) - SUM(arc(j,i), Y(j,i,k)) + E(k)$sameas(i,k) +
F(i,k)$t(i) =E= 1$sameas(i,k)
;
CONTROL_FLOW(i,s(k))$(not s(i) and not t(i)).. {MU(i,k)}
    SUM(arc(i,j), Y(i,j,k)) {+ E(k)$sameas(i,k) + F(i,k)$t(i)} =L= 1$rbar(i)
;

```

```

MODEL SUBNET_OPERATOR /
    FLOW_OBJ
    FLOW_BALANCE
    CONTROL_FLOW
;/

VARIABLES
    NODEPI(i,k)
;
POSITIVE VARIABLES
    MU(i,k)
;
BINARY VARIABLES
    X(iprime)
;

DUAL_OBJ..
    Z =E= SUM(s(k), NODEPI(k,k)) - SUM((rbar(i),s(k)), MU(i,k))
;

DUAL_Y(i,j,k)$ (arc(i,j) and s(k))..
    NODEPI(i,k) - NODEPI(j,k) - MU(i,k)
    - SUM(impact(i,iprime), p*X(iprime)) - SUM(impact(j,jprime), p*X(jprime))
=L= 1
;

DUAL_E(s(k))..
    NODEPI(k,k) - MU(k,k) =L= q
;

DUAL_F(t(i),s(k))..
    NODEPI(i,k) - MU(i,k) =L= 0
;

DUAL_ATTACK_BUDGET..
    SUM(iprime,X(iprime)) =L= max_attacks
;

DUAL_UNIQUE_ATTACK(d)$ (ORD(d)<=r_iter)..
    SUM(xbard(iprime,d),X(iprime)) =L= max_attacks - 1
;

MODEL SUBNET_DUALILP /
    DUAL_OBJ
    DUAL_Y
    DUAL_E
    DUAL_F
    DUAL_ATTACK_BUDGET
;/

MODEL SUBNET_DUALILP_UNIQUE /
    DUAL_OBJ
    DUAL_Y
    DUAL_E
    DUAL_F
    DUAL_ATTACK_BUDGET
    DUAL_UNIQUE_ATTACK
;/

VARIABLE
    Z_DAD(k)

```

```

;
POSITIVE VARIABLES
    YD(i,j,k,d)
    FD(i,k,d)
    ED(i,d)
;
BINARY VARIABLES
    R(i)
;

DAD_OBJ..
    Z =E= SUM(s(k), Z_DAD(k))
;
DAD_CUT(s(k),d)$ (ORD(d)<=r_iter)..
    Z_DAD(k) =G= q*ED(k,d) +
        sum(arc(i,j),
            (1 + p*sum(iprime$(impact(i,iprime) and xbard(iprime,d)),1)
              + p*sum(jprime$(impact(j,jprime) and
xbard(jprime,d)),1))*YD(i,j,k,d))
;
DAD_FLOW_BALANCE(i,k,d)$ (s(k) and ORD(d)<=r_iter)..
    SUM(arc(i,j), YD(i,j,k,d)) - SUM(arc(j,i),YD(j,i,k,d)) + ED(k,d)$sameas(i,k)
+ FD(i,k,d)$t(i) =E= 1$sameas(i,k)
;
DAD_CONTROL_FLOW(i,s(k),d)$ (not s(i) and not t(i) and ORD(d)<=r_iter)..
    SUM(arc(i,j), YD(i,j,k,d)) {+ ED(k,d)$sameas(i,k) + FD(i,k,d)$t(i)} =L= R(i)
;
DAD_REPEATER_BUDGET..
    SUM(i,R(i)) =L= max_repeaters
;
DAD_LB..
    SUM(s(k),Z_DAD(k)) =G= lb_DAD
;

MODEL SUBNET_DAD_MASTER /
    DAD_OBJ
    DAD_CUT
    DAD_FLOW_BALANCE
    DAD_CONTROL_FLOW
    DAD_REPEATER_BUDGET
;/

DESIGN_CONTROL_FLOW(i,s(k))$ (not s(i) and not t(i))..
    SUM(arc(i,j), Y(i,j,k)) {+ E(k)$sameas(i,k) + F(i,k)$t(i)} =L= R(i)
;

DESIGN_REPEATER_BUDGET..
    SUM(i,R(i)) =L= max_repeaters
;

MODEL SUBNET_DESIGN /
    FLOW_OBJ
    FLOW_BALANCE
    DESIGN_CONTROL_FLOW
    DESIGN_REPEATER_BUDGET
;/

{Models up to here, rest of file is algorithm}

*Protect s(i) and t(i) from attack
LOOP(impact(i,iprime)$ (s(i) or t(i)),
    X.fx(iprime) = 0 ;

```

```

);

SUBNET_DAD_MASTER.optcr = epsilon_DAD_M ;

SUBNET_DAD_MASTER.optfile = 1;
SUBNET_DUALILP.optcr = epsilon_AD;

SUBNET_DESIGN.optfile = 1;

xbar(i) = 0;
IF(max_repeaters < card(s)+card(t),
    PUT 'Insufficient repeaters to build network.' / / ;
ELSE
    LOOP(s(i),
        R.fx(i) = 1;
    );
    LOOP(t(i),
        R.fx(i) = 1;
    );

{set initial solution Rbar}
{set initial bounds for DAD}
SOLVE SUBNET_DESIGN using MIP minimizing Z;

rbar(i)=no;
LOOP(i$(R.L(i)>0.5),
    rbar(i) = yes;
);

PUT SUM(i,R.L(i)):6:0,' Total Repeaters' / ;
PUT 'Initial Repeater Locations' / ;
PUT 'Site      Row      Column' / ;
LOOP(rbar(i),
    PUT i.tl:7, (CEIL(ORD(i)/15)):8:0, (MOD(ORD(i)-1,15)+1):8:0 / ;
);
PUT / ;
LOOP(i,
    IF(rbar(i),
        IF(s(i),
            PUT 'S ' ;
        );
        IF(t(i),
            PUT 'T ' ;
        );
        IF(not t(i) and not s(i),
            PUT 'R ' ;
        );
    else
        PUT '. ' ;
    );
    if(MOD(ORD(i),15)=0,
        PUT / ;
    );
);
PUT / / ;
PUT 'Arc Flows' / ;
LOOP(arc(i,j)$ (SUM(s(k),Y.L(i,j,k))>eps),
    PUT i.tl:10, ' ', j.tl:10, ' ', (SUM(s(k),Y.L(i,j,k))):5:2 / ;
);
PUT / / ;

PUT 'Blocked Flows' / ;

```

```

LOOP(s(i)$(E.L(i)>eps),
  PUT i.tl:10, ' ', E.L(i) / ;
);
PUT / / ;

lb_DAD = Z.L ;
ub_DAD = +inf ;
r_iter = 0;
SUBNET_DUALILP.optcr = epsilon_AD;

rbest(i) = no;
xbest(iprime) = no;
xbard(iprime,d) = no;

SCALAR
  num_repeats
;

put 'DAD lb=',lb_DAD:12:6 / ;
{while DAD relative gap > epsilon and r_iter < max_r_iters}
while(ub_DAD - lb_DAD > epsilon_DAD*lb_DAD,
  while(r_iter < max_r_iters,
    {solve AD: two ways to do this, either dualILP or Benders. This is
dualILP.}
    {set initial solution xbar}
    solve SUBNET_DUALILP using MIP maximizing Z;
    {if AD solution lower than DAD upper bound}
    if(SUBNET_DUALILP.object < ub_DAD,
      {update DAD UB}
      ub_DAD = SUBNET_DUALILP.object ;
      put 'DAD * ub=',ub_DAD:12:6 / ;
      {update incumbent defense}
      rbest(i) = no;
      loop(rbar(i),
        rbest(i) = yes ;
      );
      {record attack corresponding to incumbent defense}
      xbest(iprime) = no;
      LOOP(iprime$(X.L(iprime)>0.5),
        xbest(iprime) = yes;
      );
    );
    if(r_iter>1,
      {check for repeated attack plan}
      num_repeats = 0;
      loop(d$(ord(d)<=r_iter),
        if( (SUM(xbard(iprime,d), X.L(iprime)) >= max_attacks),
          num_repeats = num_repeats + 1;
        );
      );
      if(num_repeats >= 1,
        put ' repeat attack found, re-solving for unique attack' / ;
        solve SUBNET_DUALILP_UNIQUE using MIP maximizing Z;
      );
    );
    {Solve DAD Master for next r_iter}
    r_iter = r_iter + 1;
    PUT 'r_iter: ',r_iter:4:0 / ;
    loop(d$(ord(d)=r_iter),
      loop(iprime$(X.L(iprime)>0.5),
        put ' atk: ', iprime.tl:5 / ;
        xbard(iprime,d) = yes;
      );
    );
  );
};

```

```

    );
  );
  solve SUBNET_DAD_MASTER using MIP minimizing Z;
  {if master solution > LB}
  if(SUBNET_DAD_MASTER.object > lb_DAD,
    {update LB}
    lb_DAD = SUBNET_DAD_MASTER.object;
    put 'DAD    lb=',lb_DAD:12:6 / ;
  );
  {update design Rbar = R.L}
  rbar(i) = no;
  loop(i$(R.L(i)>0.5),
    put '      def: ', i.tl:5 / ;
    rbar(i) = yes;
  );
);
);

rbar(i) = no;
LOOP(rbest(i),
  rbar(i) = yes;
);

xbar(iprime)=no;
LOOP(xbest(iprime),
  xbar(iprime) = yes;
);

SOLVE SUBNET_OPERATOR USING MIP MINIMIZING Z;

PUT SUM(i,R.L(i)):6:0,' Total Repeaters' / ;
PUT 'Optimal Repeater Locations' / ;
PUT 'Site      Row      Column' / ;
LOOP(rbar(i),
  PUT i.tl:7, (CEIL(ORD(i)/15)):8:0, (MOD(ORD(i)-1,15)+1):8:0 / ;
);
PUT / ;
LOOP(i,
  if(xbar(i),
    if(rbar(i),
      PUT 'Y ' ;
    else
      put 'X ' ;
    );
  else
    IF(rbar(i),
      If(s(i),
        PUT 'S ' ;
      );
      IF(t(i),
        PUT 'T ' ;
      );
      IF(not t(i) and not s(i),
        PUT 'R ' ;
      );
    else
      PUT '. ' ;
    );
  );
  if(MOD(ORD(i),15)=0,
    PUT / ;
  );
);

```

```

);
PUT / / ;

PUT 'Attacks' / ;
LOOP(xbar(iprime),
    PUT iprime.tl:10, (CEIL(ORD(iprime)/15)):5:0, (MOD(ORD(iprime)-1,15)+1):5:0
/ ;
);
PUT / / ;

PUT 'Arc Flows' / ;
LOOP(arc(i,j)$ (SUM(s(k),Y.L(i,j,k))>eps),
    PUT i.tl:10, ' ', j.tl:10, ' ', (SUM(s(k),Y.L(i,j,k))):5:2 / ;
);
PUT / / ;

PUT 'Blocked Flows' / ;
LOOP(s(i)$ (E.L(i)>eps),
    PUT i.tl:10, ' ', E.L(i) / ;
);

PUTCLOSE out;

```

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX B. RESULTING GAMS OUTPUT FILE FOR NETWORK CONFIGURATION A WITH TWO ATTACKS

```

10 Total Repeaters
Initial Repeater Locations
Site      Row      Column
n015      1       15
n016      2        1
n021      2        6
n026      2       11
n113      8        8
n176     12       11
n211     15        1
n216     15        6
n220     15       10
n225     15       15

. . . . . T
S . . . . R . . . . R . . . .
. . . . .
. . . . .
. . . . .
. . . . .
. . . . .
. . . . . S . . . . .
. . . . .
. . . . .
. . . . .
. . . . . R . . . .
. . . . .
. . . . .
S . . . . R . . . . R . . . . T

Arc Flows
n016      n021      1.00
n021      n026      1.00
n026      n015      1.00
n113      n176      1.00
n176      n225      1.00
n211      n216      1.00
n216      n220      1.00
n220      n225      1.00

Blocked Flows

DAD   lb=      8.000000
DAD * ub=     15.000000

r_iter:    1
  atk: n160
  atk: n200
DAD   lb=      9.000000
  def: n010
  def: n015
  def: n016
  def: n021

```

```

def: n056
def: n113
def: n170
def: n211
def: n225

r_iter:    2
  atk: n005
  atk: n040
DAD  lb=   10.000000
  def: n015
  def: n016
  def: n072
  def: n079
  def: n113
  def: n154
  def: n211
  def: n215
  def: n220
  def: n225

r_iter:    3
  atk: n056
  atk: n204
  def: n015
  def: n016
  def: n065
  def: n113
  def: n154
  def: n162
  def: n211
  def: n216
  def: n221
  def: n225

r_iter:    4
  atk: n146
  atk: n205
  def: n005
  def: n010
  def: n015
  def: n016
  def: n056
  def: n064
  def: n113
  def: n162
  def: n170
  def: n211
  def: n225
DAD * ub=   13.000000

r_iter:    5
  atk: n040
  atk: n146
  def: n015
  def: n016
  def: n072
  def: n079
  def: n113
  def: n154
  def: n162
  def: n211

```

```
def: n216
def: n221
def: n225
DAD * ub= 12.000000
```

```
r_iter: 6
atk: n056
atk: n146
def: n015
def: n016
def: n050
def: n072
def: n113
def: n154
def: n176
def: n211
def: n225
```

```
r_iter: 7
atk: n058
atk: n162
def: n010
def: n015
def: n016
def: n056
def: n079
def: n113
def: n154
def: n162
def: n176
def: n211
def: n225
```

```
r_iter: 8
atk: n040
atk: n161
def: n005
def: n015
def: n016
def: n056
def: n064
def: n072
def: n113
def: n170
def: n176
def: n211
def: n225
```

```
r_iter: 9
atk: n056
atk: n160
def: n015
def: n016
def: n050
def: n056
def: n072
def: n113
def: n162
def: n170
def: n176
def: n211
def: n225
```

```

r_iter: 10
  atk: n056
  atk: n161
DAD lb= 11.000000
  def: n015
  def: n016
  def: n065
  def: n069
  def: n113
  def: n128
  def: n170
  def: n176
  def: n191
  def: n211
  def: n225

r_iter: 11
  atk: n160
  atk: n205
  def: n015
  def: n016
  def: n021
  def: n065
  def: n072
  def: n113
  def: n128
  def: n170
  def: n191
  def: n211
  def: n225

r_iter: 12
  atk: n056
  atk: n175
  def: n010
  def: n015
  def: n016
  def: n051
  def: n079
  def: n113
  def: n154
  def: n211
  def: n217
  def: n222
  def: n225

r_iter: 13
  atk: n009
  atk: n208
  def: n015
  def: n016
  def: n035
  def: n079
  def: n113
  def: n128
  def: n170
  def: n177
  def: n191
  def: n211
  def: n225

```

```

r_iter: 14
  atk: n019
  atk: n142
  def: n015
  def: n016
  def: n072
  def: n079
  def: n113
  def: n128
  def: n162
  def: n170
  def: n191
  def: n211
  def: n225

r_iter: 15
  atk: n056
  atk: n176
  def: n015
  def: n016
  def: n056
  def: n065
  def: n113
  def: n114
  def: n129
  def: n163
  def: n170
  def: n211
  def: n225

r_iter: 16
  atk: n040
  atk: n147
DAD lb= 11.142857
  def: n010
  def: n015
  def: n016
  def: n050
  def: n056
  def: n067
  def: n113
  def: n170
  def: n211
  def: n220
  def: n225

r_iter: 17
  atk: n009
  atk: n040
  def: n005
  def: n010
  def: n015
  def: n016
  def: n065
  def: n069
  def: n113
  def: n162
  def: n170
  def: n211
  def: n225

r_iter: 18

```

```

    atk: n010
    atk: n146
    def: n015
    def: n016
    def: n021
    def: n050
    def: n056
    def: n113
    def: n154
    def: n172
    def: n211
    def: n221
    def: n225

r_iter: 19
    atk: n040
    atk: n205
    def: n015
    def: n016
    def: n021
    def: n026
    def: n054
    def: n07
    def: n079
    def: n113
    def: n154
    def: n211
    def: n225

r_iter: 20
    atk: n040
    atk: n056
    def: n015
    def: n016
    def: n056
    def: n064
    def: n113
    def: n154
    def: n159
    def: n162
    def: n193
    def: n211
    def: n225

r_iter: 21
    atk: n040
    atk: n177
    def: n015
    def: n016
    def: n072
    def: n079
    def: n113
    def: n154
    def: n158
    def: n207
    def: n211
    def: n215
    def: n225

r_iter: 22
    atk: n056
    atk: n191

```

```

def: n015
def: n016
def: n021
def: n050
def: n056
def: n113
def: n154
def: n173
def: n211
def: n222
def: n225

r_iter: 23
  atk: n040
  atk: n206
  def: n005
  def: n015
  def: n016
  def: n027
  def: n053
  def: n064
  def: n072
  def: n113
  def: n170
  def: n211
  def: n225

r_iter: 24
  atk: n011
  atk: n071
  def: n010
  def: n015
  def: n016
  def: n065
  def: n113
  def: n162
  def: n170
  def: n174
  def: n179
  def: n211
  def: n225

r_iter: 25
  atk: n146
  atk: n180
  def: n015
  def: n016
  def: n050
  def: n072
  def: n113
  def: n154
  def: n159
  def: n162
  def: n164
  def: n211
  def: n225

r_iter: 26
  atk: n058
  atk: n148
  def: n015
  def: n016

```

```

def: n056
def: n064
def: n113
def: n154
def: n159
def: n162
def: n207
def: n211
def: n225

r_iter: 27
  atk: n063
  atk: n138
  def: n012
  def: n015
  def: n016
  def: n065
  def: n113
  def: n162
  def: n170
  def: n174
  def: n211
  def: n223
  def: n225

r_iter: 28
  atk: n146
  atk: n173
  def: n010
  def: n015
  def: n016
  def: n056
  def: n065
  def: n069
  def: n113
  def: n162
  def: n170
  def: n211
  def: n225

r_iter: 29
  atk: n055
  atk: n146
  def: n015
  def: n016
  def: n050
  def: n072
  def: n113
  def: n162
  def: n170
  def: n174
  def: n211
  def: n220
  def: n225

r_iter: 30
  atk: n034
  atk: n154
  def: n015
  def: n016
  def: n028
  def: n065

```

```

def: n069
def: n072
def: n113
def: n211
def: n216
def: n221
def: n225

```

#### 11 Total Repeaters

##### Optimal Repeater Locations

| Site | Row | Column |
|------|-----|--------|
| n015 | 1   | 15     |
| n016 | 2   | 1      |
| n072 | 5   | 12     |
| n079 | 6   | 4      |
| n113 | 8   | 8      |
| n154 | 11  | 4      |
| n162 | 11  | 12     |
| n211 | 15  | 1      |
| n216 | 15  | 6      |
| n221 | 15  | 11     |
| n225 | 15  | 15     |

```

. . . . . T
S . . . . .
. . . . .
. . . . . X . . . .
. . . . . R . . . .
. . . R . . . . .
. . . . . S . . . . .
. . . . .
. . . . . X . . . .
. . . R . . . . . R . . .
. . . . .
. . . . .
. . . . .
S . . . . R . . . . R . . . T

```

##### Attacks

|      |    |    |
|------|----|----|
| n056 | 4  | 11 |
| n146 | 10 | 11 |

##### Arc Flows

|      |      |      |
|------|------|------|
| n016 | n079 | 1.00 |
| n079 | n154 | 1.00 |
| n113 | n154 | 1.00 |
| n154 | n216 | 2.00 |
| n211 | n216 | 1.00 |
| n216 | n221 | 3.00 |
| n221 | n225 | 3.00 |

##### Blocked Flows

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

- Ackerman, R. K. 2004. FORCEnet demands drive Navy command. *Signal*, **59**(4), 22–25.
- Alderson, D. L., G. G. Brown, W. M. Carlyle, R. K. Wood. 2011. Solving defender-attacker-defender models for infrastructure defense. *Proceedings of 12th INFORMS Computer Society Conference*, Monterey, CA, 2849, 9 – 11 January 2011. DOI: 10.1287/ics.2011.0047.
- Amante, C., B. W. Eakins. 2009. ETOPO1 1 Arc-minute global relief model: procedures, data sources and analysis. *NOAA Technical Memorandum NESDIS NGDC-24*, 1.
- Bachmayer, R., J. A. Rice, R. Crebert, C. Fletchert. 2004. Navigation and control of multiple gliders in an underwater acoustic network, *Proceedings of 2004 IEEE/OES Autonomous Underwater Vehicles*, Sebasco Estates, ME, 54–58, 17–18 June 2004. DOI: 10.1109/AUV.2004.1431193.
- Barreto, S., C. Ferreira, J. Paixão, S. S. Beatriz. 2007. Using clustering analysis in a capacitated location-routing problem. *European Journal of Operational Research*, **179**(2007), 968–977. DOI:10.1016/j.ejor.2005.06.074.
- Beidiger, J. S. 2010. *Environmental acoustic considerations for passive detection of maritime targets by hydrophones in a deep ocean trench*. Master's Thesis, Department of Physics, Naval Postgraduate School, Monterey, CA.
- Belenguer, J.-M., E. Benavent, C. Prins, C. Prodhon, R. Wolfler-Calvo. 2006. A branch and cut method for the capacitated location-routing problem. *2006 International Conference on Service Systems and Service Management*, Troyes, France, **2**, 1541–1546, 25 – 27 Oct 2006. DOI: 10.1109/ICSSSM.2006.320765.
- Berger, R. T., C. R. Coullard, M. Daskin. 2007. Location-routing problems with distance constraints. *Transportation Science*, **41**(1), 29–43. DOI: 10.1287/trsc.1060.0156.
- Blodgett, P. M. 2009. *Submarine laser communication options and the impact of light refraction at the air-sea interface*. Master's Thesis, Department of Physics, Naval Postgraduate School, Monterey, CA.
- Bohner, C. G. 2003. *A distributed approach to underwater acoustic communications*. Master's Thesis, Department of Ocean Engineering, Massachusetts Institute of Technology and Woods Hole Oceanographic Institution, Woods Hole, MA.
- Brown, G., M. Carlyle, J. Salmerón, K. Wood. 2006. Defending critical infrastructure. *Interfaces*, **36**(6), 530–544. DOI: 10.1287/inte.1060.0252.

- Brown, G. G., W. M. Carlyle, and R. K. Wood. 2008. Optimizing department of homeland security defense investments: applying defender-Attacker(-defender) optimization to terror risk assessment and mitigation. *National Research Council, 2008, "Department of Homeland Security Bioterrorist Risk Assessment: A Call for Change,"* Appendix E, National Academies Press, Washington, DC.
- Browne, H. A. 2004. FORCEnet: The Navy has it right. *Signal*, **59**(4), 14.
- Chappell, S. G., J. C. Jalbert, P. Pietryka, J. Duchesney. 1994. Acoustic communication between two autonomous underwater vehicles. *Proceedings of AUV'94, The 1994 Symposium on Autonomous Underwater Vehicle Technology*, Cambridge, MA, **1**, 462–469, 19 – 20 Jul 1994. DOI: 10.1109/AUV.1994.518661.
- Fletcher, C.L., J. A. Rice, R. K. Creber. 2003. Operator access to acoustically networked undersea systems through the Seaweb server. *Proceedings of OCEANS 2003*, San Diego, CA, **1**, 1–5, 22 – 26 September 2003. DOI: 10.1109/OCEANS.2003.178511.
- Fletcher, C.L., J. A. Rice, R. K. Creber, D. L. Codiga, D. L. 2001. Undersea acoustic network operations through a database-oriented server/client interface. *Proceedings of OCEANS 2001 MTS/IEEE Conference and Exhibition*, Honolulu, HI, **4**, 2071–2075, 5 – 8 November 2001. DOI: 10.1109/OCEANS.2001.968317.
- GAMS Development Corporation. 2013. Download GAMS Distribution 24.1.3. Retrieved 6 August 2013, <http://www.gams.com/download>.
- Goh, M. C. 2010. *Event-driven simulation and analysis of an underwater acoustic local area network*. Master's Thesis, Department of Physics, Naval Postgraduate School, Monterey, CA.
- Green, D. 2007. Navigation aids, object marking and acoustic communications - an integrated solution. *Proceedings of OCEANS 2006 - Asia Pacific*, Singapore, **1** – **7**, 16–19, 16 – 19 May 2007. DOI: 10.1109/OCEANSAP.2006.4393941.
- Green, M., J. A. Rice, S. Merriam. 1998. Underwater acoustic modem configured for use in a local area network (LAN). *Proceedings of OCEANS '98 Conference*, Nice, France, **2**, 634–638, 28 September – 1 October 1998. DOI: 10.1109/OCEANS.1998.724316.
- Grimmett, D.J. 2007. Message routing criteria for undersea acoustic communication networks. *Proceedings of OCEANS 2007 - Europe*, 16, Aberdeen, United Kingdom, 18 – 21 June 2007. DOI: 10.1109/OCEANSE.2007.4302451.
- Grimmett, D.J. 2009. Undersea communication network self-localization during the Unet'08 seatrial. *Proceedings of MTS/IEEE Biloxi - Marine Technology for Our Future: Global and Local Challenges OCEANS 2009*, Biloxi, MS, **1**–**7**, 26 – 29 October 2009.

- Hartfield, G. I. 2003. *Link-layer and network-layer performance of an undersea acoustic network at fleet battle experiment-India*. Master's Thesis, Department of Information Sciences, Naval Postgraduate School, Monterey, CA.
- IBM. 2013. IBM ILOG CPLEX Optimization Studio Preview Edition Trial. Retrieved 6 August 2013, <http://www-01.ibm.com/software/websphere/products/optimization/cplex-studio-preview-edition>.
- Kilfoyle, D. B., Baggeroer, A. B. 2000. The State of the art in underwater acoustic telemetry, *IEEE Journal of Oceanic Engineering*, **25**, 427.
- Kriewaldt, H. A. 2006. *Communications performance of an undersea acoustic wide-area network*. Master's Thesis, Engineering Acoustic Academic Committee, Naval Postgraduate School, Monterey, CA.
- Li, B., J. Huang, S. Zhou, K. Ball, M. Stojanovic, L. Freitag, P. Willett. 2009. MIMO-OFDM for high-rate underwater acoustic communications. *IEEE Journal of Oceanic Engineering*, **34**(4), 634–644, DOI: 10.1109/JOE.2009.2032005.
- McGirr, S., K. Raysin, C. Ivancic, C. Alspaugh. 1999. Simulation of underwater sensor networks. *Proceedings of MTS/IEEE Riding the Crest into the 21st Century OCEANS '99*, Seattle, WA, **2**, 945–950, 13 – 16 September 1999.
- Munk, W. H., A. M. G. Forbes. 1989. Global ocean, “warming: an acoustic measure?” *Journal of Physical Oceanography*, **19**, 1765–1778.
- Nicholas, P. J. 2009. *Optimal transmitter placement in wireless mesh networks*. Master's Thesis, Naval Postgraduate School, Monterey, CA.
- Office of Naval Research Corporate Communications. 2010. Microbial fuel cell: A new source of green energy. Retrieved September 4, 2010 from <http://www.onr.navy.mil/en/Media-Center/Press-Releases/2010/Microbial-Fuel-Cell.aspx>.
- Ong, C. W. (2008). *A discovery process for initializing ad hoc underwater acoustic networks*. Master's Thesis, Engineering Acoustic Academic Committee, Naval Postgraduate School, Monterey, CA.
- Ouimet, S. P., M. J. Hahn, J. Rice. 2005. Undersea communication network as a UUV navigation aid. *Proceedings of MTS/IEEE OCEANS 2005*, Washington, D.C., **3**, 2485–2490, 18 – 23 September, 2005. DOI: 10.1109/OCEANS.2005.1640141.
- Proakis J. G., J. A. Rice, E. M. Sözer, and M. Stojanovic. 2003. Shallow-water acoustic networks. *Encyclopedia of Telecommunications*, Wiley-Interscience.

- Ramp, S.R., J. Rice, M. Stacey, T. Garfield, J. Largier. 2009. SF bayweb 2009: Planting the seeds of an observing system in the san Francisco bay. *Proceedings of MTS/IEEE Biloxi - Marine Technology for Our Future: Global and Local Challenges OCEANS 2009*, Biloxi, MS, 1–8, 26 – 29 October 2009.
- Raysin, K.; J. Rice, E. Dorman, S. Matheny. 1999. Telesonar network modeling and simulation. *Proceedings of MTS/IEEE OCEANS '99. Riding the Crest into the 21st Century*, Seattle, WA, 2(747–752), 13 – 16 September 1999. DOI: 10.1109/OCEANS.1999.804900.
- Rice J. A. 2002. Undersea networked acoustic communication and navigation for autonomous mine-countermeasure systems. *Proceedings of 5th International Symposium on Technology and the Mine Problem*, Monterey, CA, 19.
- Rice, J. 2000. Telesonar signaling and seaweb underwater wireless networks. *Presented at NATO Research & Technology Agency Symposium on New Information Processing Techniques for Military*, Istanbul, Turkey, 1–14.
- Rice, J. (2005). Seaweb Acoustic Communication and Navigation Networks. *Proceedings of International Conference of Underwater Acoustic Measurements: Technologies & Results*, Crete, Greece, 17.
- Rice, J. A., R. K. Creber, C. L. Fletcher, P. A. Baxley, K. E. Rogers, D. C. Davison. 2001. Seaweb underwater acoustic nets, *Space and Naval Warfare Systems Center San Diego Biennial Review*, 234–250. Retrieved September 10, 2010 from <http://www.spawar.navy.mil/sti/publications/pubs/td/3117/234.pdf>.
- Rice, J. A., C. L. Fletcher, R. K. Creber, J. E. Hardiman, K. F. Scussel. 2001. Networked undersea acoustic communications involving a submerged submarine, deployable autonomous distributed sensors, and a radio gateway buoy linked to an ashore command center. *Proceedings of UDT Hawaii Undersea Defence Technology*, Waikiki, HI, paper 4A.1, 30 October – 1 November 2001.
- Rice, J., D. Green. 2008. Underwater acoustic communications and networks for the US Navy's seaweb program," *Proceedings of The Second International Conference on Sensor Technologies and Applications SENSORCOMM '08*, Cap Esterel, France, 715–722, 25 – 31 August 2008. DOI: 10.1109/SENSORCOMM.2008.137.
- Rice, J., B. Creber, C. Fletcher, P. Baxley, P., K. Rogers, K. McDonald, D. Rees, M. Wolf S. Merriam, R. Mehio, J. Proakis, Scussel, K., D. Porta, J. Baker, J. Hardiman, and D. Green. 2000 Evolution of seaweb underwater acoustic networking. *Proceedings of MTS/IEEE Conference and Exhibition OCEANS 2000*, Providence, RI, 3, 2007–2017, 11 – 14 September 2000. DOI: 10.1109/OCEANS.2000.882235.

- Sanchez, A. 2010. *Internet service provider network evolution in the presence of changing environmental conditions*. Master's Thesis, Naval Postgraduate School, Monterey, CA.
- Schrope, M. 2000. The net gets wet. *Business 2.0* 5(20), 212.
- Shankar, A. 2008. *Optimal jammer placement to interdict wireless network services*. Master's Thesis, Naval Postgraduate School, Monterey, CA.
- Sözer, E. M., M. Stojanovic, J. G. Proakis. 2000a. Initialization and routing optimization for ad hoc underwater acoustic networks. *Proceedings of Opnetwork '00*, Washington, D.C., 1 – 7, August 2000. DOI: 10.1.1.114.2208.
- Sözer, E. M., M. Stojanovic, J. G. Proakis. 2000b. Underwater acoustic networks. *IEEE Journal of Oceanic Engineering*, 25(1), 7283. Jan 2000.
- Thompson, S. R. 2009a. *Displacement of tethered hydro-acoustic modems by uniform horizontal currents*. Master's Thesis, Department of Mechanical Engineering, Naval Postgraduate School, Monterey, CA.
- Thompson, S. R. 2009b. *Sound propagation considerations for a deep-ocean acoustic network*. Master's Thesis, Department of Physics, Naval Postgraduate School, Monterey, CA.
- Urick, R. J. 1983. *Principles of underwater sound*. Peninsula Publishing, Los Altos, CA.
- Zinkhon, D. C. 2009. *Undersea node localization using node-to-node acoustic ranges in distributed seaweb network*. Master's Thesis, Naval Postgraduate School, Monterey, CA.

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